Operaciones en el Ambiente de la Información

BM (R) Mg. Alejandro Moresi
GD (R) Mg. Gustavo Motta
CL (R) Mg. Gustavo A. Trama
CR EB Dr. Márcio Saldanha Walker
TC IM (R) Carlos Amaya

FMC
Facultad Militar Conjunta

UNDEF
Universidad de la Defensa Nacional

Operaciones en el Ambiente de la Información

FMC
Facultad Militar Conjunta

UNDEF
Universidad de la Defensa Nacional

Operaciones en el Ambiente de la Información

BM (R) Mg. Alejandro Moresi
GD (R) Mg. Gustavo Motta
CL (R) Mg. Gustavo A. Trama
CR EB Dr. Márcio Saldanha Walker
TC IM (R) Carlos Amaya

Operaciones en el ambiente de la información / Alejandro Moresi ... [et al.]. - 1a ed. -
Ciudad Autónoma de Buenos Aires : Estado Mayor Conjunto de las Fuerzas Armadas, 2023.

270 p. ; 22 x 16 cm.

ISBN 978-987-26086-4-4

1. Ciberespacio. 2. Campo Electromagnético. I. Moresi, Alejandro.
CDD 355.07

Editor y propietario
Escuela Superior de Guerra Conjunta

Editorial Visión Conjunta
Secretaría de Extensión

Diseño y diagramación
Juan Santiago Gallelli

ISBN 978-987-26086-4-4

Índice

Prólogo

El ambiente de la información no es nuevo, pero la comprensión de su importancia estratégica está cada vez más presente. La información, como base de los conflictos entre estados, se ha caracterizado cada vez más por una competencia continua que involucra una naturaleza multidominio de medios militares y no militares en estos temas. Los propósitos están relacionados con los recursos que siempre serán limitados, y las necesidades e intereses nacionales de cada estado siempre buscarán el mejor bienestar para su sociedad.

El siglo XXI abrió una nueva era de competencia entre estados, que abarca la información generada en diferentes campos de poder, diplomático, económico, social, científico tecnológico y militar. Estos campos no manejan información estanca, porque siempre está conectada. La información política y estratégica implica acciones integrales y de amplio alcance, con diferentes actores en una constante búsqueda de información, superioridad en todos los ámbitos y poder.

Todo esto se basa en un entorno que considera que la tecnología avanza a velocidad exponencial y provoca cambios cognitivos de innovación que enfatizan la importancia de la información en la relación de paz y guerra entre estados. La tecnología ha agregado posibilidades militares a los activos terrestres, marítimos, aéreos y espaciales en el último siglo. En este siglo XXI, las posibilidades se han expandido a los dominios del ciberespacio y cognitivo.

De las directivas políticas de defensa de nuestro país, surge la orientación general de explorar la posibilidad de contar con nuevos efectos militares a partir de la combinación del conocimiento tradicional con formas innovadoras basadas en la tecnología y el conocimiento para hacer frente a amenazas de diferentes dominios. El desarrollo de una estrategia militar de abordaje multicapas es consecuente con esta idea y con la creciente necesidad de considerar el impacto de los efectos de la información en la estrategia de defensa nacional.

La verificación de operaciones en el ambiente de la información es un elemento reciente en la planificación militar. Existe una gran incertidumbre doctrinaria respecto de los términos conceptuales que terminaron por establecer distintas posi-

bilidades de percepción respecto del fenómeno. Los dominios de la guerra ya no se restringen a los de tierra, mar y aire, o incluso al espacio, ahora pueden incluir actividades y acciones de información y cognitivas en el ciberespacio. El advenimiento de las operaciones en el ciberespacio ha ampliado la velocidad y las posibilidades no físicas de la acción militar.

Los países buscan estructurar una capacidad de defensa activa, más allá de considerar la declaración de guerra no formal, provocando una situación de conflicto permanente. En este sentido, existe la necesidad de buscar dilucidar los conceptos que permitan el establecimiento de la correcta interacción con las capacidades especiales relacionadas con la información. Tales medidas permiten mirar hacia el futuro, considerando la necesidad inmediata de generar fuerzas armadas bien equipadas y en permanente estado de preparación para la defensa nacional.

El presente trabajo, constituye la primera contribución académica que se elabora en la Escuela Superior de Guerra Conjunta de las FFAA de la República Argentina sobre las "Operaciones en el Ambiente de la Información".

El propósito que ha motivado su elaboración es el de contribuir a su comprensión, a través de una visión interdisciplinaria que reúna en un solo documento aspectos de la evolución del conflicto hacia el ambiente de la información, así como los relacionados con el impacto y los vínculos de la guerra electromagnética, la guerra ciberespacial y la comunicación estratégica.

El trabajo ha sido preparado por varios especialistas argentinos y uno brasileño. En él, se ha privilegiado la amplia exploración y libertad académica empleando, para ello, fuentes nacionales y extranjeras.

La presentación del estado del arte y de diferentes perspectivas ha enriquecido el trabajo y permite cumplir con la triple finalidad de acercar a planificadores civiles y militares y académicos sobre lo que está ocurriendo en el mundo, acortar tiempos valiosos y contar con más elementos de juicio a la hora de tomar decisiones. En síntesis, la idea es efectuar un mínimo aporte al conocimiento en este novel campo, aun cuando se es consciente de su constante evolución y de la posibilidad de incurrir en superposiciones y porque no, contradicciones que, a nuestro juicio, en nada empañan el esfuerzo realizado.

Las definiciones presentadas buscan ampliar la discusión del tema para subsidiar el trabajo continuo de investigación e innovación. No se presentarán conceptos cerrados e irrefutables; por el contrario, la intención es mostrar la amplia discusión profesional según el enfoque doctrinario de diferentes países.

El Capítulo I nos acerca, a manera de introducción, a un marco general sobre el conflicto actual y futuro como antesala al tratamiento de las distintas interacciones que produce la información. Parte de aspectos básicos del conflicto y su interconexión con la estrategia y las relaciones internacionales, hasta alcanzar las teorías estratégicas contemporáneas, los desarrollos académicos posteriores a la Guerra Fría y las visiones doctrinarias militares sobre el ambiente del conflicto de algunos países respecto del entorno de la información.

La globalización y la creciente influencia del campo de la cibernética impactan sobre la defensa, el planeamiento y la ejecución de las operaciones militares. La forma de hacer la guerra cambia en forma permanente y los profesionales, civiles y militares, necesitan que el pensamiento estratégico evolucione al ritmo de la aparición de nuevos ambientes y medios técnicos de alcances globales. La revolución tecnológica e industrial, la inteligencia artificial (IA), la información cuántica, la Big data y la Internet de las Cosas han cobrado un impulso que parece no agotarse. En un ambiente de creciente competencia internacional, los sistemas de decisión acortan tiempos y distancias, las armas llegan más lejos, en forma más precisa y permiten proyectar poder sin mostrar vulnerabilidad.

La guerra se da en todos los ámbitos en forma simultánea, adonde el componente militar tiene un rol trascendental pero no exclusivo. Hoy no se distingue entre combatientes y no combatientes. Mientras los ciclos de la decisión se acortan y los niveles de la guerra parecen fusionarse, las percepciones, la voluntad y la moral se mueven a caballo de la tecnología de la información (TI). De allí su importancia como función en el ámbito estratégico y conjunto. Los "ciber avances" actúan sobre el campo cognitivo y la capacidad de percepción de las personas generando reacciones que afectan el resultado de los conflictos, la decisión de los dirigentes y la moral de las tropas. En suma, como dice Nievas[1], "la matriz bélica ha cambiado". La guerra actual demanda que las respuestas contemplen un enfoque conjunto, combinado, integrado y multi-agencial de toda la sociedad. Una sociedad adonde la información fluye libremente, los niveles de la guerra tienden a subsumirse y las estrategias pueden fracasar fácilmente.

El capítulo II presenta los aspectos de la guerra electromagnética y su relación con otras capacidades especiales del ambiente de la información. Desde el punto de vista de la ciencia básica electromagnética la intención es interpretar o imaginar las potenciales amenazas de la exploración de este recurso y, por lo tanto, las medidas defensivas u ofensivas a adoptar en cada caso, comprendiendo mejor el verdadero sentido que tienen las acciones dentro de este ambiente. Las capacidades electromagnéticas están en permanente expansión de posibilidades ofensivas, defensivas y exploratorias. En este sentido, se puede considerar operar entre diferentes bandas de frecuencia considerando las posibilidades de los transmisores y receptores.

La intención es aclarar que en la guerra electromagnética es dable considerar que hay otros aspectos en juego, como la propaganda, la psicología, la desinformación, que afectan a la voluntad de pelear y a la toma de decisiones estratégicas. Estos son todos dominios, ambientes, o dimensiones de la guerra, para los cuales las comunicaciones electromagnéticas son hoy el campo de batalla inseparable de los aspectos cognitivos y del ciberespacio. Al final del capítulo se propone establecer la conexión entre los conceptos electromagnéticos en relación a las posibles acciones a considerar en la planificación militar.

---

1 Nievas, F. H. (2021, junio). Hacia una nueva geopolítica. La cuarta revolución espacial. (n. d. Germani, Ed.) Cuadernos de Marte (20), 395-429.

En el capítulo III, se debate acerca de la guerra cibernética, a partir de un análisis de la naturaleza de la guerra y su evolución hasta nuestros días con el impacto que implica tecnologías como la inteligencia artificial, la big data y la computación cuántica en el espectro cibernético.

La cuestión es abordada desde diferentes perspectivas comenzando por las normas legales que rigen en nuestro país, para continuar desarrollando consideraciones sobre una posible estrategia cibernética militar y operacional dando una idea de modelización de la problemática. El capítulo se cierra con una mirada que retrotrae al inicio del mismo para abordar la problemática actual y futura del conflicto cibernético.

En el capítulo IV se explora la forma en que la información, como un factor de poder, es empleada por países de occidente y también por organizaciones supranacionales, en conjunto con la diplomacia, la economía y el poder militar, para contrarrestar las acciones de oponentes y adversarios al mismo tiempo que se generan percepciones/adhesiones favorables, en los ámbitos de interés propios. Los conceptos doctrinarios en este ambiente todavía están en desarrollo. No existe una definición clara de métodos y responsabilidades que permitan establecer organizaciones lógicas para el uso del instrumento militar. Más allá de presentar conceptos, este capítulo pretende ampliar la discusión y análisis de las diferentes perspectivas doctrinarias militares y académicas acerca de la información.

Luego de analizar diferentes definiciones de los variados términos interrelacionados se concluye en la necesidad de elaborar una estrategia de comunicación y una narrativa propia, a partir de la cual los niveles estratégico, operacional y táctico, sean consistentes con ellas, puedan identificar y desarrollar las acciones necesarias para contribuir a prevenir y/o resolver un conflicto. Las narrativas estratégicas en el actual conflicto entre la Federación de Rusia y Ucrania y la integración de operaciones en el ambiente de la información para lograr efectos estratégicos son presentadas como un ejemplo para futuras operaciones militares. Concluye el capítulo señalando que la defensa contra las operaciones en el ambiente de la información casi siempre reflejará la necesidad de una respuesta de toda la nación y que cada vez más, los sistemas de defensa y seguridad dependerán de la explotación de la investigación comercial y la innovación razón por la cual, en el nivel nacional, el sector privado e incluso el público, necesitan ser convocados, ya que hay oportunidades para ello.

En el capítulo V se analiza, en base a la bibliografía occidental, la estrategia de confrontación de información de la Federación de Rusia y la equivalente de la República Popular de China.

La perspectiva académica de análisis de bibliografía de fuentes abiertas se vio limitada por la ausencia de este tipo de fuentes libre de militares, lo cual restringió el trabajo en relación a obtener un análisis adecuado en el caso de China y Rusia. Por lo tanto, con un enfoque contemporáneo se destaca, en lo posible, la importancia de la desinformación y el engaño para la doctrina rusa y la guerra de la opinión y psicológica de la escuela china.

El capítulo presenta una metodología para comparar las dos doctrinas, teniendo en cuenta que la lectura académica suele aproximarse a la visión entre China y Rusia. Sin embargo, destaca las diferencias y similitudes entre ambos puntos de vista sobre el uso de la información con fines militares. Concluye mostrando que, aunque es probable que persistan las diferencias clave en los enfoques chino y ruso, existe una creciente evidencia de que ambos países están aprendiendo uno de otro y mejorando su coordinación, lo que lleva a una creciente convergencia en sus esfuerzos de influencia.

El capítulo VI profundiza el tema de discusión sobre el concepto y aplicación doctrinaria de la Comunicación Estratégica en la planificación militar. La Comunicación Estratégica asume distintas perspectivas según las distintas percepciones. La percepción genera parámetros programables de amplio uso en sistemas de información. Estos conceptos presentan posibilidades estratégicas de empleo en el ambiente cognitivo. Sin embargo, la naturaleza abstracta del fenómeno ha provocado no sólo, la ausencia de una definición doctrinaria y la falta de consenso sobre qué es la comunicación estratégica sino también que el concepto pueda adquirir una connotación diferente en el entorno civil que en el militar.

El capítulo propone un análisis de lo que está presente en la doctrina de algunos países como EE. UU., Reino Unido, la OTAN, China y Rusia. Estos países son los protagonistas de una competición en el campo de la información, y por lo tanto han establecido su propia definición para buscar la superioridad constante en el control de la toma de decisiones. Sin embargo, existen otros países como la República Argentina que aún no ha establecido una definición doctrinaria del empleo en la planificación militar. En esta dirección, el capítulo enfatiza la importancia de estar preparados para actuar proactivamente en relación a los efectos que generan las políticas estratégicas de los países competidores.

En un desafío conceptual, la idea es separar el concepto de Comunicación Estratégica, que considera informar e influir en los más altos niveles, en relación con el de Operaciones de Información, más relacionado con la concepción del empleo militar en operaciones en el ambiente de la información. El intento es de organizar los conceptos de la comunicación estratégica desde los niveles más altos y proponer la coordinación que se espera. Esta coordinación resultará en la organización del tema en diferentes niveles, dirigiendo acciones estratégicas a los niveles más bajos operacional y táctico, facilitando o planeamiento militar.

La lectura de los capítulos de esta obra permite al estratega y a los académicos establecer parámetros constructivos para un análisis conceptual del fenómeno de la información en aspectos militares. La conclusión natural bajo una nueva perspectiva a generar, apunta a la existencia de un ambiente propio para las operaciones de información. Este ambiente no es en modo alguno aislado y es esencialmente un fenómeno social de construcción de relaciones en defensa de los intereses de un Estado nacional.

Capítulo 1
El conflicto

Por GD (R) Mg. Gustavo Motta

1. **Introducción**

Hablar del marco del conflicto en la actualidad es un ejercicio de compleja realización por dos razones. En primer lugar, porque a partir de 1988 se inició un período de cambios importantes, con impactos en la dinámica internacional y en la política doméstica de los estados. El 7 de diciembre de 1988, Mikhail Gorbachev anunció en la Asamblea General de la ONU, una drástica reducción de sus medios militares y nucleares y, un año después, el 9 de noviembre de 1989, se producía la caída del Muro de Berlín. Estos hechos producirían en el mundo un reacomodamiento en las relaciones de poder entre los estados, el debilitamiento del concepto de soberanía, la aparición de conflictos que responderían a dinámicas nuevas, cambios en las políticas y estrategias domésticas, con una creciente agenda social, una globalización cada vez más notoria y la búsqueda de nuevos mecanismos para atender los conflictos que surgieron a partir de 1990.

Adicionalmente, la velocidad en el procesamiento de la información, la inteligencia artificial, la robótica, la nanotecnología y la computación cuántica vienen produciendo indudables avances, pero también generan desafíos y retos a las élites de los estados por sus implicancias en la política, el derecho, las sociedades y los conflictos.

La revolución en la Tecnología de la Información (TI) toca todos los aspectos de la vida en sociedad, desde la forma de ganar de dinero y conectarse, hasta de confrontar y enamorarse. El ciberespacio se ha manifestado en los conflictos modernos y los sustratos informativos pasaron a la primera plana.

Los avances en el área de la informática actúan sobre el campo cognitivo y la capacidad de percepción de las personas genera diferentes reacciones individuales y colectivas e influencia en la adopción de decisiones en el nivel estado.

En el campo de la defensa se viene observando una creciente gravitación de la tecnología con evidentes impactos en la forma de hacer la guerra, en el desarrollo y generación de fuerzas y en las estrategias integrales de los estados (Finney , 2020, pág. 219).

Los nuevos espacios y dominios (ciber espacio y espacio) se agregaron a los ya tradicionales (terrestre, naval y aéreo), los cuales no perdieron su vigencia. Pero recalcaron la necesidad de abordar los problemas actuales a partir de soluciones integrales de todo el estado, con interconexiones y relaciones múltiples de naturaleza heterogénea, donde las fuerzas militares ocupan un rol importante, pero, de ninguna manera único, ni exclusivo.

En los dominios se busca lograr la libertad de acción necesaria para obtener los objetivos estratégicos. De allí la importancia que poseen para las maniobras y la obtención de efectos. La concepción de los dominios ha ido variando con el transcurrir de los años y hoy pareciera que un sexto dominio, el cognitivo, viene a consideración a caballo de las nuevas tecnologías.

El presente capítulo busca, al mismo tiempo, dar un marco general al conflicto actual y permitir el posterior tratamiento de las distintas interacciones que produce la información –en su concepto más amplio- sobre la defensa, el planeamiento y ejecución de las operaciones militares, ante la creciente influencia del campo de la cibernética en los conflictos modernos.

Para ello, se propone seguir el siguiente esquema. En primer lugar, se desarrollan aspectos básicos sobre el conflicto. Luego, se abordan dos perspectivas de las relaciones internacionales, la realista y de la "interdependencia compleja" y también, se trata la influencia de la cultura, los valores y "significados". Seguidamente, se trata la conexión entre el conflicto y la estrategia, con eje en la voluntad política y la fuerza moral de los contendientes. Luego, se desarrolla el impacto del dominio cibernético en la estrategia, la comunicación y los conflictos. Posteriormente, se exploran las teorías estratégicas contemporáneas, los desarrollos académicos ocurridos luego del fin de la Guerra Fría y las visiones doctrinarias militares sobre el ambiente del conflicto en algunos países. A modo de cierre, se abordan las respuestas de la política y estrategia en términos de diseño de fuerzas, como paso importante en el marco del conflicto actual.

2. **¿Qué es el conflicto?**

De acuerdo a la Real Academia Española (RAE), la palabra "conflicto" posee seis acepciones, tres de ellas se refieren a que es un "combate, lucha, pelea", un "enfrentamiento armado" y el "momento en que la batalla es más dura y violenta". Las restantes, tratan de situaciones desgraciadas y "de difícil salida" y de problemas o cuestiones que son materia de discusión. En todos los casos, el conflicto es un enfrentamiento de intereses, una cuestión que es materia de discusión y hasta de "lucha" o "combate"; lo que no significa que todo conflicto tenga características violentas, debido a que ellos pueden solucionarse o canalizarse a través de otros medios, como puede ser el diálogo

y la negociación u otras herramientas conforme a los objetivos perseguidos (Real Academia Española, 2022).

Julien Freund entiende por conflicto "al enfrentamiento de dos o más voluntades (individuales o colectivas), que manifiestan una respecto de la otra, una intención hostil a causa de un derecho, y que, para mantener o recuperar este derecho, tratan de quebrantar la resistencia del otro, recurriendo eventualmente a la violencia" (Freund, 1979, pág. 192).

Agrega que para lograr sus fines, puede ser que el "hombre del conflicto" ponga "en juego sus fuerzas materiales (armas) y humanas que él controla (fanáticos, bandas, tropas o ejércitos)", y "utilice la violencia. Lo que significa en el caso extremo que puede conducir la lucha hasta el aniquilamiento físico del otro" (Freund, 1979, pág. 194).

Schmitt da un enfoque un poco diferente. Al referirse al concepto de "enemigo" sostiene que éste no es el competidor o el adversario en general, sino un "conjunto de hombres que combate, al menos virtualmente, o sea sobre una posibilidad real, y que se contrapone a otro agrupamiento humano del mismo género". Agrega que los conceptos de amigo, enemigo y lucha adquieren su significado real por el hecho de la posibilidad real de eliminación física (Schmitt, 1984, pág. 179).

En un conflicto hay una red de intereses que son, en parte coincidentes y en parte discrepantes, según la "diversidad de visiones del mundo que tienen los actores, de su natural evolución y de la dialéctica de voluntades con que se influyen mutuamente" (Frischknecht, Lanzarini, Alonso, Moya Latrubesse, & Hernandez Otaño, 1995, pág. 23).

Coincidentemente, desde el punto de vista de la defensa nacional, la propia doctrina conjunta plantea al conflicto como el enfrentamiento de intereses, entre uno y otro u otros actores y que requiere la posibilidad cierta del empleo de las fuerzas militares. Los intereses reflejan las preferencias, ideas o conveniencias de cada actor, a las cuales les asignan un valor como la expresión de su voluntad (EMCO, PC 00-01 (proyecto), 2018, pág. 22).

Cuando Galtung hace una síntesis conceptual de la historia de la humanidad destaca la existencia de tres enfoques con referencia a los conflictos. El individual apuntado hacia el interior del ser humano con sus procesos y contradicciones; otro enfoque de "competición" darwiana –de incompatibilidad de objetivos entre las partes- y, por último, las que llama contradicciones intra-sociales (Calderón Concha, 2009, pág. 11).

Los conflictos son una constante en la historia de la humanidad porque, al decir de Calderón Concha, son inherentes "a todos los sistemas vivos en cuanto portadores de objetivos" (Calderón Concha, 2009, pág. 3). Por otra parte, Frischknecht y otros, sostienen que el conflicto es el estado natural de la interacción humana (Frischknecht, Lanzarini, Alonso, Moya Latrubesse, & Hernandez Otaño, 1995, pág. 23). Y, en la misma línea, aunque agregando la perspectiva del "poder", de Vergara sostiene que las disputas de poder y los conflictos son inherentes a la naturaleza humana y a la vida de los pueblos organizados en naciones (de Vergara, 2017, pág. 118).

3. **Conflictos, estados y actores**

Los grupos sociales, como sujetos con intereses, se fueron formando paulatinamente hasta alcanzar estados naciones[2] que luego dieron lugar a civilizaciones y regiones. Luego de la paz de Westfalia de 1648, el estado moderno separó la religión de las formas políticas y dio origen a la soberanía territorial, la libre determinación y la no injerencia en asuntos internos de otros estados. Así se fueron consolidando elementos constitutivos del estado, es decir, un pueblo, gobierno, territorio, fuerzas armadas y el establecimiento de relaciones con otros estados. La salud, la educación, la justicia y la seguridad fueron tomadas como funciones básicas de un estado y dieron origen a la aceptación de sus reglas por parte de los individuos (de Vergara, 2017, pág. 118).

Los estados, en su devenir histórico, han buscado seguridad, como condición básica para el bienestar y desarrollo. El orden wesfaliano, fue dando lugar a un sistema internacional que permitió que diferentes naciones vivieran acorde a sus preferencias mientras se respetaran sus mismos derechos y evitara el peligro de la "asimilación" (Williams & Bellamy, 2021, pág. 12). Pero los conflictos, como una inevitable constante continuaron, tanto en la política doméstica como en la política internacional (de Sousa & Carvalho de Oliveira, 2021, pág. 4).

Consecuentemente, una arista ineludible al hablar del conflicto es la que deviene de las perspectivas de las relaciones internacionales. En particular, para este trabajo, se aborda el enfoque "realista" en general y el denominado de la "interdependencia compleja".

Respecto del primero, la concepción estatocéntrica de Morgenthau se basa en dos elementos fundamentales que tienen una valoración sustantiva sobre la política y la estrategia de un estado. El primero, es el interés nacional y, el segundo, el equilibrio del poder. Aquí, el equilibrio o estabilidad internacional puede ser interpretado como la maximización de la posición política de cada unidad estatal dentro del sistema, mediante la acumulación de recursos militares y económicos (de Vergara, 2017, pág. 62).

Para Schmitt, el Estado como unidad política decisiva ha concentrado en sus manos una atribución inmensa: "la posibilidad de hacer la guerra y por consiguiente a menudo de disponer de la vida de los hombres". Sin embargo, aclara que la tarea de un Estado consiste en asegurar una paz estable (Schmitt, 1984, pág. 187).

El estado es la forma histórica de organización del ejercicio del poder y, según Morgenthau, el único actor digno de consideración en el sistema internacional, con intereses proyectados a través de una política exterior que pueden generar estados de conflicto (Barbé, 1987, pág. 155 y 157).

Del mismo modo, Tettamanti expresa que, según el enfoque realista, un estado asume compromisos en el mundo no por las normas de convivencia y del deber ser, sino por las referidas a la "lógica del interés" que es el mundo del ser. En consecuen-

2 El estado parte de una comunidad humana que, dentro de un determinado territorio, como uno de los elementos distintivos, reclama con éxito para sí el monopolio de la violencia física legítima porque "... "ha reunido todos los medios materiales en manos de su dirigente" (Weber, 2001, pág. 2 y 4).

cia, "...para quienes conciben el mundo como una relación de fuerzas y de confrontación, este razonamiento conlleva a ciertas consecuencias prácticas: a) el más fuerte se impone y b) todo país debe procurar ser el más fuerte o aliarse con éste, lo demás es puro idealismo" (Tettamanti, 1995, pág. 25).

Richard Nixon[3] sostenía que los estados tienen ideales e intereses y que al promoverlos entran en conflicto. Sin "un árbitro que resuelva las disputas, tal conflicto puede -y casi con certeza- conducir a la guerra. Estos principios precedieron a la Guerra Fría y sobrevivirán a la Guerra Fría. A menos que el mundo trascienda el sistema internacional actual, debemos aceptarlos como hechos inmutables de la vida" (Tettamanti, 1995, pág. 26).

Sin embargo, el enfoque realista pareciera quedarse corto en la consideración de otros actores importantes y las relaciones que se establecen. En los marcos de cooperación y competencia, la "interdependencia compleja"[4] permite explicar la existencia de canales múltiples que se establecen a través de nexos, formales e informales en el ámbito internacional y que podrían resumirse en relaciones interestatales, transnacionales y trans gubernamentales (Keohane & Nye, 1988, pág. 40).

Esta interdependencia ofrece algunas características que tipifican las relaciones entre estados y/o actores y las estrategias resultantes, ante diferentes escenarios adonde se pueden suceder los conflictos. Sucintamente se podría decir que: las agendas de los estados no son, para este enfoque, simétricas y sus múltiples temas no poseen una clara jerarquía. Del mismo modo, la "seguridad militar no domina consistentemente" la agenda como en otras perspectivas de las relaciones internacionales y "muchos temas surgen de lo que se acostumbraba considerar como terreno exclusivo de la política interna" (Keohane & Nye, 1988, pág. 41).

La consecuencia directa de estos aspectos de la interdependencia compleja es que "la diferencia entre temas internos y externos en un estado se vuelve borrosa" y, por ello, los variados asuntos a tratar en sus agendas deben ser considerados por "distintas áreas del gobierno y en diferentes niveles" con una amplia política de coordinación para evitar costos significativos (Keohane & Nye, 1988, pág. 41).

Las relaciones entre los estados son sólo una parte a considerar, "algo determinado e innegablemente objetivo" (Halliday, 2006, pág. 7). Pero, la problemática de los conflictos, no se circunscribe solamente a las relaciones inter estatales, porque existen otros elementos intervinientes que han aflorado producto de la globalización y sus derivaciones, la economía política, las tendencias sociales y la cultura en la comunidad mundial (Halliday, 2006, pág. 16). En el actual orden internacional han aparecido múltiples actores[5] importantes (que no son estados), -algunos con gran poder-, que

---

3 Nixon, Richard. (2013). *"Seize the Moment: America's Challenge in a One-superpower World".* USA: Simon&Schuster.

4 Ver "Poder e Interdependencia. La política mundial en transición" (Keohane & Nye, 1988, pág. 41).

5 Un actor es toda persona o grupo con intereses en el escenario del conflicto. Representa una racionalidad (intereses) y una motivación (Frischknecht, Lanzarini, Alonso, Moya Latrubesse, & Hernandez Otaño, 1995, pág. 71).

influyen tanto en el ámbito doméstico e internacional (Boone Bartholomees Jr., y otros, 2006, pág. 3).

> Los actores en el escenario global, tanto estatales como no estatales, deciden participar en alianzas y coaliciones y llevar a cabo políticas que apoyen el equilibrio y el cambio de tendencia en función de la evaluación de su poder relativo en el sistema internacional (Boone Bartholomees Jr., y otros, 2006, pág. 8).

En la actualidad, un actor no estatal es un elemento de absoluta gravitación a la hora de analizar los conflictos actuales y futuros y su interrelación con el campo de la información. Un actor no estatal, es cualquier participante que puede actuar en el sistema internacional con capacidad para desafiar la influencia de las unidades políticas estatales. Aquí entran las organizaciones internacionales y regionales, las corporaciones multinacionales, las ONG (Boone Bartholomees Jr., y otros, 2006, pág. 3 a 5) y también, porque no, los individuos que se manifiestan en las redes sociales y ejercen un poder anónimo sobre los estados, los dirigentes y sus componentes.

La política internacional maneja conceptos de asimetría materializados en capacidades de acción y proyecciones diferentes de cada uno de los actores. En ese contexto, Putnam sostiene que los tomadores de decisiones deben pensar en una lógica de dos niveles, es decir, en una visión de coaliciones de poder domésticas que ejercen presión sobre los decisores y otra que efectúa una visión internacional para maximizar ganancias (Putnam, 1996).

La viabilidad nacional de la política está dada entonces, por los márgenes de maniobra obtenidos. El análisis del "juego de doble nivel" presentado por Putnam (1996, pág. 79) permite comprender que, en muchas negociaciones internacionales, diferentes grupos que persiguen sus propios intereses presionan al gobierno para que adopte políticas favorables a ellos. Los gobiernos nacionales buscan entonces, maximizar su propia capacidad en los escenarios internacionales, para satisfacer las presiones internas, minimizando al mismo tiempo las consecuencias adversas de los acontecimientos del contexto internacional. De esta forma, al enfrentar oportunidades y dilemas estratégicos característicos de los estados, buscan reconciliar a un tiempo las exigencias nacionales y las internacionales poniendo de relieve "la inevitabilidad del enfrentamiento interno" acerca de lo que requiere el «interés nacional» (Putnam, 1996, pág. 118 y 119).

Los intereses relacionados con la seguridad estarán definidos por actores que responden a factores culturales que pueden ser diferentes, lo que no significa que las capacidades materiales estatales no sean importantes para el análisis de los asuntos de seguridad internacional. Los estados seguramente buscarán el poder material, pero los "significados" que asignan al poder y a la seguridad ayudarán a explicar su comportamiento (Katzenstein, 1996, pág. 2).

La cultura refleja normas, valores, reglas y modelos que definen, qué actores sociales existen en un sistema, cómo operan y cómo se relacionan entre ellos (Kat-

zenstein, 1996, pág. 6 y 7). El estado, como actor social, está incorporado a reglas sociales y convenciones que constituyen su identidad. El contexto cultural y social y el ambiente doméstico e internacional son "determinantes sociales" que dan forma a las entidades estatales y exhiben una gran centralidad a la hora de tratar de entender la política de un actor estatal (Katzenstein, 1996, pág. 19 a 22).

La DPDN 2021 de nuestro país, da cuenta de todos estos mismos fenómenos e interacciones, al expresar que las tensiones y conflictos interestatales militares si bien vuelven a ubicarse en el centro del escenario (República Argentina Ministerio de la Defensa, 2021, pág. 3), existe un "mayor grado de dispersión del poder, una multiplicidad de actores involucrados y una diversidad de dinámicas en juego, lo que redunda en un escenario cambiante cuya evolución resulta difícil de prever".. (2021, pág. 7).

Como se viene observando y, a modo de consideración final de esta sección, existen en la actualidad varios elementos que modelan la historia y los conflictos. Van desde lo que podría ser un menguante rol del estado y del sistema de seguridad internacional, la aparición de una multiplicidad de actores de diversa índole con agendas e intereses coincidentes o discrepantes que se despliegan en tiempos, espacios y dominios diferentes y un contexto cultural y social determinado donde las percepciones de las personas juegan un rol preponderante.

4. **La estrategia y el conflicto**

4.1 **Utilidad de la Estrategia y sus Niveles**

Es bien conocido que el concepto "estrategia" estaba inicialmente ligado al empleo de las fuerzas militares en un conflicto armado. Posteriormente, sufrió evoluciones, no ajenas a confusiones y generalizaciones diversas, tanto en el ámbito civil como el militar[6].

Pero en lo que interesa a este trabajo, la estrategia trata de fines, medios, riesgos y costos dentro de entornos conflictivos en tiempos y espacios cada vez menos precisos. Mientras que para Beaufre estrategia "es el arte de la dialéctica de las fuerzas, o aún más exactamente, el arte de la dialéctica de las voluntades que emplean la fuerza para resolver su conflicto" (Beaufre, 1963, pág. 13), para Bartlett, Holman, y Somes es la conexión entre fines y medios, un "plan de juego" que dice cómo los recursos serán empleados en función del contexto de seguridad internacional y de los medios disponibles (Bartlett, Holman, & and Somes, 1995, pág. 19).

La estrategia es una "función humana perdurable" que se manifiesta mientras las sociedades modernas, "tengan intereses y necesiten contrarrestar desafíos y alinear sus recursos para obtener sus propios objetivos". (Hoffman, 2020). Parte de la dificultad para hacer una buena estrategia deriva de la creciente incertidumbre y fricción en el que se desarrolla. Esto se debe a "su propia naturaleza, que perdura en el tiempo y en todos los contextos", a "la multiplicidad y gran variedad de fuentes de fricción" y porque se planifica "para contextos que literalmente no han ocurrido y

6 El término se ha generalizado tanto que se ha agregado una gran confusión conceptual.

podrían no ocurrir", porque "el futuro no ha sucedido" (Gray, Why Strategy is so Difficult, 1999, pág. 82).

Los escenarios adonde los conflictos pueden tener lugar son, además de complejos, únicos e irrepetibles y no permiten aplicar recetas estandarizadas. Entonces, se ratifica una y otra vez la sentencia de Clausewitz, respecto a la obligación suprema del hombre de estado y del comandante en jefe de apreciar correctamente la naturaleza del conflicto en que se embarca (Murray, Knox, & Bernstein, 1994, pág. 392).

Los medios a generar y diseñar en una estrategia deberían ser afines al carácter del conflicto planteado, sean estos escenarios anticipados de corto plazo o aquellos más abstractos de mediano o largo plazo. Michael Howard advierte en este asunto, sobre la necesidad de que la estrategia no cometa errores garrafales en la apreciación del conflicto futuro respecto de los medios para enfrentarlos:

> No importa cuán claro uno piense, porque es imposible anticipar precisamente el carácter del conflicto futuro. La clave está en no caer tan lejos de la marca de manera que sea imposible ajustarse una vez que el carácter del conflicto sea revelado (United Kingdom MoD, 2015, pág. 2).

La estrategia también puede ser vista como un modo de pensar (Corbacho, 2011, pág. 4), siendo la que permite pasar las ideas a la acción, a través de tres niveles: la concepción, el diseño y la elección (Frischknecht, Lanzarini, Alonso, Moya Latrubesse, & Hernandez Otaño, 1995, pág. 2). Los niveles estratégicos se concibieron en función de la categoría fines-medios y cada uno de ellos, tiene responsabilidades específicas y actividades que crean efectos deseados y contribuyen al logro de los objetivos establecidos.

El nivel de la Estrategia General y el Militar son niveles de Dirección, es decir, donde se toman las decisiones, mientras que el Operacional es de planeamiento y ejecución (de Vergara, 2012, pág. 72).

Pero esta división no debería hacernos pensar que es taxativa y rigurosa. Por el contrario, los niveles se confunden y solapan y esto es aún más válido en las actuales circunstancias, adonde "la naturaleza omnipresente de la información y de la tecnología, transforman a cada soldado y piloto en un nodo de un medio de fuerzas centradas en red" y ello "está cambiando inevitablemente los modelos de liderazgo de las fuerzas armadas" (Rosenberg B. , 2007).

En su reciente doctrina, el Cuerpo de Marines de EEUU sostiene que la "naturaleza instantánea, global y persistente de la información comprime los niveles de guerra y aumenta las posibilidades de que una acción local tenga un impacto global" porque "permite a las personas monitorear continuamente los eventos locales en una escala mundial" (United States Marine Corps, MCDP8, 2022, pág. 18).

El diseño de una estrategia de nivel general permite articular los diferentes niveles y componentes del poder nacional, antes, durante y después de un conflicto. De esta forma, puede atender los problemas de la defensa nacional en un ciclo continuo e intemporal. Antes del conflicto, formulando supuestos, equilibrando medios, modos

y fines y calculando costos y riesgos. Luego, en la realización de un ajuste constante de fines con medios y en la reevaluación permanente de costos y riesgos. Finalmente, en el uso que se da los resultados obtenidos (de Vergara, 2012, pág. 20).

La elaboración e implementación de una estrategia constituye, en gran parte, un ejercicio de gestión y reducción de riesgos. La diferencia entre las amenazas que un adversario puede plantear y las capacidades y medios disponibles, determinan los riesgos de un estado nacional (Drew & Snow, 2006, pág. XI).

4.2 **Los medios y la importancia de la voluntad y el componente moral.**

En el nivel nacional, los medios se pueden categorizar de diferentes maneras. Una de ellas, es la tradicional basada en los componentes del poder nacional: diplomático, de informaciones, militar y económico (DIME) empleada por los profesionales de la seguridad en los EEUU (Boone Bartholomees Jr., y otros, 2006, pág. 9).

La doctrina conjunta argentina, por su parte, reconoce como factores de poder básicos al psicosocial, político, económico, diplomático, militar, científico y tecnológico (República Argentina EMCO, PC 00-02, 2015, pág. 98) a lo que se podría agregar hoy el de las informaciones.

Otra forma, es la que incluye, además de los nombrados instrumentos DIME, al factor cultural, la unidad nacional y la inteligencia estratégica (Boone Bartholomees Jr., y otros, 2006, pág. 9). Y una cuarta manera de clasificar los medios disponibles por un estado para hacer estrategia, es la que apela a la división entre poder "duro" y "poder blando" tratados por separado o, en forma sinérgica como poder "inteligente". El poder duro se refiere a la influencia que emana de los medios militares y económicos que son fuentes de disuasión y de empleo efectivo. El poder blando, mientras tanto, trata de los medios indirectos, como la diplomacia, la cultura y la historia (Boone Bartholomees Jr., y otros, 2006, pág. 9). Describe el uso de la atracción positiva y la persuasión para lograr objetivos de política exterior, buscando lograr influencia mediante la construcción de redes, la comunicación de narrativas convincentes, el establecimiento de reglas internacionales y el aprovechamiento de los recursos que hacen que un país sea naturalmente atractivo para el mundo[7].

Pero independientemente de las herramientas del poder que se utilicen en el nivel estado, la habilidad de un actor para transformar el "poder potencial" en "poder operacional", necesita para llevar adelante sus objetivos y como consideración más importante, ser iluminada por la "voluntad política" (Boone Bartholomees Jr., y otros, 2006, pág. 9).

Los medios nunca se pueden disociar de los fines perseguidos, sino que dependen de ellos y viceversa. Caso contrario, la estrategia es un mero ejercicio fútil y sin sentido. La libertad de acción de un actor le otorga poder y estará dada por los medios que disponga, pero también dependerá, en gran medida, de su motivación, determi-

7 El poder blando evita las herramientas tradicionales de la política exterior del palo y la zanahoria. (USC Center on Public Diplomacy, 2022).

nación y fuerza moral. Estos aspectos son claves a la hora de la toma de decisiones en un conflicto o guerra y parecen haber cobrado en la actualidad, una especial gravitación por la incidencia que poseen las percepciones en su conformación.

La referencia a la incidencia del componente moral y la fuerza de voluntad de las tropas y pueblos en un conflicto, ha sido tratada por cientos de años. Baste recordar que la guerra es un fenómeno político que constituye "un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad" (Clausewitz, 1992, pág. Capít I). O que el poder "se pone de manifiesto como producto de dos factores indisolubles: la magnitud de los medios con que el oponente cuenta y la fuerza de su voluntad" (Clausewitz, 1992). O bien cuando Clausewitz refiere a que si tomamos los cuatro componentes "del ambiente en que se desarrolla la guerra, el peligro, el esfuerzo físico, la incertidumbre y el azar, fácil será comprender que se requiere una gran fuerza moral y mental" (Clausewitz, 1992).

Del mismo modo, Colin Gray dice que el componente "moral" es un elemento clave en una sociedad y sus dirigentes, para llevar adelante un esfuerzo de guerra (Gray, Out of the Wilderness: Prime time for Strategic Culture, 2009, pág. 231). Y sobre el mismo tema Finney dice que:

> T. R. Fehrenbach lo expresó mejor cuando escribió: "Un pueblo que no se prepare para pelear debería moralmente prepararse para rendirse. Fallar en preparar a los soldados y ciudadanos para una acción terrestre limitada y sangrienta, y luego participar en ella, es una locura que raya en lo criminal. Así como existe un estándar moral y ético para ir a la guerra, y un estándar de conducta mientras se libra una guerra, existe la responsabilidad moral de preparar y equipar adecuadamente a los hombres y mujeres que lucharán en una guerra (Finney , 2020, pág. 104)

Sun Tzu refiere a cinco factores fundamentales para la guerra entre los cuales incluye a la influencia moral[8] (Finney , 2020, pág. 18) y su célebre máxima "conoce a tu enemigo y conócete a ti mismo…", nos orienta a las diferentes formas de pensar, decidir y guerrear de cada actor estratégico, pero también, a la fuerza de voluntad para llevar adelante el esfuerzo de guerra (Lantis, 2009, pág. 33).

Según la OTAN, el poder de combate de una fuerza posee tres componentes[9]. Uno de ellos es el moral que incluye a la "motivación, cohesión moral y fundación ética" de las tropas (Malan, 2018, pág. 38).

La doctrina conjunta argentina, por su parte, incluye a la moral como principio de la guerra (EMCO, PC 00-01 (proyecto), 2018, pág. 97) y, al referirse al conductor, dice que "los principios éticos y morales son inmutables, sea cual fuere el tipo de conflicto

8 Los otros son el clima, el terreno, el comando y la doctrina. Ver Finney, N. (2020). On Strategy: A Primer. Fort Leavenworth, Kansas, EEUU: Combat Studies Institute Press U.S. Army. pp. 18.

9 Según la OTAN son el conceptual, el físico y el moral.

o adversidades que el hombre de armas deba enfrentar" (EMCO, PC 00-01 (proyecto), 2018, pág. 53).

Del mismo modo, la doctrina del Ejército Argentino asigna un lugar superlativo a la motivación y la moral individual y colectiva de las tropas (República Argentina Ejército Argentino, MFP 51-13, 1968, pág. 56 y 97) y expresa, en lo referido a este trabajo, que la motivación de un grupo podrá ser afectada por causas externas como la información, la acción sicológica y los rumores, que podrán alterar el estado sicológico y su comportamiento (1968, pág. 16).

Algunos autores de la historia militar han sugerido que Napoleón confiaba mayormente en la cantidad y volumen de sus tropas; sin embargo, el componente motivacional fue fundamental en su visión del conflicto. La popularidad de la lucha sostenida por los "nuevos" soldados ciudadanos franceses, fue crucial para el éxito en las batallas a través de toda Europa y el fracaso de los ejércitos napoleónicos en España ratificó que la voluntad del pueblo y la guerrilla que siguió, fueron componentes determinantes en el éxito español (Smith, 2007, pág. 34 y 42).

En el nivel estratégico, "las partes interesadas son demasiado variadas, las demandas en conflicto o competencia demasiado duraderas y el proceso demasiado complicado para que sea razonable esperar una coherencia conceptual perfecta" (Finney , 2020, pág. 123).

Las nuevas relaciones y tensiones de poder entre estados poderosos, el debilitamiento de las soberanías estatales y los cambios tecnológico-informativos impactan en el ámbito social, psicológico y organizacional e influencian en las agendas domésticas, regionales y mundiales.

A partir de la revolución digital iniciada a principios de los ochenta, una dinámica novedosa viene incidiendo en la conformación de los conflictos y la voluntad, el componente moral y la capacidad de percepción de las audiencias, juegan un papel preponderante en la toma de decisiones.

5. **Estrategia, influencia y cibernética**

5.1. **Estrategia y comunicación**

La comunicación constituye un factor imprescindible para el logro de los objetivos de un grupo social y representa un medio para transmitir información vital (Sanchez de Gallardo & Nava Romero, 2007, pág. 72).

Su propósito es vincular, establecer «puentes» entre las personas o grupos humanos pero, en un sentido más profundo, es disponer de información para actuar en los procesos de cambio o facilitarlos, esto es, "influir en la acción para lograr los objetivos de la organización de que se trate" (Koontz, Weihrich , & Cannice, 2012, pág. 456).

La estrategia es ante todo comunicación con un propósito, que no es otro que el de ejercer *una influencia* afín a los intereses del que la emite. De ahí la importancia que posee para este trabajo.

La comunicación estratégica se produce con cualquier medio. "Interacción, ya lo decía Max Weber, es siempre acción que comunica un significado". "No hay influencia

sin comunicación porque no hay otro modo de acceder a las mentes de los demás, única manera de cambiar sus intereses. Toda interacción social puede reducirse a una forma de comunicación, desde la religión hasta la guerra" (Frischknecht, Lanzarini, Alonso, Moya Latrubesse, & Hernandez Otaño, 1995, pág. 20).

5.2 **Cibernética e influencia**

Según la RAE el término cibernética tiene varias acepciones, de las cuales se resaltan dos. La que la define como lo "perteneciente o relativo a la realidad virtual" y la "ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas". En cuanto a "influencia" la misma academia refiere a la "acción y efecto de influir, entendiendo por ello al "ejercicio de predominio, o fuerza moral" sobre una cosa o persona y, a la obtención de "...una ventaja, favor o beneficio" (Real Academia Española, 2022).

Se podría decir que la cibernética es vehículo de la influencia; y que esta última es un elemento dinámico, lejano de la relación subordinado-superior y asociado a su carácter multidireccional, características que se ven promovidas en la actualidad por el ciberdominio.

En síntesis, la cibernética es vehículo de la influencia. Según Moresi, hoy presenciamos una nueva revolución tecnológica que ha cambiado la forma de la comunicación, "donde la robótica, la inteligencia artificial y la computación cuántica prometen un nuevo paraíso" y el "ciberespacio es un nuevo ambiente virtual que se concibe a partir de la interconectividad de sistemas informáticos" (Moresi A. , 2021, pág. 7).

En la misma línea Nievas sostiene que la:

> ...revolución espacial se desarrolló de manera concomitante y solidaria con una revolución tecnológica, que, en definitiva, conformó el sustrato material para el desarrollo de la cuarta gran revolución espacial. Sin satélites no habría Internet, ni sistemas de posicionamiento global, ni telefonía celular, entre otras cosas (Nievas, 2021, pág. 410).

Los avances tecnológicos en el campo de la informática y el uso intensivo de las redes sociales son herramientas que actúan "sobre el ámbito cognitivo, o lo que es lo mismo, sobre la capacidad de percepción de las personas, sobre la que, a su vez, se asienta su capacidad para tomar partido por una u otra opción y adoptar decisiones. De ahí su extraordinaria importancia, dado que el uso de la información o desinformación se puede convertir en un arma de guerra potencialmente decisiva en los conflictos actuales" (España Ministerio de Defensa, 201, 2019, pág. 14).

En la llamada era posmoderna, los hechos y las verdades son cuestionados en forma sistemática y de ahí la importancia estratégica que adquieren las percepciones a partir del valor asignado a los mensajes y la narrativa, sea para justificar y legitimar motivos y acciones de una de las partes o aún, para desacreditar y socavar las de los adversarios.

Betz y Stevens dicen que la información digital y la infraestructura de comunicaciones están presentes en cada faceta de una sociedad moderna (Betz & Stevens, 2011, pág. 36). Del mismo modo, de Vergara y Trama sostienen que en el ciberespacio, interactúan un sinnúmero de participantes con capacidad de influirse mutuamente a través de la comunicación y que es un vasto dominio, una red interdependiente de tecnología de la información (redes de telecomunicaciones, sistemas de computación y procesadores y controladores) dedicada a tareas de procesamiento en tiempo real (de Vergara, 2017, pág. 434).

Como venimos viendo, el ciberespacio (derivado de la cibernética) ha efectuado un largo recorrido desde su nacimiento al inicio de los 80. En términos generales se puede decir que posee tres atributos y efectos que afectan los conflictos y estrategias de respuesta:

> Oculta la identidad y ubicación de los actores a través de una infraestructura física y protocolos de software de fácil uso y sin claves de identificación,
> Incrementa radicalmente la velocidad, volumen y alcance de las comunicaciones de todos –desde los estados más poderosos y corporaciones hasta los individuos- que pueden comunicarse en el nivel global en forma casi instantánea y con razonable seguridad y,
> Sus barreras de entrada son cada día más baratas y accesibles (Betz & Stevens, 2011, pág. 10).

Sólo en tres décadas el ciberespacio ha sido definido en la doctrina militar como un nuevo dominio del conflicto, mientras que "en términos sociales más amplios ha llegado a ser visto como el sustrato informativo en el que crecen industrias y ecosistemas económicos completos. En estados desarrollados toca la mayoría de los aspectos de la vida de los ciudadanos, desde la forma en que ganan dinero y son gobernados, hasta cómo construyen y mantienen relaciones sociales y encuentran sustento espiritual e intelectual". (2011, pág. 10).

Byung-Chul Han[10] dice que el acortamiento de las distancias entre los seres humanos subsume e intercambia los roles de emisores y receptores de información en una combinación interminable y no distinguible. Todos producen y consumen datos al mismo tiempo. Los medios de comunicación tradicionales influyen, pero quedan en un rol secundario. Las redes sociales no tienen dueño y allí fluye información de todo tipo (verdadera o falsa) en forma permanente que ejerce influencia.

> Somos programados de nuevo a través de este medio reciente, sin que captemos por entero el cambio radical de paradigma. Cojeamos tras el medio digital, que, por debajo de la decisión consciente, cambia decisivamente nuestra conducta, nuestra percepción, nuestra sensación, nuestro pensamiento, nuestra convivencia.

10 Filósofo y ensayista surcoreano experto en estudios culturales y profesor de la Universidad de las Artes de Berlín.

> Nos embriagamos hoy con el medio digital, sin que podamos valorar por completo las consecuencias de esta embriaguez. (Han B.-C. , El enjambre, 2013, pág. 11)

El autor surcoreano agrega que hoy, en el ciberespacio, "se realiza otro cambio de paradigma" y, entonces, introduce la dimensión del "panóptico[11]" digital que tiene la posibilidad "de sacar modelos de conducta de las masas a partir de grandes datos" y que ello "marca el comienzo de la psicopolítica digital". (2013, pág. 106).

5.3. **Operaciones militares y ciberespacio**

En un artículo de 2021, Nievas sostiene que hubo en la historia cuatro revoluciones "espaciales" que afectaron al derecho, las unidades políticas y la guerra (Nievas, 2021, pág. 395).

Hasta entrado el siglo XX, "al igual que toda la actividad humana, la guerra había sido un fenómeno de expresión bidimensional, es decir terrestre y marítima (pág. 404). La irrupción, durante la Primera Guerra Mundial, de la aviación y el submarinismo "hizo que la especie humana, que había vivido en dos dimensiones, es decir al ras de la tierra o del agua, comenzara a desplazarse volumétricamente" (pág. 406).

El mismo autor señala que la cuarta revolución espacial, es decir, la que considera que el espacio se hizo tetradimensional a partir del desarrollo del ciberespacio está teniendo un impacto mucho mayor en la actividad bélica, el estado y sus formas jurídicas (pág. 408).

Las nuevas tecnologías basadas en la información tienen la capacidad de degradar, denegar, afectar, manipular o destruir a un adversario en cualquier momento con una dimensión cierta, factible y concreta. Consecuentemente, la seguridad internacional y estatal pueden verse menguadas y es posible que surjan conflictos de diferente carácter en cualquier momento y circunstancia.

La globalización cibernética puede reforzar o agravar, en términos de intensidad y alcance, las amenazas que enfrente un estado. En estos contextos dinámicos y difusos puede percibirse que el estado de conflicto es permanente, se dificulte la posibilidad de identificar el origen de la agresión y, consecuentemente, se requiera una respuesta integrada.

El ciberespacio es un nuevo dominio que atraviesa de los demás[12]. Las operaciones cibernéticas suponen el empleo de las capacidades disponibles en el ciberespacio con el propósito primario de obtener objetivos dentro o través de éste (United States Joint Chiefs of Staff, JP 2-12, 2018, pág. vii). Emplearán un modelo de tres capas interrelacionadas para ayudar a su planificación y ejecución, es decir, una red física, una red lógica y lo que la doctrina estadounidense llama "ciber persona" (cognitiva o quizás virtual) (2018, pág. viii).

---

11 Un panóptico es una construcción cuyo diseño hace que se pueda observar la totalidad de su superficie interior desde un único punto y que, por lo tanto, facilita el control de quienes se hallan dentro del edificio.

12 Aéreo, terrestre, marítimo y espacial.

Respecto del uso efectivo de la información en el campo de batalla, el General Glavy[13] de los EEUU declaró recientemente, que "aquellos que tarden en captar los mensajes y ver cuán importante es su narrativa... tendrán problemas" (Seck, 2022).

En esa línea Trama y de Vergara señalan que, desde la era industrial, la difusión de las tecnologías de información tendieron a cambiar algunos parámetros operacionales "y no siempre en beneficio de quien las posee" (Trama & de Vergara, 2017, pág. 258):

> Eso ha afectado especialmente la forma de hacer la guerra y dio paso a la denominada guerra híbrida. La infraestructura del espacio cibernético fue desarrollada, pero ahora está abierta y disponible para cualquiera que tenga los medios para acceder a él. ...el uso del espacio cibernético puede causar efectos en los niveles táctico, operacional y estratégico, cuando ataca a sistemas de comando y control, no solamente militares sino de instalaciones civiles como usinas eléctricas o cualquier otra fuente de poder hidroeléctrico o nuclear o se pretende alterar los datos de una elección en el nivel nacional (2017, pág. 258).

La Directiva Política de Defensa Nacional de 2014 señalaba que:

> La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la "guerra real" y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también al ciberespacial. (República Argentina Ministerio de Defensa, 2014, pág. 6)

Y la de 2021 establece entre los lineamientos de nivel estratégico nacional que el Estado Mayor Conjunto de las Fuerzas Armadas debe actualizar la doctrina de nivel operacional y "delinear una estrategia militar" que favorezca una estrategia disuasiva, priorizando las acciones de guerra cibernética, información, energía dirigida y vehículos no tripulados (para su empleo en diferente tipo de operaciones)" (República Argentina Ministerio de la Defensa, 2021).

Por otra parte, la doctrina básica del Ejército Argentino refiere que la velocidad de propagación de todo tipo de información influencia en los líderes políticos, conductores militares y en los grupos o individuos integrantes de la sociedad, afectando en forma positiva o negativa la imagen y legitimidad de las propias fuerzas o las del enemigo en un área de operaciones (República Argentina Ejército Argentino, ROB 00-01, 2015, págs. I-10).

---

13 2do Comandante del área de Información del Cuerpo de Marines de EEUU.

6. **Viejos y nuevos abordajes de los conflictos**

Varios autores coinciden que, en el siglo XXI, el carácter de los conflictos y las guerras ha cambiado una vez más, en una validación repetitiva de la expresión de Clausewitz en cuanto a que ellos son como un camaleón que cambian de carácter (Clausewitz, 1992, págs. Libro primero, capit I), según sea su naturaleza, propósito, la manera en que se los conducen, la tecnología y el ambiente operacional donde tienen lugar (de Vergara, 2017, pág. 58).

Al referirse a estos cambios, de Vergara expresa que la seguridad de una nación y su defensa se han vuelto multidimensionales (de Vergara, 2017, pág. 49) y, Calderón Concha sostiene que los problemas, peligros y oportunidades derivados de la violencia en general y de la guerra en particular son actualmente de gran complejidad y, por ello, las respuestas deben ser igualmente complejas y multidimensionales (Calderón Concha, 2009, pág. 16).

Del mismo modo, Moresi dice que en la actualidad se han agregado dominios y dimensiones al conflicto humano, de la mano de la tecnología, de tácticas, de ideas o de formas de implementación (2021, pág. 2).

Como ya se ha mencionado, la matriz bélica también ha cambiado:

> Ya casi no existen conflictos que enfrenten a fuerzas estatales. Lo corriente, desde el inicio del siglo –aunque de manera creciente desde mediados del siglo pasado– es el enfrentamiento de fuerzas estatales con fuerzas paraestatales. Estas nuevas formas han derivado en lo que hoy algunos autores denominan guerras híbridas, una suerte de composición entre la acción psicológica, la política y la fuerza. Para la acción psicológica y la política, el uso de las redes sociales es fundamental tanto por su extensión como por la desactivación de toda vigilancia epistemológica sobre el contenido de lo que allí aparece. Este tipo de conflicto se observó tanto en la llamada primavera árabe, como actualmente en Ucrania y Venezuela (Nievas, 2021, pág. 415).

Y continúa:

> Como ya dijimos, en la guerra actual se difumina la distinción entre combatiente y no combatiente, pero también entre guerra y paz, tal como se observa en la llamada guerra al terrorismo; asimismo, hay una marcada tendencia a la indistinción entre fuerzas militares y fuerzas policiales, lo que indica que la segmentación de la violencia legítima (externa, como defensa de la unidad política, e interna, como defensa del orden político), una característica propia de los Estados nacionales, también se desvanece (pág. 416).

Según la ONU, luego del Fin de la Guerra Fría, un "nuevo tipo de conflictos intraestatales" surgió; en los que actúan "no sólo ejércitos regulares sino también milicias

y civiles armados con escasa disciplina y estructuras de mando mal definidas",... con frentes de combate indefinidos" y donde los "civiles son las principales víctimas y, con frecuencia, los principales objetivos". Las autoridades "no tienen capacidad para hacerles frente debido a la "desarticulación de las instituciones estatales, especialmente de la policía y el poder judicial, con la consiguiente paralización de la capacidad de gobernar, el desmoronamiento de la ley y el orden público y la aparición del bandolerismo y de un caos generalizado". Estas situaciones "prácticamente no ocurren en las guerras entre Estados" (United Nations SG, 1995, pág. 5).

Del mismo modo, pero en una oportunidad más reciente (2018), la Doctrina para el Empleo de las Fuerzas Armadas (FAS) del Reino de España, ha observado un predominio de los conflictos armados de carácter intra estatal, con la presencia de grupos o fuerzas de variado origen y motivación que emplean con frecuencia métodos de todo tipo, incluyendo al terrorismo y otros no convencionales lo que ha dado lugar a diferentes manifestaciones asimétricas. Según esta doctrina, hoy los contendientes, aun aquellos de escasa magnitud y relevancia podrían causar daños significativos debido a un acceso más fácil a tecnologías accesibles más modernas "con la irrupción cada vez mayor de situaciones que se mueven en una zona ambigua entre la normalidad y el conflicto" (España Jefe de Estado Mayor de la Defensa, PDC-01 (A), 2018, pág. 11).

Korybko por su parte sostiene que "la guerra híbrida es el caos administrado" (Korybko A. , 2015, pág. 52)" y que sus dos pilares son las Guerras No Convencionales y las Revoluciones de Colores (2015, pág. 46) llevadas a cabo dentro de la Dominación de Espectro Completo impulsada por los EEUU (Guerras Híbridas, 2015, pág. 62) .

Sin embargo, debe entenderse que respecto de los conflictos actuales y del concepto "guerra", conviven diferentes perspectivas. Ello ha dado lugar a estrategias y doctrinas nacionales de lo más diversas y que responden a culturas estratégicas propias. Snyder, sugería que las "élites articulan una cultura estratégica única relacionada con los asuntos de seguridad y militares que son una manifestación más amplia de la opinión pública, socializada de un modo distintivo de pensamiento estratégico" (Lantis, 2009, pág. 35).

Figueroa y Taján dicen que la guerra "es un mismo fenómeno social considerado por múltiples abordajes" (Figueroa & Taján, 2018, pág. 95) y Frank Hoffman sostiene que persiste un amplio debate sobre la guerra, sus caracterizaciones y definiciones:

> Como debería de esperarse en cualquier intento de definir aspectos de algo tan complejo como la guerra, existe un amplio debate sobre las caracterizaciones y definiciones, como si una forma de guerra es más o menos compleja que cualquier otra, o si la guerra puede clasificarse tan claramente como para subdividirla a lo largo de un espectro en primer lugar. (Hoffman, 2015)

Mientras que algunos estados se han mantenido más apegados a visiones tradicionales y han evitado o minimizado cualquier flexibilización en la visión del conflicto y de

las guerras, otros flexibilizaron los conceptos y facilitaron la proliferación de perspectivas, doctrinas y abordajes diferentes.

El resultado en el primer caso fue una suerte de inmovilización doctrinario-conceptual y, en el caso de la seguridad internacional, su remisión "a la forma de empleo del instrumento militar y a la guerra, siendo esta última una actividad de claro sesgo interestatal" (Bartolomé, 2017, pág. 46). En el segundo caso, "el carácter cambiante de los conflictos se atribuyó, básicamente, a la transformación del ambiente estratégico y las mutaciones en los patrones de los conflictos" (Jones & Cherif, 2003, pág. 1) y a "la necesidad de adaptación y transformación" (Farrell, Rynning, & Terriff, 2013).

A modo de síntesis, M. Klare[14], citado por Bartolomé, sostiene que la seguridad internacional de los últimos años ha discurrido en una "doble confirmación". Por un lado, en la "insoslayable vigencia de las guerras tradicionales y sus probabilidades de ocurrencia en el corto y mediano plazos, sobre todo de la mano de renovadas pujas geopolíticas clásicas motivadas por el acceso a, o el control de, recursos naturales estratégicos" (Bartolomé, 2017, pág. 49 y 50). Pero también, la validez de la existencia de criterios cualitativos en los conceptos guerra y conflicto que tipifican y caracterizan los ambientes operacionales y dan forma a diferentes estrategias y transformaciones de los medios del estado – incluyendo el militar- con un variado componente de flexibilización (2017, pág. 49 y 50).

En esta línea, Hoffman sostiene que otros términos "han entrado en el léxico de los analistas de seguridad nacional y defensa" con el objeto de describir a aquellos conflictos que no llegan a la guerra convencional y que no son ni contrainsurgencia ni operaciones de estabilización (Hoffman, 2015).

Si nos remitimos a 1991, van Creveld sostuvo que las guerras convencionales e interestatales habían casi fenecido para dar lugar a la preeminencia de guerras de baja intensidad. La "guerra convencional puede que esté dando sus últimas boqueadas" y en "la medida en que los conflictos de baja intensidad se tornen predominantes mucho de lo que ha pasado por estrategia durante los últimos dos siglos se tornará inútil" (Van Creveld, 1991, pág. 277).

En el mismo sentido, el general Rupert Smith reconocía en su obra "un cambio de paradigma en la guerra" de la "guerra industrial" hacia la "guerra entre la gente". Los campos de batalla de fuerzas militares con poderes de combate relativos comparables, pasaron a una "confrontación estratégica entre una gama de combatientes, de los cuales no todos son ejércitos", que usan diferentes tipos de armas, "a menudo improvisadas" (Smith, 2007, pág. 5).

Kaldor escribe que, durante las últimas décadas del siglo XX, se desarrolló un nuevo tipo de violencia organizada, especialmente en África y Europa del Este, que es un aspecto de la actual era globalizada. La «nueva guerra», según Kaldor, difiere de la

14 Ver Klare, M. (2001). Resource Wars: The New Landscape of Global Conflict. Nueva York. Henry Holt/ Metropolitan; Klare, M. (2003). Guerra por los recursos. El futuro escenario del conflicto global. Madrid: Urano Tendencias; Klare, M. (19 de marzo de 2006). Se avecinan guerras por los recursos. La Jornada. Recuperado de http://firgoa.usc.es/drupal/node/27135

anterior («vieja guerra») como también de la llamada Revolución en Asuntos Militares (RAM) que no es más que el "estado del arte" de las viejas guerras. Esa autora agrega que, el modelo de violencia organizada que captura nuestra forma actual es la guerra en Bosnia-Herzegovina (1992-1995) y agrega que las nuevas guerras tienen medios de financiación, fuerzas privatizadas y patrones de violencia particulares. (Nickels, 2009, pág. 1 y 2).

Qiao Liang y Wang Xiangsui explican que el campo de batalla de la guerra más allá de los límites difiere de los del pasado, en que abarca todos los espacios naturales, como el ámbito social, y el ámbito de la tecnología en continuo desarrollo.

> Hoy, estos espacios están entrelazados entre sí. Por ejemplo, el espacio exterior puede verse como un espacio natural, y también como un espacio tecnológico, porque cada paso en la militarización del espacio exterior requiere un avance tecnológico. De la misma manera, las dinámicas internas entre sociedad y tecnología se deben ver constantemente. No hay un ejemplo más típico de esto que el efecto de la tecnología de la información en la sociedad. De estas cosas podemos ver que el campo de batalla está en todos lados, y solo podemos verlo con omnidirección (Qiao Liang & Xiangsui, 2021, pág. 302).

En este punto se podrían efectuar dos observaciones. La primera es que en el siglo XX y lo que va del XXI, han surgido categorizaciones y teorías diferentes de las guerras y los conflictos, "muchas de ellas no suficientemente consolidadas doctrinariamente" (Figueroa & Taján, 2018, pág. 95).

Y la segunda es que el necesario y loable trabajo efectuado por diferentes académicos y estudiosos de los temas de la guerra y los conflictos, no debería hacernos perder de vista que las heterogéneas interpretaciones y teorías de la guerra son sólo eso, y que, en muchos casos, revisitan temas pasados con otras ópticas o perspectivas. Muchos temas, en apariencia novedosos, no lo son realmente. De ahí la importancia de un estudio y formación amplia del profesional militar en el desarrollo del pensamiento crítico y de las habilidades como conductor a través de la lectura permanente y continua (Motta, 2020, pág. 65).

Entre los escritos académicos más salientes que han despertado el interés de los especialistas, se pueden mencionar los siguientes: Las Guerras de 4ta Generación (Lind y otros - 1989), la Transformación de la Guerra (Martin van Creveld – 1989), las Perspectivas de la Guerra Civil (Enzensberger – 1993), La Ciberguerra está arribando (Arquilla y Ronfeldt - 1993), Las Nuevas y Viejas Guerras (Kaldor -2007), la Guerra Compuesta (Huber – 1996), la Guerra Centrada en Red, la Guerra más allá de límites (Qiao Liang y Wang Xiangsui – 1999), las Guerras Híbridas (Frank Hoffman y James Mattis – 2005), las Guerras híbridas - Revoluciones de Colores y Guerra No convencional (Andrew Korybko – 2019), la Guerra de Información – Operaciones de Información[15] (Vertuli y Loudon -

15 Uno de los textos más conocidos en el ambiente es "Percepciones son Realidad"

2018), Ciberseguridad y Ciberguerra (Singer y Friedman – 2014), Las Nuevas Reglas de la Guerra (Sean Mc Fate - 2019), la "maskirovka" y la doctrina Gerasimov (2013) y, los "conflictos en la zona gris" (Jordán , 2022).

Genéricamente, el planeamiento estratégico militar de un estado responde, tanto a las contingencias que se pueden enfrentar en el corto plazo, como también al diseño de la estructura de fuerzas proyectadas en el futuro. Podrá ser una guerra convencional entre estados, una guerra nuclear, o incluso responder, a diferentes designaciones de conflictos de variada intensidad como por ejemplo de baja intensidad, conflictos no convencionales, híbridos, de información, contra–insurgencia, de estabilización, etc.

En el cuadro siguiente se presentan algunas de los conceptos más comunes que se pueden encontrar sobre guerras y conflictos elaborados por los autores enunciados más arriba, independientemente de las posiciones estatales reconocidas y de sus doctrinas y perspectivas:

ILUSTRACIÓN 1 . **Conceptos más comunes que se pueden encontrar sobre guerras y conflictos provenientes de la academia mundial.**

Guerras y conflictos	Tipo
Conflicto armado en ambiente convencional/ regular Guerra convencional	Se caracteriza como una lucha violenta por la dominación entre estados o coaliciones de estados. Esta confrontación, típicamente involucra operaciones militares de fuerzas contra fuerzas, en las que los adversarios emplean una variedad de capacidades militares convencionales, en los diferentes ámbitos/ dominios: aéreo, terrestre, marítimo, espacial y ciberespacial. El objetivo puede ser convencer o coaccionar a los decisores políticos, forzando su voluntad al derrotar sus fuerzas armadas y/o destruir su capacidad para la prosecución del esfuerzo (EMCO, PC 00-01 (proyecto), 2018, pág. 26).
Conflicto armado en ambiente no convencional/ irregular[16]	Actividades realizadas para permitir que un movimiento de resistencia o insurgencia coaccione, interrumpa o derroque un gobierno u ocupe un poder operando a través de fuerzas encubiertas, auxiliares y guerrilleras en un área denegada. Las fuerzas emplean un amplio espectro de operaciones militares y paramilitares, normalmente de larga duración, generalmente conducidas organizadas, entrenadas, equipadas, apoyadas y dirigidas en diversos grados por un actor externo. Incluye la guerra de guerrillas, operaciones directas ofensivas, de baja visibilidad, clandestinas, así como las actividades indirectas de subversión, sabotaje y actividades de inteligencia (Figueroa & Taján, 2018, pág. 97). Se define como un enfrentamiento violento entre actores estatales y no estatales en procura de legitimidad e influencia sobre la población. Este tipo de conflicto armado favorece los enfoques indirectos y asimétricos, aun-que puede emplear toda la gama de capacidades militares y de otro tipo para erosionar el poder, influencia del adversario, y su voluntad (EMCO, PC 00-01 (proyecto), 2018, pág. 26).

Guerra Hibrida	Situación en la que un país recurre al uso abierto de la fuerza armada contra otro país o contra un actor no estatal, además de usar otros medios por ejemplo políticos, económicos y militares (NATO European Centre of Excellence, 2022).
Conflicto híbrido	Situación en la cual las partes se abstienen del uso abierto de la fuerza armada y actúan combinando la intimidación militar sin llegar a un ataque convencional y a la explotación de vulnerabilidades económicas, políticas, tecnológicas o diplomáticas (NATO European Centre of Excellence, 2022).
Guerra asimétrica - conflicto en ambientes asimétricos	Es una metodología adoptada cuando un bando no puede prevalecer si se adhiere a los estándares aceptados para la guerra de la época y, por lo tanto, busca cambiar las reglas para tener su oportunidad. El lado convencional (simétrico) siempre verá la desviación de las reglas como traicionera e ilegal o inmoral (o ambas) y condenará la desviación. En el período 1991-2001, gran parte de la violencia en los conflictos intra-estatales y estados fallidos (por ejemplo, Somalia, Sierra Leona y el Congo) fueron posiblemente asimétricos en naturaleza o intención. (Drew & Snow, 2006, pág. XVII). Refiere a cuando existe "cualquier disparidad significativa con respecto a la configuración militar o técnica de las fuerzas; el grado de cumplimiento de las convenciones legales internacionales; o el respectivo interés en una resolución exitosa del conflicto.(...) El propósito de la estrategia asimétrica es disuadir o interrumpir la intervención militar; derrotar la voluntad a través del desgaste; o coaccionar al oponente, su coalición de socios o aliados, para que retiren su apoyo a la fuerza militar" (Newman, 2000, pág. 92). Es la que enfrenta a un ejército profesional y permanente con un movimiento de resistencia o insurgencia en el que el poder militar relativo entre ambos es significativamente dispar. Los combatientes más débiles intentan usar la estrategia y la táctica para compensar las deficiencias en cantidad o calidad de los recursos (Figueroa & Taján, 2018, pág. 98).
Conflicto de baja intensidad	Lucha político-militar limitada con participación de actores estatales y no-estatales, para lograr una victoria política, social, económica o psicológica. Puede ser prolongada y abarca presiones diplomáticas, económicas y psicosociales a través del terrorismo y la insurrección. El conflicto de baja intensidad generalmente se limita a un área geográfica y se caracteriza por armamento y tácticas convencionales con acotado nivel de violencia (Figueroa & Taján, 2018, pág. 97).

CONTINÚA EN PAG 38

16 Como se ha visto previamente en este capítulo existen otras interpretaciones.

Guerras y conflictos	Tipo
de 4ta Generación	Considera que las ideas y la tecnología son los conductores de los cambios producidos en la guerra, desde la Paz de Westfalia hasta nuestros días. Sus características principales son: descentralización de las operaciones, participación de actores no estatales, respeto relativo por las leyes de la guerra, presencia de no combatientes en el área de operaciones, organizaciones armadas sin jerarquías definidas, y uso de tácticas uso premodernas, de insurgencia, terrorismo y guerrilla. Hay estudiosos detractores de esta conceptualización (Figueroa & Taján, 2018, pág. 99).
Conflicto en la zona gris	Espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política (blanco), del enfrentamiento armado directo y continuado (negro), empleando estrategias "multidimensionales –también conocidas como híbridas–, de implementación gradual y con objetivos a largo plazo" (Jordán , Conflicto en la zona gris y estrategias híbridas, 2022).
Guerra sin restricciones Guerra irrestricta o Guerra más allá de los límites[17]	Implica que en el contexto de este tipo de guerra "todos los medios estarán disponibles, la información será omnipresente y el campo de batalla estará en todas partes, pero también significa que todas las armas y tecnologías podrán superponerse a voluntad, que todas las fronteras trazadas entre los dos mundos, las operaciones de guerra y las operaciones de no-guerra, las de lo militar y lo no militar, quedarán absolutamente decimonónicas y ello implica, a su vez, que muchos de los principios que gobiernan actualmente el combate se verán alterados..." (Liang, 1999, pág. 78) Una traducción más fiel del concepto guerra más allá de los límites. Sus ideas rectoras son: análisis, planeamiento y ejecución en todos los niveles y con todos los recursos, conducción simultánea de todas las operaciones en todos los espacios, objetivos alcanzables, amplio rango de opciones, búsqueda del desbalance entre los medios propios y los del enemigo, economía de recursos, movilización en esferas militares y no militares, e información ininterrumpida sobre el avance de los procesos (Figueroa & Taján, 2018, pág. 99).

FUENTE: EL AUTOR

La doctrina de EE. UU. al referirse a las Operaciones Multidominio y los objetivos estratégicos sostiene que una Fuerza Conjunta debe derrotar a los adversarios y lograr objetivos estratégicos en competencia, conflicto armado y en el retorno a la competencia. Agrega que se expande:

17 Para los chinos Qiao Liang y Wang Xiangsui Guerra sin restricciones y guerra combinada más allá de los límites son sinónimos.

> ...el espacio competitivo a través del compromiso activo para contrarrestar la coerción, la guerra no convencional y la guerra de información dirigida contra los socios. Estas acciones disuaden simultáneamente la escalada, derrotan los intentos de los adversarios de ganar sin luchar y establecen las condiciones para una transición rápida al conflicto armado. En un conflicto armado, la Fuerza Conjunta vence la agresión al optimizar los efectos de múltiples dominios en espacios decisivos para penetrar los sistemas estratégicos y operacionales de negación de acceso y área del enemigo, desintegrar los componentes del sistema militar del enemigo y explotar la libertad de maniobra necesarios para alcanzar los objetivos estratégicos y operacionales que crean condiciones favorables para un resultado político. (United States Army, TP525-3-1, 2018, pág. VII)

7. **Las teorías estratégicas contemporáneas y las doctrinas nacionales**

Esta sección describe, luego de una breve introducción, algunas de las cinco teorías estratégicas contemporáneas y luego trata el ambiente estratégico reconocido por las doctrinas de empleo de fuerzas militares de Estados Unidos, Rusia, China y Reino Unido. Pero antes de comenzar, se insiste con una observación efectuada por Trama y de Vergara:

> En lo que respecta a la conceptualización relativa a la seguridad y a la defensa, no debe olvidarse que muchas de las cuestiones que se presentan como los nuevos retos del siglo XXI son perfectamente identificables en conflictos del pasado y que los conceptos en desarrollo pueden ser novedosos en su denominación, pero no lo son tanto en su fondo (Trama & de Vergara, 2017, pág. 172)

Hoy se habla en los EE. UU. de estrategias de compensación, defensa activa y operaciones multidominio y hace pocos años, se trataban la Revolución de Asuntos Militares (RAM), las operaciones basadas en efectos, el enfoque global de la seguridad y las operaciones de estabilización y contrainsurgencia. Lo cierto es que, los responsables de la elaboración de las estrategias militares se plantearon en el pasado, cuestiones muy similares y lo hicieron apoyándose tanto en "las lecciones aprendidas de conflictos anteriores como en la puesta en práctica de teorías que, en algunos casos, se remontan a más de 2.000 años de antigüedad" (de Vergara, 2017, pág. 173).

Por otra parte, se debería tener presente que mientras se escriben estas líneas, las tensiones y conflictos interestatales, como aquellos en los que intervienen actores poderosos, parecen que vuelven a tener una importante gravitación; incluso, otros autores, hablan del regreso de la guerra industrial[18] cuando se refieren a la Guerra de

18 Ver Ruiz Arévalo, Javier Mª en Global Strategy: Ucrania: el regreso de la guerra industrial. 24/06/2022. https://global-strategy.org/ucrania-el-regreso-de-la-guerra-industrial/

Ucrania actual. Pero también hay otros conflictos menos visibles pero muy presentes como aquellos que ocurren en Etiopía, Haití, Afganistán, el Medio Oriente, Yemen, Myanmar y en varios países del norte de África.

7.1. **Las teorías estratégicas contemporáneas**

En forma sintética, "existen dos visiones predominantes respecto de la visión de la guerra", la occidental de Clausewitz y la oriental de Sun Tzu (Trama & de Vergara, 2017, pág. 172).

El general prusiano buscaba entender el carácter esencial de la guerra en vez de dar recetas, en la idea que los conductores estén mejor preparados para formular soluciones a problemas singulares y únicos. Inicialmente, plantea que el principio fundamental de la guerra era la destrucción de las fuerzas enemigas (de Vergara, 2017, pág. 18). Tres citas lo ilustran de esta forma: "Repetimos, pues, nuestro aforismo: la guerra es un acto de fuerza y no existen límites en el empleo de ésta" (von Clausewitz, 2021, pág. 23), y "las fuerzas militares deben ser anuladas, esto es, puestas en tal estado que no puedan continuar la lucha" (2021, pág. 42) o bien "Conseguidos estos dos extremos, la guerra, esto es, la tensión hostil y la acción de medios hostiles, no puede creerse hayan cesado mientras la voluntad del enemigo no sea violentada, es decir, sometidos sus gobiernos y aliados a firmar la paz o subyugados los pueblos (2021, pág. 42). Sin embargo, en honor a la verdad debería aclararse que posteriormente, von Clausewitz se dio cuenta que la guerra "no siempre implicaba la completa destrucción del enemigo" (de Vergara, 2012, pág. 19). Por ello, el prusiano habla de la "doble modalidad de la guerra" que "consiste: en aquella cuyo fin es el abatimiento del contrario, sea que lo aniquilemos políticamente, o simplemente lo dejemos indefenso para obligarle a la deseada paz, y en aquella en que solo se pretende hacer algunas conquistas en las fronteras de su reino…" (von Clausewitz, 2021, pág. 13).

Por otra parte, Sun Tzu privilegia la importancia de la inteligencia y el engaño como medio para derrotar la mente del enemigo y saber que las relaciones entre las cosas son más importantes en la estrategia de guerra, …sojuzgar al enemigo sin combatir es el mérito máximo" (de Vergara, 2017, pág. 172).

Al referirse a las teorías estratégicas contemporáneas, Ryan W. Kork explica que se pueden condensar en cinco amplias categorías. Incluyen la "aniquilación, desgaste y agotamiento; el enfoque indirecto; estrategias de control; disuasión nuclear; y estrategias basadas en la teoría de sistemas" (Finney , 2020, pág. 67). De ellas se tratan solamente las de más interés para este trabajo.

La estrategia de aniquilamiento "pretende atacar directamente a las fuerzas armadas enemigas y destruirlas e imponer la voluntad…", términos que serían familiares para Clausewitz o Jomini y están asociados en muchas formas a la aproximación directa, en el sentido de focalizarse exclusivamente en la destrucción de las fuerzas enemigas en el terreno (Finney , 2020, pág. 67 a 69).

La de desgaste se asocia a la destrucción gradual de las fuerzas enemigas, que tuvieren la intención de participar en la batalla, maniobrar para establecer una posición más

favorable o amenazar algo que el adversario aprecia (Finney , 2020, pág. 68).

La estrategia de agotamiento se enfoca en la destrucción de los recursos y la voluntad de un adversario para continuar la lucha. Consecuentemente, busca desgastar la sociedad y la economía que son el apoyo de las fuerzas militares a través de la imposición de costos inaceptables en el tiempo (Finney , 2020, pág. 68).

Sun Tzu "conceptualiza" la teoría de la aproximación indirecta. Una estrategia de este tipo busca la dislocación de un adversario aplicando la fuerza contra sus debilidades, o adoptando un enfoque inesperado, con el propósito de desintegrar la resistencia a través del shock y la confusión. De esta manera, el objetivo es provocar el colapso de los medios militares y su voluntad política (Finney , 2020, pág. 69). Liddell Hart en su famosa obra[19] sostuvo a la estrategia de aproximación indirecta, la cual aseguraba la victoria con menos riesgos y costos para las fuerzas militares, porque lograría la dislocación del enemigo al sacarlo de una posición preparada y también lo afectaría sicológicamente (Finney , 2020, pág. 69 y 70).

El inglés fue un severo crítico de von Clausewitz, sosteniendo que su conceptualización sobre la estrategia, la política y los objetivos era errónea y que éste había restringido el significado de la «estrategia» "a la mera utilización de las batallas", con lo cual transmitía la idea de ésta era el "único medio para alcanzar el fin estratégico". La estrategia no se limita simplemente a intentar derrotar el poder militar enemigo, sino a actuar con inteligencia sobre objetivos limitados y una "estrategia perfecta sería aquella que consiguiese resolver el conflicto sin necesidad de combates serios" (Liddel Hart, 2019, pág. Capít 19).

Las estrategias de control son particularmente de interés para este trabajo de investigación. Se centran en la idea de dar forma a los eventos, "ya sea antes o durante las hostilidades declaradas, para permitir que un competidor ocupe una posición ventajosa o manipule las percepciones populares de los eventos en curso. Las teorías de control ocurren a lo largo de la "competencia continua" y, a menudo, "asumen formas diferentes de las concepciones tradicionales de la guerra, pero el resultado final sigue siendo lograr y continuar con los objetivos de la política a través de otros medios" (Finney , 2020, pág. 72).

La estrategia de "control reflexivo" es una derivación de la estrategia original de control. Su objetivo principal gira alrededor de controlar los resultados a través de la "manipulación de la información, o en el ámbito militar influir en la comprensión situacional de un adversario para dar forma a las acciones potenciales para favorecer sus intereses" (Finney , 2020, pág. 73). Según W. Kork, la llamada «Doctrina Gerasimov» posee elementos de esta estrategia de control (Finney , 2020, pág. 73).

En el mundo actual, este tipo de estrategias (de control) están "en uso activo por parte de grandes potencias" desde "variados antecedentes históricos y culturales con el objeto de "moldear el entorno para que se ajuste a los objetivos nacionales, tanto dentro como fuera del conflicto" (Finney , 2020, pág. 74).

---

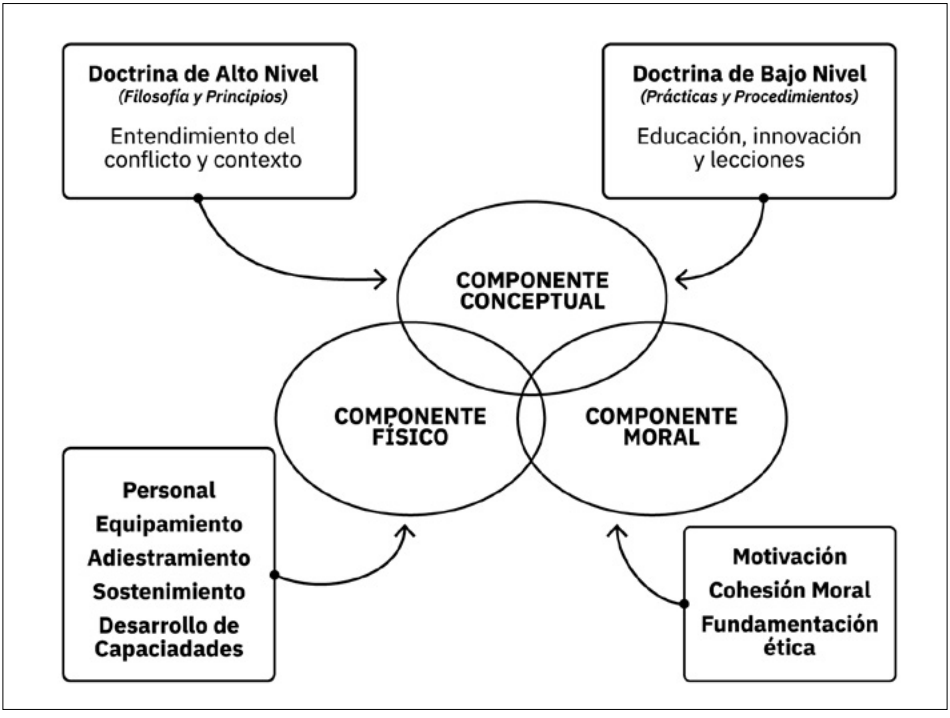
19 "Estrategia: la aproximación indirecta".

7.2. **Los ambientes estratégicos reconocidos por las doctrinas nacionales**

La doctrina conjunta trata de conceptos ordenados esenciales y principios aceptados por las fuerzas armadas de un país, que guían su preparación y empleo en el conflicto. Tiene una vinculación estrecha con el cumplimiento de su misión y es esencial para la formación de una base de pensamiento común en el ámbito de la acción militar conjunta y para el empleo de los medios militares.

Para la OTAN, la doctrina es un conjunto de: "(...) principios fundamentales por los cuales las fuerzas militares guían sus acciones en apoyo a los objetivos. Es mandatoria, pero requiere juicio en su aplicación" (NATO, AAP-06, 2019, p. 44). Es decir, que la doctrina debe ser conducente al logro de los objetivos que se definan para las fuerzas militares. Cuando es adecuada proporciona una "aproximación común y una forma de pensar que no está limitada, en el nivel conjunto, por reglas prescriptivas" (Motta, 2020).

ILUSTRACIÓN 2 . Componentes del Poder de Combate de una Fuerza Militar según la OTAN



FUENTE: (TOMADO DE MALAN, M. (2018). [20]

20 Action adapted to circumstance: Peacekeeping doctrine and the use of force. En P. Nardin, & otros, The use of force in Peacekeeping Operations. Nueva York, EEUU: Rouledge y NATO Standarization Agency, Allied Joint Doctrine AJP-0p1 (D) (Brussels, Belgium: NATO, 2017).

Para el Glosario de Términos de empleo militar para la Acción Militar Conjunta argentino (República Argentina EMCO, PC 00-02, 2015) la doctrina conjunta es un:

> Conjunto ordenado de conceptos esenciales, principios y conocimientos aceptados por las Fuerzas Armadas de la Nación, que guían la preparación y empleo del instrumento militar tanto en tiempo de paz como en la guerra y que hacen al cumplimiento de su misión en la acción militar conjunta.

A su vez, la doctrina militar podría ser vista desde una doble perspectiva. Aquella vinculada con la "filosofía y principios" y la que trata de procedimientos (Cohen & Gooch, 1998). Esta línea divisoria es muy importante al considerar a la doctrina de un país en forma integral y porque no, en forma multidimensional y, aquella vinculada a las rutinas y lo estándar de los procedimientos. Ambas son necesarias para la obtención de un adecuado "poder de combate" (NATO, AJP-01, 2017, págs. 1-16 y 17) en términos de capacidades militares.

La doctrina de "alto nivel" refiere a "la naturaleza del conflicto" y a su esencia, es decir, a la preparación de toda una nación para la guerra, sus fuerzas armadas y los métodos para conducirla (Cohen & Gooch, 1998). La de "bajo nivel trata de las prácticas y procedimientos o rutinas propias del combate o de la operación de sistemas y equipos y de las coordinaciones necesarias para el funcionamiento de la organización (Cohen & Gooch, 1998).

Por otra parte, el ambiente estratégico contiene la amplia gama de factores que influyen en la comprensión que hace un comandante de su entorno operacional en términos de condiciones, circunstancias e influencias globales que afectan el empleo de todos los elementos del poder nacional.

Para la doctrina argentina conjunta el Ambiente Operacional es el conjunto de condiciones y características que existen en forma estable y semiestable en una región e incluye la influencia de la política nacional, el ambiente geográfico, la composición y capacidades de las fuerzas enemigas, las características de la lucha, los sistemas de armas que puedan emplearse y el marco de la conducción militar (República Argentina EMCO, PC 00-02, 2015).

En función de lo expresado se explora, en esta sección, la visión que sobre el ambiente estratégico poseen las doctrinas conjuntas del más alto nivel de Estados Unidos, Rusia, China y el Reino Unido, adonde se desarrollará el conflicto futuro y sus conexiones con la información. Y se hace referencia a la doctrina española y a un proyecto de doctrina conjunta argentina, más o menos reciente, que posee perspectivas de interés para este trabajo, al acercar una visión más moderna del conflicto, los dominios y perspectivas de tipo multidimensional e interagencial, en un contexto de marcada de incertidumbre y fricción.

7.2.1. El ambiente estratégico en el conflicto según la doctrina conjunta de China

Desde la perspectiva china, la situación internacional de seguridad experimenta

cambios con tendencias irreversibles en términos de la globalización económica, la sociedad de la información y la diversificación cultural en un mundo "cada vez más multipolar". Existen "importantes factores desestabilizadores e incertidumbres en la seguridad internacional. El orden y el sistema de seguridad internacional se ven "socavados por el creciente hegemonismo, la política de poder, el unilateralismo y los constantes conflictos y guerras regionales" (China, State Council Information Office of the People's Republic of, 2019, pág. 3)

Asimismo, señala que:

> Impulsada por la nueva ronda de revolución tecnológica e industrial, la aplicación de tecnologías de punta como la inteligencia artificial (IA), la información cuántica, los grandes datos, la computación en la nube y el Internet de las Cosas está cobrando impulso en el campo militar. La competencia militar internacional está experimentando cambios históricos. Las tecnologías militares nuevas y de alta tecnología basadas en TI se están desarrollando rápidamente. Existe una tendencia predominante a desarrollar armas y equipos de precisión de largo alcance, inteligentes, sigilosos o no tripulados. La forma de guerra está evolucionando hacia una guerra informatizada, y la guerra inteligente está en el horizonte. (2019, pág. 6)

China establece como fin fundamental de su defensa nacional en la "nueva era" el "salvaguardar resueltamente la soberanía, la seguridad y los intereses de desarrollo de China". Su "directriz estratégica militar" adhiere a los principios de defensa, autodefensa y respuesta posterior al ataque mediante una "defensa activa" y "subraya la unidad de la defensa estratégica y la ofensiva en el nivel operacional y táctico"; adopta "un enfoque holístico de la seguridad nacional" y se adapta activamente al nuevo panorama de competencia estratégica, las nuevas demandas de seguridad nacional y los nuevos desarrollos en la guerra moderna, para cumplir con eficacia sus tareas y misiones en la nueva era" (2019, pág. 8).

Las misiones y tareas asignadas a las Fuerzas Armadas chinas se enmarcan en los siguientes empleos: la salvaguarda de la soberanía, los derechos marítimos e intereses, el mantenimiento del alistamiento para el combate, el adiestramiento militar en condiciones de combate reales, la protección de intereses en los principales campos de seguridad, el contraterrorismo y el mantenimiento de la estabilidad, la protección de los intereses de ultramar y la participación ante desastres. (2019, pág. 11 a 16).

Respecto de la Protección de intereses en los principales campos de seguridad define que la "capacidad nuclear es la piedra angular estratégica para salvaguardar la soberanía y la seguridad nacionales", que el "espacio ultraterrestre es un dominio crítico" y que China "participa activamente en la cooperación espacial internacional, desarrolla tecnologías y capacidades relevantes" (2019, pág. 13).

Para China el ciberespacio es un área clave y sus fuerzas militares "aceleran la construcción" de sus capacidades en ese dominio, "desarrollan medios de defensa y seguridad cibernética, y construyen capacidades de defensa cibernética consistentes

con la posición internacional de China y su estatus como un importante país cibernético" (2019, pág. 13)

Las reformas en el área de la defensa China incluyen la promoción de la innovación en C&T de defensa y teoría militar para fortalecer áreas de innovación emergentes y en doctrinas militares, operaciones conjuntas y sistemas de información (2019, pág. 23).

Según el Manual *Chinese Tactics* (ATP 7-100.3) del Ejército de los EEUU, China describe la guerra como un largo continuo donde el poder militar es solo un componente. El poder duro incluye la capacidad militar, la industria de defensa, la inteligencia y acciones diplomáticas relacionadas, como las amenazas y la coerción. El poder blando al poder económico, los esfuerzos diplomáticos pacíficos, el desarrollo extranjero, la imagen global y el prestigio internacional (United States Army, ATP 7-1003, 2021, págs. 1-5).

Para esta publicación de los EE.UU., China emplea las operaciones de engaño, no como un "habilitador periférico", sino como una parte integral en todos los niveles de la guerra (2021, págs. 1-13), y el concepto de operaciones de información es similar al de EEUU, aunque no es tan inclusivo. Las operaciones de información chinas incluyen guerra de información, encubrimiento, el engaño como esfuerzos generales para engañar a un oponente, y artimañas como planes específicos dirigidos a un oponente en particular (2021, págs. 1-6).

7.2.2. El ambiente estratégico en el conflicto según la doctrina conjunta de EEUU

Según la NSS[21] publicada en octubre 2022, un interés vital de los Estados Unidos es el de "disuadir la agresión de la República Popular China, Rusia y otros estados" (Gobierno EEUU (NSS), 2022). A su vez, este documento estratégico sostiene que la "Estrategia de Defensa Nacional" norteamericana "se basa en la disuasión integrada" reconociendo que los competidores emplean todos los "dominios militares (terrestres, aéreos, marítimos, cibernéticos y espaciales) y no militares (económicos, tecnológicos y de información), y que EEUU también debe hacerlo (2022, pág. 22). En todo el texto de la Estrategia de Seguridad Nacional se observa la importancia dada por este país a la información y al uso que adversarios diferentes pueden hacer de ésta. Sólo como ejemplos, bajo el subtítulo "Fortaleciendo nuestra democracia" se menciona la necesidad de contrarrestar "las operaciones de manipulación de la información" y, al referirse a la centralidad de la cooperación, se señala la necesidad de contrarrestar el uso de la información como arma que busca socavar las democracias y polarizar las sociedades (2022, pág. 16 y 22).

La "Disuasión integrada", como eje de la Estrategia de Defensa, refiere no sólo a la integración a través de todos los dominios, sino también de las regiones, en todo el espectro del conflicto, a través de todo el gobierno de los EEUU (es decir empleando todos sus medios) y junto con aliados y socios (2022, pág. 22).

La visión de los EEUU indica que una forma de ver "cómo hacer la guerra" (warfare) es la distinción entre la guerra tradicional e irregular. Cada una de ellas sirve a propósi-

21 National Security Strategy 2022

tos estratégicos diferentes que derivan en formas distintas de empleo. La guerra es un todo unificado, que incorpora todos sus aspectos juntos, sean tradicionales e irregulares. Es, de hecho, una combinación creativa, dinámica y sinérgica (United States Joint Chiefs of Staff, JP 1, 2017, págs. I-5).

El propósito estratégico de la guerra tradicional es la imposición de la voluntad de una nación sobre otro u otros estados y evitar que este imponga su voluntad. Las operaciones militares en la guerra tradicional normalmente se centran en las fuerzas armadas de un adversario e implica la ejecución de operaciones militares de fuerza contra fuerza con una variedad de elementos convencionales y fuerzas de operaciones especiales (SOF) en todos los dominios físicos, así como en el entorno de información (que incluye el ciberespacio) (2017, págs. I-5 y I-6).

La forma de guerra irregular[22] se caracteriza como una lucha violenta entre actores estatales y no estatales por la legitimidad y la influencia sobre la población con la intención de obtener o mantener el control o la influencia y el apoyo de esta (2017, págs. I-6).

Los adversarios menos poderosos pueden ser actores estatales o no estatales y aplicar toda la gama de capacidades militares y de otro tipo para erosionar el poder, la influencia y la voluntad del oponente. También se pueden emplear métodos diplomáticos, informativos y económicos (2017, págs. I-6).

En cuanto al ambiente estratégico señala que se caracteriza por la:

> ...incertidumbre, la complejidad, los cambios rápidos y los conflictos persistentes. Este entorno es fluido, con alianzas y asociaciones que cambian continuamente y nuevas amenazas nacionales y transnacionales que aparecen y desaparecen constantemente. El entorno de seguridad estratégica presenta amplios desafíos de seguridad nacional que probablemente requerirán el empleo de fuerzas conjuntas en el futuro. (2017, págs. I-10).

Agrega que la capacidad de los EEUU para promover sus intereses nacionales depende de la eficacia del gobierno en el empleo de los instrumentos de poder nacional para alcanzar los objetivos estratégicos nacionales. El instrumento militar puede ser utilizado en una amplia variedad de formas que varían en propósito, escala, riesgo e intensidad de combate a través de un continuo de conflicto que va desde la paz hasta la guerra (2017, págs. I-12).

Por otra parte, incluye como funciones conjuntas que facilitan la planificación y el empleo de la fuerza conjunta al comando y control (C2), inteligencia, fuegos, movimiento y maniobra, protección, sostenimiento e información (2017, págs. I-17).

Esta última (información), "abarca la gestión y aplicación de la información y su integración deliberada con otras funciones conjuntas para influir en las percepciones, el comportamiento, la acción o la inacción de los actores relevantes y la

22 Ver N del A 16.

toma de decisiones humana y automatizada. Agrega que ayuda "a los comandantes y estados mayores a comprender y aprovechar la naturaleza generalizada de información, sus usos militares y su aplicación durante todas las operaciones militares" (2017, págs. I-19).

7.2.3. El ambiente estratégico en el conflicto según la doctrina de defensa del Reino Unido

A principios de 2021, Gran Bretaña presentó la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior, titulada "Gran Bretaña global en una era competitiva, la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exte–rior"[23] (United Kingdom MoD, 2021).

El documento identifica en extrema síntesis, el rol global que se busca alcanzar y las acciones a emprender para la presente década. Es interesante señalar que los aspectos referidos al ciberespacio se mencionan más de 130 veces, lo cual refleja su relevancia actual y la integración con el resto de las estrategias sectoriales.

Gran Bretaña sostiene que la adaptación a un mundo más competitivo requiere de un enfoque integrado[24] adonde se integra toda la gama de capacidades en un esfuerzo integral y transversal (2021, pág. 24).

EL "Marco Estratégico" de la Revisión responde a la visión que sobre las tendencias prevalecientes en el contexto internacional sirven de base para la elaboración de futuras políticas en forma integrada (2021, pág. 18). Un enfoque adaptativo y una integración más profunda en todo el gobierno se materializa en una estrategia planificada basada en la "Doctrina Fusión" presentada en la Revisión de Capacidad de Seguridad Nacional de 2018 (2021, pág. 19).

El enfoque integrado a su vez "respalda una toma de decisiones más rápida, una formulación de políticas más efectiva y una implementación más coherente al reunir la defensa, la diplomacia, el desarrollo, la inteligencia y la seguridad, el comercio y aspectos de la política interna en la búsqueda de objetivos nacionales intergubernamentales (2021, pág. 19).

Respecto de los cambios en la naturaleza y distribución del poder global refiere a un mundo más competitivo y multipolar, con cuatro tendencias generales que serán de particular importancia para el Reino Unido y el cambiante orden internacional: cambios geopolíticos y geoeconómicos, competencia sistémica, rápido cambio tecnológico y desafíos transnacionales (2021, pág. 24).

La doctrina de defensa británica de 2014 (JDP 0-01) expresaba que la seguridad nacional abarcaba la seguridad del estado y la protección de amenazas externas e internas y también la de los conciudadanos en el extranjero (United Kingdon MoD, JDP 0-01 , 2014, pág. 3).

---

23 En inglés Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy.

24 Whole-of-cyber approach en inglés.

> Las amenazas externas pueden dar lugar a invasiones, ataques o bloqueos. Las amenazas internas pueden incluir terrorismo, subversión, desorden civil, criminalidad, insurgencia, sabotaje y espionaje. Otras amenazas incluyen la inestabilidad causada por la crisis financiera, los eventos climáticos, cibernéticos u otras formas de ataque a la infraestructura nacional crítica y la posibilidad de una enfermedad pandémica. No podemos mantener nuestra propia seguridad de forma aislada. Nuestra seguridad nacional está integrada y depende de la seguridad de nuestros vecinos y socios (2014, pág. 3).

Agrega que para mantener la autoridad y la estabilidad dentro de los estados democráticos se requiere cumplir las legítimas necesidades políticas, económicas, sociales, religiosas y ambientales de individuos y grupos. Estas necesidades suelen expresarse colectivamente como seguridad humana, cuyas características son, para la doctrina de defensa británica las siguientes:

ILUSTRACIÓN 3 . **Seguridad Humana de acuerdo con la Doctrina de Defensa británica Fuente: JDP 0-01 Ministerio de Defensa de Gran Bretaña (2014)**

La seguridad humana se caracteriza por:	La seguridad humana está amenazada por:
La disponibilidad de *commodities* esenciales (agua, asistencia médica, refugio y alimento)	Tensiones políticas e ideológicas
Seguridad ambiental más amplia	Eventos originados por el ambiente
Libertad de no ser perseguidos o tener temor.	Tensiones raciales, étnicas o religiosas.
Proteger los valores culturales	Pobreza, desigualdad, criminalidad e injusticia
Gobernanza transparente y global	Competición para o por el acceso a los recursos naturales

FUENTE: JDP 0-01 MINISTERIO DE DEFENSA DE GRAN BRETAÑA (2014)[25]

La doctrina británica hace hincapié en la creciente competencia por los recursos dentro de un mundo globalizado que incrementa la amenaza a la seguridad humana y socava la estabilidad de un estado o región (2014, pág. 4 y 5).

> Los individuos pueden transferir su lealtad a cualquier grupo que parece, o promete, satisfacer sus necesidades. Estos grupos incluyen organizaciones no gubernamentales y estructuras transnacionales, y organizaciones que puedan existir temporalmente y/o, en parte, virtualmente. Una vez que estos

25 UK Defense Doctrine. Gran Bretaña: Ministerio de Defensa de Gran Bretaña.

> grupos reciben el respaldo popular, la amenaza a la seguridad aumenta (2014, pág. 4 y 5).

La seguridad tiene sus raíces "en las percepciones tanto de la soberanía nacional e intereses nacionales, y cómo se protegen y promueven" y surge de una combinación compleja de factores geoestratégicos, incluidos los ambientales, recursos, sociales, políticos, científicos, tecnológicos y aspectos militares (2014, pág. 4 y 5).

En cuanto a la estrategia militar expresa que su objetivo es asegurar una planificación estratégica coherente y eficaz en el uso de las Fuerzas Armadas y que es "inherentemente conjunta". También se sitúa por encima de los intereses de una sola fuerza y para ello, combina las capacidades militares para generar un efecto que cumpla con los requisitos de corto plazo, pero que está firmemente arraigada en una comprensión clara de los fines de la política a largo plazo (2014, pág. 11).

Las actividades que realiza el componente militar del poder nacional respaldan la estrategia y objetivos nacionales y pueden variar desde la disuasión y la coerción hasta la aplicación de la fuerza para contrarrestar una amenaza específica. El instrumento militar es más efectivo junto con el empleo de otros instrumentos, no es "un fenómeno independiente, sino la continuación de la política por diferentes medios" e influye en las mentes como en la producción de efectos físicos (2014, pág. 13 y 14).

La doctrina británica sostiene que la información sustenta los tres instrumentos nacionales de poder y permite la comprensión y la toma de decisiones. En consecuencia, es "un recurso crítico y su flujo será cuestionado". Se puede lograr una ventaja administrando, en términos relativos, el flujo de información mejor que el oponente. Esto se conoce como superioridad de la información (2014, pág. 14).

> 1.42. La difusión de información, a través de una estrategia de información intergubernamental, permite al Reino Unido ejercer influencia diplomática, económica y militar de manera eficaz e integrada. Al mismo tiempo, la inteligencia y la información recibida en todo el gobierno da forma a la planificación y ejecución de operaciones en todos los niveles (2014, pág. 13 y 14).

Y agrega que:

> En tiempos de crisis, la estrategia de información debe incluir una narrativa estratégica, que describa por qué el Reino Unido está comprometido y cuáles son sus objetivos. Esta narrativa es crucial para administrar la información de manera eficiente, así como para influir en una variedad de audiencias y actividades de manera consistente y coherente. (pág. 14 y 15)

Asimismo, al referirse al ciberespacio expresa que es un "entorno operacional" dentro del "entorno de la información". Enfatiza que la defensa depende cada vez más del ciberespacio y se puede esperar que los adversarios exploten esta dependencia. Final-

mente, sostiene en forma enfática que la capacidad para operar en el ciberespacio es vital para el interés nacional y facilita la seguridad nacional, prosperidad y forma de vida (2014, pág. 15).

7.2.4. El ambiente estratégico en el conflicto según la doctrina de empleo de Rusia

La Estrategia de Seguridad Nacional de la Federación Rusa (FR) de 2021 contiene propósitos y objetivos para "asegurar los intereses nacionales, las prioridades estratégicas, la seguridad nacional y objetivos duraderos de largo plazo" (Sapmaz, 2022). Incluye como objetivos de seguridad nacional la protección de los intereses nacionales contra las amenazas internas y externas, la preservación de los derechos y libertades constitucionales de los ciudadanos y un alto nivel de vida, el establecimiento de la paz y armonía dentro del país, la protección de la soberanía nacional, la independencia y la integridad territorial y el desarrollo socioeconómico de la FR (Sapmaz, 2022).

La FR ha ampliado y endurecido las dimensiones de la rivalidad y el conflicto con EEUU y Occidente y se ha convertido en algo más que la sola dimensión militar, para incluir cuestiones relacionadas con el campo de la cultura y la información.

En este sentido, "el liderazgo moral y la creación de una base ideológica atractiva para el orden mundial futuro emergen como un problema importante" (Sapmaz, 2022). La estrategia sostiene que se está llevando a cabo una operación de información para crear la imagen de «la Rusia enemiga» y expresa que la FR "está acusada de violar compromisos internacionales, realizar ataques cibernéticos e interferir en los asuntos internos de otros países" (Sapmaz, 2022).

Como prioridades nacionales estratégicas enumera: la protección del pueblo ruso y el desarrollo del potencial humano, la defensa nacional, la seguridad estatal y pública, la seguridad de la información, la seguridad económica, el desarrollo científico y tecnológico, la seguridad ambiental y la gestión ambiental, la preservación de los valores tradicionales y morales, culturales y memoria histórica de Rusia, la estabilidad estratégica y la cooperación internacional mutuamente beneficiosa (Sapmaz, 2022).

La estrategia rusa observa que el uso de la información y las comunicaciones cuando se emplea para "inmiscuirse en los asuntos internos de los países" es una violación a la "soberanía e integridad territorial de los países y constituye una amenaza para la paz y la seguridad internacionales" (Sapmaz, 2022) y:

> ...observa un aumento de los ciberataques contra los sistemas de información rusos. La mayoría de los ciberataques contra la FR se originan en el extranjero. Los intentos de la FR de garantizar la seguridad de la información internacional se encuentran con la resistencia de los países que quieren dominar el entorno mundial de la información. Las corporaciones transnacionales quieren fortalecer su monopolio en Internet, para controlar todo el entorno de la información. ... [En este contexto], el propósito de la seguridad de la información es garantizar la soberanía de la FR en el espacio de la información (Sapmaz, 2022).

Y agrega que:

> ...la «occidentalización» de la cultura rusa por operaciones psicológicas en el campo del conocimiento conduce a la pérdida de la soberanía cultural (Sapmaz, 2022).

Durante la conferencia llevada a cabo en la Academia Rusa de Ciencia Militar[26], el 2 de marzo de 2019 disertó el General Gerasimov. Sostuvo que las condiciones de los conflictos modernos indican para Rusia, que "el principio de la guerra" ha evolucionado basado en el uso coordinado de medidas militares y no militares, con un papel decisivo de las fuerzas militares (Johnson, 2019).

...afirmó que la variedad de guerras potenciales (utilizando una gama de medios asimétricos o "clásicos") y con participantes potenciales (estados soberanos, formaciones ilegales, empresas privadas y cuasi estados) está aumentando y ...que la amenaza de guerra está creciendo (Johnson, 2019).

Según la opinión de Gerasimov (y presumiblemente del Estado Mayor ruso), EEUU continúa "invadiendo" la esfera de acción rusa con infraestructura militar y socavando la estabilidad estratégica mediante una política exterior agresiva respaldada por medidas militares ofensivas como el ataque global, la coerción en los dominios, las revoluciones de colores y el poder blando (Johnson, 2019).

La llamada "doctrina Gerasimov" sostiene que las mismas "reglas de la guerra" han cambiado y que el rol de los medios no militares para lograr objetivos políticos y estratégicos ha crecido y, en muchos casos, han excedido el poder de la fuerza de las armas en su efectividad (Gerasimov, 2016, pág. 24).

Esta doctrina agrega que "los métodos aplicados en el conflicto se han modificado en la dirección del amplio uso de medios políticos, económicos, medidas informacionales, humanitarias y otras medidas no militares aplicadas en coordinación con el potencial de protesta de la población", incluyendo el empleo de "medios militares de carácter encubierto", que realizan acciones en el campo informativo y uso de fuerzas de operaciones especiales. "El uso abierto de las fuerzas, a menudo bajo la apariencia de mantenimiento de la paz y regulación de crisis, se recurre solo en una determinada etapa, principalmente para lograr el éxito final en el conflicto" (2016, pág. 24).

En el 2019 este jefe militar ruso dijo que las circunstancias actuales requerían que se continuara desarrollando formas y medios para el uso de las fuerzas militares afines a la disuasión estratégica y la defensa del estado (Johnson, 2019).

La respuesta de Rusia a las amenazas actuales y previstas consiste en una «estrategia de defensa activa» totalmente en línea con el carácter defensivo de la doctrina militar de Rusia. La estrategia comprende "medios integrados para la neutralización preventiva de las amenazas a la seguridad del Estado". Respecto

26 Академия военных наук Российской Федерации: traducido como Academia de Ciencias Militares de la Federación Rusa.

del empleo de todos los medios del poder ruso, el general Gerasimov aclaró el cambio en el peso relativo del componente militar, los roles principales y de apoyo, a medida que el conflicto pasa de ser un conflicto no militar a uno de tipo militar directo. Pero igualmente, aclaró que los conflictos modernos se "llevan a cabo mediante el empleo integrado de medios políticos, económicos, informativos y otros medios no militares, todos implementados con la confianza en la fuerza militar" (Johnson, 2019).

Los analistas y líderes rusos han desarrollado su propio conjunto de términos que aplican a la agresión percibida por Rusia entre los que se encuentran: el caos controlado, la estrategia de desgaste y destrucción, el uso de tecnología, las revoluciones de colores y la guerra híbrida. Desde esa perspectiva, las respuestas defensivas de Rusia se circunscriben a las nuevas formas de conflicto armado y se traducen ahora en una estrategia de defensa activa.

Además de los tradicionales dominios operacionales militares terrestres, aéreos y marítimos, Rusia resalta la creciente importancia del dominio de la información en los conflictos recientes. Éste, al no tener una "frontera internacional claramente definida, brinda la posibilidad de una acción oculta de largo alcance no sólo sobre la infraestructura de información de importancia crítica, sino también sobre la población de un país, lo que influye directamente en la condición de seguridad nacional de un estado" (Johnson, 2019).

El general ruso continuó diciendo que, "por esta misma razón, el trabajo sobre las cuestiones de preparación y conducción de acciones de carácter informativo es la tarea más importante de la ciencia militar" (Johnson, 2019).

Por otra parte, en un reciente estudio se precisan algunos términos empleados por la FR asociados a la "rivalidad en la esfera de la información" (Grisé, 2022, pág. 8). La "Guerra de información puede ser vista desde tres diferentes perspectivas: la primera se relaciona con un "enfrentamiento entre dos o más estados en el espacio de la información con el propósito de causar daño a los sistemas, procesos y recursos de información, infraestructura crítica y de otro tipo, socavar los sistemas políticos, económicos y sociales, la manipulación psicológica masiva de la población para desestabilizar el estado y la sociedad, además de coaccionar al Estado para que tome decisiones en interés de la fuerza contraria " (2022, pág. 8).

La segunda refiere a que es un "choque transparente y severo entre estados" caracterizado por causar un "impacto dañino en la esfera de la información", y la tercera, al "uso agresivo de información"[27] (2022, pág. 8).

Con referencia al modo de hacer la guerra de información (*information warfare*) el mismo trabajo cita que incluyen a las "actividades emprendidas para ganar la superioridad en el proceso de una confrontación armada" (2022, pág. 8).

Finalmente, entiende por operaciones de información al "conjunto de actividades de información coordinadas en términos de propósito, objetos, lugar y tiempo condu-

27 MoD, Military Encyclopedic Dictionary, sin fecha.

cidas para obtener y mantener la superioridad de la información sobre el enemigo o reducir" su superioridad de información en un teatro de combate dado o dirección estratégica (2022, pág. 8).

Boston y Massicot han desarrollado lo que denominan "claves" en la forma en que Rusia hace la guerra y cómo ve el conflicto. A continuación se mencionan aquellas de interés para este trabajo (Boston & Massicot, 2017).

Las fuerzas militares están posicionadas para defender su territorio, centros industriales y población vitales, utilizando diferentes capas, integrando defensas aéreas, mediante un número limitado de baluartes defensivos y usando estados amortiguadores para ganar espacio y tiempo para reaccionar ante posibles ataques.

Dadas las debilidades convencionales en una guerra prolongada con un adversario similar o cercano, intentará utilizar estrategias de acción indirecta y respuestas asimétricas en múltiples dominios para mitigar los desequilibrios percibidos.

1. Es probable que los enfoques de guerra convencional y no convencional se mezclen en muchos escenarios de conflictos potenciales; con el uso de las fuerzas de operaciones especiales, paramilitares y civiles simpatizantes que pueden proporcionar orientación, conocimiento de la situación y brindar algunas capacidades de hostigamiento en todo el espacio de batalla.

2. En el nivel operacional y táctico, es probable que se centre en interrumpir, degradar o destruir el mando y control y la proyección del poder del enemigo mediante el uso de fuegos cinéticos, guerra cibernética/electrónica y ataques directos (Boston & Massicot, 2017).

La estrategia de acciones limitadas enfatizaría, según Johnson, el dominio de la información. El despliegue oculto de un grupo de fuerzas apuntaría a la creación de un sistema integrado de inteligencia, medios de ataque y comando y control para permitir la ubicación, selección de objetivos y ataque a elementos de importancia crítica y blancos casi en tiempo real, por armas no nucleares estratégicas y tácticas (Johnson, 2019).

El general Gerasimov también espera que las fuerzas rusas necesiten emplear y contrarrestar la tecnología digital, la robótica, los drones y los medios de combate radioelectrónico en escenarios más allá del territorio ruso (Johnson, 2019).

7.2.5. El conflicto según la doctrina española y el proyecto conjunto de Argentina de 2018

La doctrina española para el Empleo de las Fuerzas Armadas, PDC-01 (A), reconoce que las dinámicas actuales generan una gran incertidumbre y un rápido proceso de transformación. Aunque la naturaleza de los conflictos permanece intacta, los potenciales adversarios ya no se reducen a Estados u organizaciones internacionales, y la tradicional frontera entre guerra y paz se difumina dificultando la identificación del

final de dichos conflictos con la concepción clásica de victoria o derrota. Los instrumentos de poder de una nación son el diplomático, el militar, el económico, el de la información y el social y son resultado de la suma de las capacidades de los poderes de su estado y de su sociedad (España Jefe de Estado Mayor de la Defensa, PDC-01 (A), 2018, pág. 15).

Entre los riesgos y amenazas a enfrentar resalta al terrorismo y los ataques cibernéticos; la limitación de acceso a los recursos y la injerencia y apropiación de los espacios comunes globales; los efectos derivados de conflictos locales y regionales, como el tráfico ilegal de armas y personas, la dispersión de combatientes o los flujos migratorios; las catástrofes, naturales o no; la proliferación de armas de destrucción masiva; el crimen organizado; la inestabilidad económica y financiera; la manipulación de la información; la vulnerabilidad energética; las pandemias y los efectos del cambio climático. Entre los potenciales adversarios, ya no se encuentran solo Estados u organizaciones multinacionales sino también actores de otro tipo (2018, pág. 18).

Respecto de las tendencias del conflicto actual remarca la presencia de la incertidumbre y adaptabilidad; la difuminación de los límites y de las referencias; la presencia generalizada y permanente de la población en los conflictos; y la importancia del componente tecnológico. La población civil pasa a ocupar un papel preferente en entornos en los que se mezclan combatientes y no combatientes y adquiere especial relevancia la comunicación estratégica y la cultura de defensa. (2018, pág. 20).

> La rápida evolución científica, tecnológica y social obliga a valorar los aspectos éticos del futuro entorno de seguridad, derivados principalmente del desarrollo de la robótica, la biotecnología, los sistemas autónomos, las actividades llevadas a cabo en el ciberespacio, el combate urbano y la difusa separación entre combatientes y no combatientes (2018, pág. 19).

Y agrega:

> Las tecnologías multiplican las posibilidades de generación, acceso y propa–gación de información de todo tipo. Su volumen e inmediatez dificultan su regulación y control, complicando la gestión y el discernimiento de su relevancia y veracidad, espacio, el combate urbano y la difusa separación entre combatientes y no combatientes (2018, pág. 19).
>
> Las tendencias generales de los conflictos imponen a los estados la integración del "poder militar con otros instrumentos de poder nacionales, tanto en el planeamiento de la estrategia como en su desarrollo. Ello requiere una estructura de inteligencia eficaz, segura y colaborativa, así como sistemas de mando y control que sean verticalmente ágiles, horizontalmente integradores y posibiliten el asesoramiento oportuno y eficaz para la toma de decisiones en todos los niveles (2018, pág. 19).

Por otra parte, el proyecto de doctrina conjunta básica argentina de 2018 (Proyecto PC 00-01) contiene aspectos relevantes para esta investigación. Reconoce la existencia de conflictos más allá de lo meramente tradicional e incorpora las perspectivas multidominio e interagencial empleadas por casi todos los países más adelantados en la materia (EMCO, PC 00-01 (proyecto), 2018).

Expresa que la paz es una condición ideal de la situación internacional que se caracteriza por el uso de medios no violentos en la resolución de intereses contrapuestos y, cuando "los medios no violentos fallan en resolver...disputas, al menos una de las partes podría buscar una ventaja a través del uso de la violencia" (2018, pág. 22).

Plantea la incertidumbre que caracteriza al escenario mundial y cómo este afecta al desarrollo del modelo de fuerzas para el largo y mediano plazo. Reconoce que los conflictos en las últimas décadas han adquirido una creciente variación en sus manifestaciones y que resulta cada vez más difícil la separación entre los períodos de paz y guerra. Por ello, parece que existe un "contínuum" o espectro del conflicto adonde sus extremos "serán la paz y la guerra" y entre ellos "encontraremos desde las operaciones militares a gran escala, hasta el apoyo humanitario en situaciones de emergencia", que adoptan distintos niveles según la intensidad del conflicto (2018, pág. 23).

De acuerdo a esta interpretación doctrinaria señalada en ese proyecto, los estadios del conflicto se pueden graficar de la siguiente manera:

ILUSTRACIÓN 4 . **Espectro del conflicto**

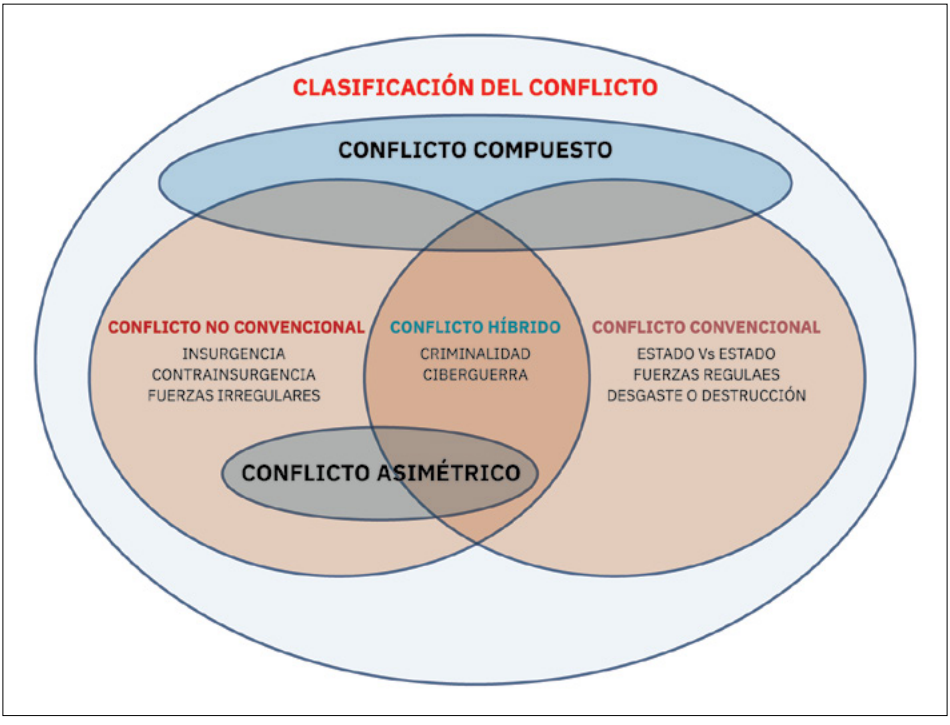
FUENTE: PROYECTO CONJUNTO ARGENTINO 2018 (PC 00-01 PROYECTO, PÁG. 23)

Continúa diciendo que la "naturaleza compleja del entorno estratégico puede requerir que las fuerzas conduzcan diferentes tipos de operaciones y actividades conjuntas simultáneamente a lo largo del espectro del conflicto" y que los "conflictos y su correspondiente evolución posibilitan percibir variaciones en sus niveles de intensidad", es decir, tensión, crisis y guerra que, en todos los casos quedan comprendidos dentro del Derecho Internacional Humanitario, también llamado DICA (2018, pág. 23 a 26).

Durante la tensión se pueden "adoptar medidas que contribuyan a disuadir potenciales agresiones y que persuadan" (2018, pág. 25 y 26). Respecto de la guerra reconoce que ha adoptado "diversas formas de ejecución, acorde con las modalidades de cada época y con los avances de la tecnología y del pensamiento estratégico militar, abarcando campos cada vez más amplios, con la participación activa de sectores de la población y el creciente empleo de medios y técnicas más evolucionadas" (2018, pág. 25 y 26).

Clasifica a los conflictos armados en varios tipos los cuales se pueden apreciar en la siguiente ilustración:

ILUSTRACIÓN 5 . **Tipos de conflicto armado**



FUENTE: PROYECTO DE LA DOCTRINA CONJUNTA ARGENTINA (PC 00-01 – PROYECTO, PÁG. 23).

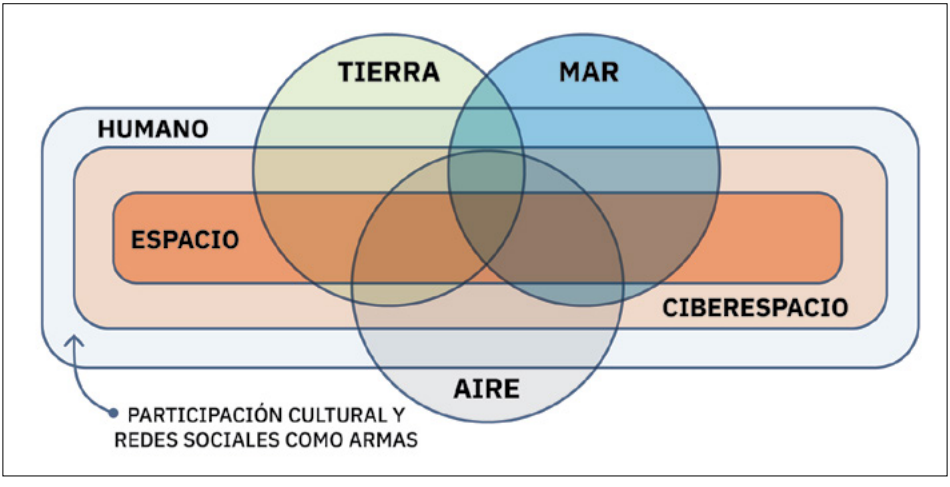
Para este proyecto el conflicto convencional/regular involucra el empleo en operaciones de una variedad de capacidades militares convencionales, en los diferentes ámbitos/dominios: aéreo, terrestre, marítimo, espacial y ciberespacial. El conflicto en ambiente no convencional/irregular favorece los enfoques indirectos y asimétricos para erosionar el poder, influencia del adversario, y su voluntad. Ambos no son exclu-

yentes y, el segundo, se enfoca en la afectación de la población del adversario, modificando su comportamiento.

El conflicto compuesto se caracteriza por la utilización de una combinación de medios convencionales y no convencionales y el híbrido es una característica general de los conflictos armados contemporáneos destacando el empleo del debilitamiento de su potencial militar y económico, mediante la presión informativa, psicológica y el apoyo activo a la oposición interna, combinando de acciones irregulares y operaciones especiales.

Como se muestra en la siguiente ilustración, el concepto de empleo en la batalla requiere para este proyecto que el instrumento militar posea la capacidad para accionar en diferentes ámbitos/dominios, aéreo, marítimo, terrestre, espacio, ciberespacio, electromagnético y humano, en una sinergia multiplicadora del poder de combate.

ILUSTRACIÓN 6 . **6 Tipos de conflicto armado**



FUENTE: PROYECTO DE LA DOCTRINA CONJUNTA (EMCO, PC 00-01 (PROYECTO), 2018, P. 28).

8. ¿Adónde va el diseño de las fuerzas militares para el conflicto futuro?

Hasta aquí hemos visto que hablar de guerra o de conflictos es referirse a un fenómeno social fundado en la naturaleza humana (von Clausewitz, 2021, pág. 803). Es un "acto de fuerza para obligar al contrario al cumplimiento de nuestra voluntad"; pero también es un instrumento de la política y no un fin en sí mismo, una parte del intercambio político por otros medios (2021, pág. 803). De la lucidez que tenga la élite política, su cultura estratégica y las decisiones que tome, dependerá la preparación que un estado realice para enfrentar los retos de un ambiente complejo y plagado de incertidumbre, como los que se han presentado a partir del fin de la Guerra Fría.

La "fuerza militar" se materializa en un vector[28] que es aplicado por las fuerzas armadas de un estado. Se compone de una combinación de materiales, maniobras, recursos humanos y logística. Posee una estructura y organización determinada la cual siempre debe tener relación con los objetivos políticos. La presencia de un enemigo le dará una característica única al conflicto. El enemigo no es un elemento inerte y no espera, sino que es una voluntad concreta que responde a una inteligencia (Smith, 2007, pág. 9) y una cultura propia y hará todo lo posible para evitar los objetivos propios.

Las guerras, las batallas y los conflictos son contingentes a un ambiente, un tiempo y un espacio único. El Siglo XXI ha acentuado la necesidad de realizar una visión holística y contar con un pensamiento sobre los conflictos presentes y futuros que se traduzca en estrategias de seguridad y defensa integradas o al menos estrechamente complementadas, en las cuales se integren todas las herramientas del estado. Las fuerzas militares no se preparan de la noche a la mañana para una guerra, conflicto o eventual contingencia de cualquier tipo.

Los conflictos son únicos e irrepetibles y aquellas fuerzas "que pretenden prepararse para todas las contingencias, terminan no siendo aptas para ninguna" (de Vergara, 2012, pág. 79 a 81) y (de Vergara, 2017, pág. 211).

Al respecto, Grissom, Farrell[29] y Jordán[30], sostienen que las transformaciones e innovaciones de las fuerzas militares a partir del fin de la Guerra Fría, surgieron de la necesidad de introducir cambios sustanciales ante los nuevos conflictos en términos de doctrina, adiestramiento y, "a menudo, en la orgánica y/o materiales de una o varias ramas de un ejército[31], al tiempo que supusieron un aumento considerable de su efectividad para cumplir alguna o varias de las misiones asignadas…" (Jordán, 2017, pág. 205).

La innovación militar apunta al diseño futuro de las fuerzas militares. Al respecto, la literatura especializada en transformación militar identifica cuatros factores claves intervinientes que están asociados a: los intereses organizacionales, las nuevas ideas y la cultura estratégica, el rol del liderazgo civil y militar y la respuesta a la experiencia en el nivel operacional (Farrell, Rynning, & Terriff, 2013, pág. 9) y que es de interés hacer una breve referencia.

Los intereses organizacionales se vinculan a las tareas y recursos de cada fuerza armada y a las tensiones y pujas que se pueden dar entre los servicios (2013, pág. 9 y 10). Una acción conjunta firme y un liderazgo civil efectivos, permiten trabajar con

---

28 En el sentido que posee una dirección y sentido y donde su módulo representa la intensidad.

29 Farrell, T., Rynning, S., & Terriff, T. (2013). Transforming Military Power since Cold War. Cambridge: Cambridge University Press.

30 Jordán, J. (2017). Un modelo explicativo de los procesos de cambio en las organizaciones militares. La respuesta de Estados Unidos después del 11-S como caso de estudio. Revista de Ciencia Política. Universidad de Granada, 27(1), 203-226. Obtenido de http://www.ugr.es/~jjordan/procesos-cambio-militar.pdf

31 El autor emplea "ejército" al referirse a todas las fuerzas militares.

sinergia en pos de un objetivo común y mando unificado, evitando o mitigando este tipo de situaciones ligadas a los medios y fines estratégicos (2013, pág. 10).

Del mismo modo, las nuevas ideas se deben propiciar para identificar, mediante el análisis de los conflictos futuros, qué acción o acciones son apropiadas y efectivas para los escenarios de la defensa y seguridad internacional. Por ejemplo, los EEUU se encuentran elaborando la doctrina de las Operaciones Multidominio para enfrentar a Rusia y China, el Ejército británico el "Future Land Combat System (FLCS)" que se inserta en el nuevo Concepto Operacional de Defensa Integrado[32] y el EMCFFAA argentino, ya habla de una doctrina original que se centraría en una aproximación multicapas (Paleo, 2022) a partir de que en la DPDN 2021 se expresa la necesidad de contar con una doctrina propia que potencie la alerta temprana estratégica, la ciberdefensa y el fortalecimiento de organizaciones de "despliegue rápido y/o grupos de operaciones especiales…." (República Argentina Ministerio de la Defensa, 2021, pág. 21).

Ya se mencionó también que la cultura estratégica[33] de un estado se manifiesta en patrones decisionales que van más allá de la "mera política" para responder a una cosmovisión particular o distintiva asentada en las clases dirigentes. Opera para dar forma a cómo los que toman las decisiones ven el mundo, el rol que le toca como actor y las posibilidades de su acción militar (Farrell, Rynning, & Terriff, 2013, pág. 11).

El cambio estratégico y socio-tecnológico ha tenido un rol destacado como impulsor de la transformación militar. En la actualidad se están desarrollando y combinando nuevas tecnologías, como las de macrodatos junto a la digitalización con conectividad constante, sumado a la inteligencia artificial, dando lugar a lo que se ha dado a conocer como la "cuarta revolución industrial –o sistemas ciberfísicos" (Finney , 2020, pág. 223).

Los cambios emanados en la seguridad internacional, los conflictos, la aparición de una agenda social heterogénea y la promoción de valores democráticos en los estados influyeron en la sociedad en su conjunto y, dentro de ella, en las fuerzas militares. Rapp indica entonces la necesidad de ampliar, en los entornos actuales, el diálogo civil militar para "alinear mejor los medios y las estrategias, con los fines deseados", construir relaciones adecuadas y brindar el mejor asesoramiento militar como parte de una estrategia holística para lograr los objetivos nacionales (Rapp, William, 2015, pág. 16).

Pareciera que el tipo de conflicto actual que se tiende a configurar es el que se vincula con el empleo combinado de actores estatales y no estatales, en una manifestación híbrida o bien dentro de la llamada "zona gris". En este sentido, es necesario destacar que las acciones empleadas en dicha zona, tales como la propaganda, la influencia política o económica o la desestabilización no son elementos novedosos, sino que se han encontrado presentes en la humanidad desde tiempos remotos. El desarrollo de los "sistemas tecnológicos, así como de los medios de comunicación y redes sociales"

32 En inglés "Integrated Operating Concept (IOpC)".
33 Pp. 22.

ha otorgado ventajas a los seres humanos pero también "creado nuevas vulnerabilidades, incrementando exponencialmente las posibilidades de éxito de las actividades de dicha naturaleza" (España Ministerio de Defensa, 201, 2019, pág. 31)

> ...no solo porque hayan surgido mecanismos de gran potencial de daño y fácil uso, como pueden ser los ciberataques, sino especialmente porque las nuevas tecnologías en el ámbito social e informativo permiten explotar de forma muy eficaz los resultados de las acciones llevadas a cabo por cualquier otro medio, multiplicando así sus efectos y contribuyendo de forma decisiva al éxito global en la consecución de los objetivos estratégicos pretendidos (2019, pág. 31).

Al respecto, Moresi expresa al referirse a este tipo de conflictos que no llegan a constituirse en guerras de tipo interestatal y se conducen en zonas grises o guerras híbridas, donde todo el andamiaje del Derecho Internacional Humanitario (DIH), posee es desafiado. Este tipo de conflictos adoptan "un formato transnacional y/o intraestatal, cuando en realidad también se trata de una forma de confrontación de terceros por la hegemonía de poder a través del sistema denominado "guerra proxy" (Moresi A. , 2021).

En un ambiente altamente conectado y globalizado, la solución no es sólo militar, ni exclusiva de un dominio terrestre, marítimo, aéreo o espacial, ni tampoco proviene solamente del campo de las informaciones. Por el contrario, surge de una combinación conjunta, interagencial y de ser propicio combinada de todos los medios disponibles del estado, sean estos letales o no letales.

Los conflictos que estamos presenciando, aún aquellos con alto contenido híbrido y empleo intensivo de herramientas propias del *soft power,* no invalida en lo absoluto, la vigencia en el empleo de las llamadas operaciones cinéticas[34] en la guerra moderna. Las fuerzas militares en un empleo verdaderamente conjunto e integrado, con unidad de comando y objetivo unificado permiten operar en todos los dominios y parece que caracterizarán el conflicto en los años por venir. Porque su uso garantiza la efectividad para vigilar y controlar, proteger, posicionar, disuadir y combatir para lograr la influencia esperada.

En un reciente documento titulado *Soldado Futuro*[35], el Ejército británico refiere a que el campo de batalla futuro será diferente y que las capacidades heredadas van quedando rápidamente obsoletas. Las armas destruirán con mayor alcance, precisión y letalidad. Las personas conservarán su centralidad en el campo de las voluntades, mientras que los sistemas autónomos, robots y UAV reducirán cada vez más el número de individuos comprometidos en primera línea. Los datos y las redes digitales serán la clave. Se privilegiará la disponibilidad de un ejército[36] adaptado, ligero,

34 Refiere a las formas activas de hacer la guerra incluyendo el uso letal de la fuerza en contraposición a un empleo del poder blando en todas sus formas.

35 En inglés "Future Soldier - Transforming the British Army".

36 El documento se refiere al ámbito terrestre.

rápido, integrado sostenible y escalable, para responder en forma efectiva a las amenazas actuales y futuras (British Army, 2021).

Tal vez el conflicto actual en Ucrania (2022) permita observar con mayor detenimiento el papel de la guerra de la información y la estrategia de defensa integral en el nivel estratégico general y sectorial, donde se afiance la necesidad de rearme convencional, el aumento de la potencia nuclear y la inversión en sistemas defensa mientras que en el nivel operacional, se potencia la necesidad de empleo de capacidades militares multidominio, con la combinación de otras herramientas, en una suerte de totalización entre técnica, industria, fuerzas armadas, estado y sociedad.

Los cierto es que las operaciones militares actuales son cada vez más dinámicas y activas y carecen de frentes y profundidades. El dominio del ciberespacio ha permitido reducir en forma significativa los espacios y tiempos, acortando las cadenas de comando y control, los tiempos de decisión y la conciencia situacional del soldado en el terreno. Las acciones de fuerzas enfrentadas pueden, más a menudo, no llegar al contacto, al igual que el logro objetivos operacionales y tácticos alcanzado por fracciones menores. Los niveles de la guerra tienden a confundirse y la aplicación de armas de precisión, uso de drones, medios informativos y la combinación de otras diferentes tecnologías se confunden, sumado al uso de acciones de tipo asimétrico para anular las ventajas de un eventual enemigo que puede o no ser una fuerza militar.

Pero en cualquiera de los casos, los entornos en donde los comandantes decidirán serán únicos, porque ya se afirmó una y otra vez, que no hay guerra igual a la anterior. Los ambientes operacionales impondrán limitaciones a la conducción de las fuerzas militares. Ellas serán normales y ocurrirán en mayor o menor grado durante el desarrollo de todo tipo de operaciones militares (República Argentina Ejército Argentino, ROB 00-01, 2015).

La revolución sin precedentes en las comunicaciones excederá a los "…ciber–ataques y ciberdefensa, aunque estas sean importantes. Las guerras de estado a estado están sucediendo y continuarán sucediendo, pero algunos no ven cómo evolucionarán…" (Betz & Stevens, 2011, pág. 80).

El ciberespacio continuará accionando con una influencia creciente en la estrategia de los estados, abarcando todos los espacios de actuación de las personas adonde la ecuación "hombre-teclado-máquina" es esencial. En este contexto la idea de defensa tiene una mayor magnitud que la de la defensa de fronteras y recursos para incluir aspectos que apuntan a preservar las fundaciones de la sociedad misma en una idea de nación (Girardi, 2023).

Es más, pareciera que las percepciones de la realidad tienen más peso que la realidad misma y allí los líderes toman sus decisiones. Consecuentemente, el "valor en el conflicto ha pasado a ser el cerebro de las personas que componen una sociedad" (Moresi A. , 2021, pág. 10).

En extrema síntesis y parafraseando a Gerasimov, la guerra llevada a cabo simultáneamente en todos los entornos físicos y en el espacio de información y el uso de

operaciones asimétricas e indirectas, un comando y control de fuerzas y empleo de activos en el espacio informacional, parecen ser la norma en los actuales y futuros conflictos adonde se verá una creciente gravitación de la tecnología.

De esto se trata esta contribución que busca fomentar el libre pensamiento y la reflexión de los lectores en un ámbito caracterizado por la libertad académica en pos de generar un propio pensamiento estratégico.

Capítulo 2

Las operaciones en el espectro electromagnético (EEM)

Por TC OIM (R) Carlos Amaya

1. **Introducción**

Así como las moléculas de aire y los principios de la aerodinámica definen el dominio del aire, las moléculas de agua y los principios de la hidrodinámica definen el dominio del mar, el espectro electromagnético (EEM) y los componentes electrónicos relacionados que se propagan en forma de energía definen el ciberespacio.

Mucho se ha dicho y escrito sobre las operaciones en el EEM, pero realmente, ¿conocemos que es el EEM, el concepto casi esotérico que el común de las personas tiene respecto de lo que verdaderamente es el EEM?

A lo mejor si lo analizamos desde el punto de vista de ciencia básica nos será fácil interpretar o imaginar las potenciales amenazas que sobre él pueden producirse y por lo tanto, las medidas defensivas u ofensivas a adoptar en cada caso. Así comprenderemos mejor el verdadero sentido que tienen las acciones dentro de este ambiente, donde el EEM se transforma en el protagonista, dado que, a lo largo de él, considerando las frecuencias como el eje de las ordenadas de un par de ejes de coordenadas cartesianas, se puede visualizar todo tipo de información pasible de ser atacada, infiltrada, perturbada, inhibida e incluso transformada con la finalidad de engaño o influencia sobre las decisiones o la voluntad del adversario.

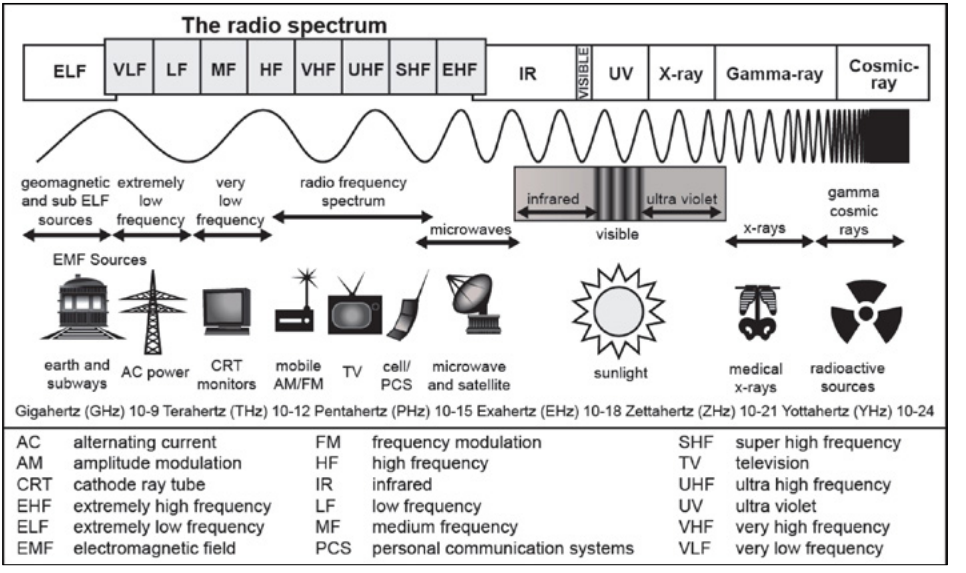
En este capítulo hemos pretendido reflexionar sobre la concepción o la comprensión de las acciones relacionándolas con el EEM donde la informática, las redes y la transmisión de datos son una parte del escenario protagónico.

Por lo tanto, es interesante que tratemos de hacer una abstracción y nos centremos en el análisis sobre la concepción y el significado de lo que pretendemos mostrar.

Luego, para que sea posible acercar el tema a los propósitos militares de la planificación estratégica y operacional, se analizarán las posibilidades de integración en el dominio de la información, para ampliar las posibilidades del ciberespacio y competencia de fuerzas multidominio. De manera complementaria, también se presentan conceptos doctrinarios necesarios para la integración de los conceptos electromagnéticos a las acciones físicas en el escenario de un conflicto bélico.

2. **Evolución del concepto electromagnético**

ILUSTRACIÓN 7 . **Cyberspace operations and electromagnetic warfare**



FUENTE: UNITED STATES ARMY, FM 3-12 (2021, P. 1.8)

La perturbación que nos preocupa se propaga en lo que se da en llamar comúnmente el éter o por un medio sólido particular, entendiendo por particular aquel medio que cumple con condiciones de conductividad eléctrica.

Pero el espectro electromagnético es mucho más amplio que solo las ondas de radio, tv y telefonía. Una pequeña porción de ese espectro es accesible de forma directa por los seres vivos, a través de la vista, dando origen a la optoelectrónica (ver ilustración), posiblemente la más explotada dentro del 5to dominio[37], dado que por este sector del EEM se desplazan las portadoras de datos de alta velocidad, telemetría,

37 A medida que los dominios de la guerra han aumentado de dos (tierra y mar), a tres (aire), a cuatro (ciberespacio) y cinco (espacio). (NATO CCDCOE , 2020)

guiado de sistemas de armas y una amplia gama de servicios de sensores con la gran ventaja de poder detectar la irradiación sin que la misma pueda ser detectada fácilmente por algún tipo de contramedida del adversario (visión o imagen térmica).

Y aquí comienza el relato de una pequeña gran historia que nos lleva a reflexionar que lo que estamos tratando no es algo nuevo o que está *por venir*.

Es algo que nació en el pensamiento y la historia con Platón y Aristóteles.

Hablemos entonces del ÉTER, pero no del gas utilizado en los laboratorios cuya existencia es completamente real, sino del concepto desarrollado hace siglos, que afirmaba la existencia de un fluido llenando el espacio, más allá de la atmósfera de la tierra.

El temor a la nada era razón suficiente para imaginar un éter que llenará todo el espacio, más allá de cualquier objeción.

Se trataba de un fluido sutil, sin peso, impalpable en el cual se propagaban las ondas luminosas.

En esa teoría las ondas luminosas o de manera general lo que hoy diríamos parte de la radiación electromagnética únicamente podía propagarse si existía un medio que lo hacía posible, para ese entonces se pensaba que la luminosidad no podía propagarse en el vacío.

La noción de éter tuvo un rol importante en la elaboración de la teoría de los fenómenos electromagnéticos, pero es partir de la teoría de la relatividad restringida que empezó a dudarse la existencia del éter, perdió todo rigor científico, pero sin embargo aún perdura en el imaginario popular.

Por un lado, somos propensos a utilizar el éter como una forma de referirnos a la propagación de ondas. Y su conceptualización ha transitado diversas épocas con significados diferentes, pero finalmente asociados.

En la mitología griega, que era una estructura de explicación del mundo, no es extraño encontrar un Dios primordial de la luz. ÉTER, en este caso fue el Dios de los cielos capaz de llenar el espacio entre el sol y la cúpula de éste.

El aire de la tierra estaba gobernado por la diosa primordial CAOS, pero el aire situado por encima era dominio de ÉTER.

Siendo un Dios primordial, ÉTER no era la personificación humana de un elemento sino el elemento mismo, era todo el aire situado entre la tierra y el cielo. Para la mitología, el primer ÉTER es un Dios y paradójicamente, comenzamos aquí con los paralelismos que fundamentan la evolución del concepto de ciberespacio y 5to dominio.

Más tarde Platón y luego Aristóteles como dijéramos, recrearon el significado de ÉTER dándole una connotación más cercana a la ciencia. Mientras que para Platón el ÉTER era la forma más pura del aire. Para Aristóteles era un elemento que existía solamente en la bóveda celeste pero que tenía la capacidad de moverse en círculos sin influencia de ninguna fuerza externa.

Veamos entonces cómo vamos llegando a conclusiones un poco más lógicas y no tan esotéricas.

La teoría aristotélica establecía la existencia de cinco elementos, los cuatro que conocemos, fuego, aire, agua, tierra y el éter. Pero consideraba que este último era el primero de los cinco porque constituía el lugar que podía contener y justificar el movimiento de los astros. En este concepto aristotélico ÉTER era una forma de principio de vida.

Llega el siglo XVII y se inicia otra línea de pensamiento científico más formal.

Rene Descartes (1596-1650), filósofo, matemático y físico francés, padre de la geometría analítica y la filosofía moderna utilizó al éter para explicar los movimientos planetarios. Lo definía como una materia compuesta de lóbulos transparentes cuyos remolinos eran el origen de los movimientos de los planetas.

En resumen, para Descartes, gracias al éter los planetas permanecían en sus trayectorias, y además poseía función igualmente importante, era la de transmitir la luz en forma de una presión.

Si hacemos abstracción de lo que hoy sabemos y consideramos la explicación correcta de los fenómenos que hoy nos rodean y nos ubicamos en el siglo XVII, podemos decir que se trataba de una teoría absolutamente correcta.

Para Descartes, el vacío no tenía la capacidad de transmitir nada ni de engendrar o permitir el movimiento; se necesitaba un soporte y a ese soporte lo llamó "ETER", total el concepto ya estaba creado para cubrir esa incógnita espacial.

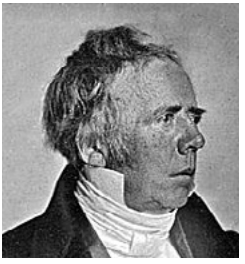
Fue lo que pocos años más tarde se transformó en la gravitación traída de la mano de Newton a fines del siglo XVII.

Newton concluyó en la falsedad de la existencia de los remolinos de Descartes en el éter y se dio cuenta que la armonía del movimiento en el universo era producto de una fuerza que se transmitía instantáneamente entre los cuerpos a cualquier distancia y en cualquier medio vacío o no y nació así la ley de la gravitación universal.

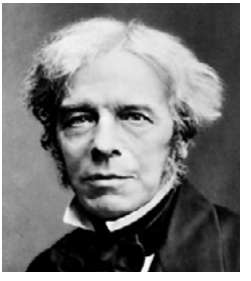
Si bien Newton no estaba totalmente convencido de que las acciones gravitatorias entre los cuerpos pudieran transmitirse sin que existiera un elemento que las albergará y habló entonces de un éter mecánico que llenaba el espacio y permitía la transmisión de la fuerza gravitatoria, no escapó a la idea del origen divino del éter; el éter tampoco escapó a la explicación de la propagación de la luz que la mecánica Newtoniana consideraba formada de corpúsculos que transmitían oscilaciones al éter generando de esta manera los colores. Con posterioridad existió la teoría ondulatoria de la luz.

Poco a poco este concepto va tomando cuerpo y con Ampere (1775 y 1836) que es quien interpretó el fenómeno del

magnetismo con la teoría de la corriente molecular según la cual innumerables partículas minúsculas cargadas, estarían en movimiento dentro del elemento físico que cumpla la función de conductor. Esta teoría es rechazada por los científicos de la época y no se impone hasta setenta años después gracias al descubrimiento del electrón.



Hans Christian Oersted, quien nació en Dinamarca en 1777 y murió en Copenhague en 1851, lleva a cabo el experimento que consistió en colocar una aguja imantada próxima a un conductor por el que circulaba una corriente eléctrica y observó que la aguja se movía; lo que demuestra que las corrientes eléctricas generan campos magnéticos. De esta manera la relación entre corriente eléctrica y campos magnéticos quedaba demostrada.

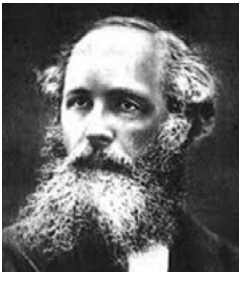


El Británico Michael Faraday, que vivió entre 1791 y en 1867, basándose en estos experimentos, desarrolla el primer motor eléctrico conocido y postula que *"...la diferencia de potencial eléctrico inducido en un circuito es directamente proporcional a la rapidez con que cambia en el tiempo el flujo magnético que atraviesa una superficie".*

El alemán Carl Friederich Gauss entre 1777 y 1855 contribuyó significativamente en muchos ámbitos incluido la teoría de números, el análisis matemático, la geometría diferencial, la estadística, el álgebra y en especial para lo que nos importa en este momento, en el magnetismo y la radiación en el rango de radiación del visible.

Por último, James Clerk Maxwell, científico escocés (1831-1879), basado en los hechos investigados por los citados científicos, enuncia una serie de ecuaciones que son las que hoy nos describen el fenómeno de la propagación electromagnética, teatro de operaciones donde se soporta la actividad cibernética.

De esta forma Maxwell nos describe que "si un campo eléctrico variable produce un campo magnético variable y éste a su vez produce un campo eléctrico, crea otro campo magnético y así sucesivamente debe tener lugar una serie de transformaciones de energía cuando tiene lugar cualquier perturbación eléctrica o magnética, la energía pasa del campo magnético al eléctrico y viceversa", dándonos la idea de una perturbación que se propaga.



Las ecuaciones de Maxwell conducen entonces al fenó–meno que se describe en la "ecuación de onda", como para demostrar en principio que "la energía se propaga en forma de onda electromagnética."

Cuando una onda electromagnética se propaga lo hace en todas direcciones y como una onda esférica.

Es así que la física del siglo XX ya avanzado, concluyo que el ÉTER no era necesario para explicar la propagación de la energía gravitatoria y las ondas electromagnéticas, ellas se transmiten en el vacío. Pero la búsqueda de explicaciones a los fenómenos que observamos es interminable.

A principios del siglo XX comenzaron a desarrollarse los sistemas de comunicaciones por radio. Guglielmo Marconi fue el gran impulsor de la idea de utilizar las ondas electromagnéticas para transmitir mensajes.

Cada vez "son más numerosas las aplicaciones de las telecomunicaciones inalámbricas, podríamos aventurar coincidir metafóricamente con los pensadores del pasado expresando que hoy el éter es el alma del mundo". (Reggini, 2010)

¿Es posible que nos preguntemos, a qué vienen estas historias?. Pues si reflexionamos, veremos que el *dominio* al que muchas veces escuchamos llamar *nuevo*, para nada lo es, tiene su historia y ha existido desde siempre.

Una vez más, estamos demostrando que lo que verdaderamente ha evolucionado es la tecnología de los materiales que han permitido desarrollar las estructuras de los componentes que conforman los sistemas de telecomunicaciones llegando hoy, como dijéramos, a provocar la generación de frecuencias cada vez más elevadas y por lo tanto un *ancho de banda* que permite la transmisión de datos a velocidades inimaginables, hecho que retomaremos un poco más adelante.

Es por ello que comprendiendo que nada ha cambiado sobre la concepción del fenómeno de propagación electromagnética, siempre desde el punto de vista de ciencia básica, desde Maxwell a nuestros días, nos será fácil entender cómo las operaciones ofensivas, defensivas o de explotación, pueden materializarse casi idénticamente a como se acostumbraba en las experiencias de la *guerra electrónica,* hoy *guerra electromagnética.*

Sirva lo relatado hasta este momento como introducción al concepto de energía en movimiento o traslación sobre distintos medios, sin considerar una teoría corpuscular de dicho fenómeno, entrando entonces al concepto específico del fenómeno de propagación electromagnética.

3. **Fenómeno de propagación electromagnética**

este fenómeno, incluye todas las señales que circulan por el espectro electromagnético (teléfonos celulares, internet, radio difusión comercial, emisiones espontáneas, rayos X, telecomunicaciones en general).

Si un equipo radioeléctrico emite o recibe, quiere decir que está usando un lugar que hoy llamamos genéricamente el *Ciberespacio*.

> El reino del ciberespacio comprende mucho más que la guerra de redes. El ciberespacio es un dominio, como la tierra donde se aplican cada uno de los principios de la guerra. Para entender este concepto se requiere un cambio cultural de las personas y estructural de las instituciones dada la importante afectación en la planificación de las operaciones bélicas. (Wynne, 2007)

"La guerra electromagnética es una acción militar que involucra el uso de energía electromagnética dirigida, para controlar el espectro electromagnético o para atacar al enemigo" (United States Joint Chiefs of Staff, JP 3-85, 2020).

Las aplicaciones del fenómeno electromagnético fueron transitando un camino de acelerado desarrollo, de ello son solo algunos ejemplos el radar, las radios, televisión, telefonía celular, navegación satelital, telemetría y estas aplicaciones constituyen una dimensión de lucha permanente.

Cada parte de los protagonistas del conflicto, trata de tener, por ejemplo, un radar que vea mejor, o una contramedida que *ciegue* los radares enemigos, una comunicación que transmita más volumen de información, pero que también sea inmune a la interceptación y que tenga un sistema de cifrado más robusto.

Estos conceptos podríamos considerarlo como el *"entendimiento clásico"* que se tiene de la guerra electromagnética.

Pero "es dable considerar que hay otros aspectos en una guerra, como la propaganda, la psicología, la desinformación, que afectan a la voluntad de pelear y a la toma de decisiones estratégicas. Estos son todos dominios, o dimensiones de la guerra, para los cuales las comunicaciones electromagnéticas son hoy el campo de batalla" (Dubois, 2020).

Por lo tanto no podemos ni siquiera imaginar el ciberespacio sin considerar prioritariamente la Guerra Electromagnética (GEM). Por ello a lo largo de este capítulo siempre que consideremos el ciberespacio estaremos considerando la GEM.

Sin dudas, el ciberconflicto de hoy en lo que llamamos el *quinto dominio,* no es otra cosa que una evolución natural de lo que era la Guerra Electrónica devenida en Guerra Electromagnética de mano del avance en el estudio del aprovechamiento de las propiedades de los materiales y elementos electroquímicos.

Ejemplo de lo mencionado lo tenemos en los siguientes hechos evolutivos:

Según Wynne[38], en septiembre de 2006 el Estado Mayor Conjunto de los Estados Unidos, aprobó una definición del ciberespacio considerándolo como "un dominio caracterizado por el uso de componentes electrónicos y el espectro electromagnético (EEM) para guardar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas relacionadas" (Wynne, 2007).

En agosto de 2018, el mismo Estado Mayor, lo define como "un dominio global dentro del entorno de la información que consiste en la interdependencia entre redes de infraestructuras de tecnología de la información y datos residentes, incluido Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados" (United States Jont Chiefs of Staff, JP 3-12, 2018).

"Las operaciones en el ciberespacio necesitan del uso de enlaces y nodos ubicados en otros dominios físicos para materializar operaciones lógicas. Funciones estas que crean efectos en el mismo y que luego se filtran a través de los dominios físicos, utilizando las redes y el EEM" (United States Army, FM 3-12, 2021).

---

38 Michael W. Wynne, fué secretario de la Fuerza Aérea de los EU entre Noviembre de 2005 y junio de 2008.

Notemos entonces como en quince años se evolucionó en la concepción de lo que entendemos por ciberespacio. En 2006 nos remitíamos solo a los componentes electrónicos, el EEM, las redes e infraestructuras físicas relacionadas y al intercambio de datos.

En 2021 al mismo concepto lo hemos integrado con el dominio global (necesidad de nodos dispersos), el entorno de la información, las redes e infraestructuras de tecnologías de la información, los datos residentes, la Internet, las redes de telecomunicaciones, los procesadores y controladores informáticos y el espectro electromagnético.

Evidentemente se han sumado: el dominio global, el entorno de la información, la internet, el almacenamiento de datos, el procesamiento y controladores informáticos. Pero han permanecido casi invariables las redes, los datos que sobre ellas se transportan y el EEM.

Nos preguntamos entonces, ¿qué es lo que ha permitido esta evolución?

Concluimos y reafirmamos que lo que ha evolucionado es la profundización del conocimiento de los materiales que hoy conforman el *hard* de los sistemas, al haber podido sacar de ellos un mayor rendimiento el que nos ha permitido como mencionamos anteriormente, subir las frecuencias en el EEM y en consecuencia aumentar los anchos de bandas para poder transferir mayor cantidad de datos por unidad de tiempo, dando origen de esta manera a ingenios que se materializan en el desarrollo de la *Big Data* (procesamiento de gran cantidad de datos por unidad de tiempo), el empleo de las técnicas de Inteligencia Artificial (IA) y la naciente era de la Computación Cuántica.

Observamos que ha permanecido invariable el protagonismo del EEM, reafirmamos de esta manera que el ciberespacio incluye la totalidad del EEM.

En definitiva, la definición mencionada y que compartimos en este capítulo, no centra el conflicto en el ciberespacio solo en la internet y las redes, sino que incluye además las capacidades como la energía dirigida del fenómeno del electromagnetismo (Inhibición de señales), de la que hablaremos más adelante. El propósito de ello es reflexionar que "nada es nuevo" en esta área, solo basta con asumir que la evolución sobre el conocimiento de los materiales es exponencial y que todo va hacia lo que se da en llamar "punto de singularidad tecnológica".

Pero el EEM siempre está presente.

Es dable comentar que es en 1984, cuando William Gibson inventa el término ciberespacio en su novela futurista "Neuromante", donde relata las aventuras de un pirata que recibe la oferta de concretar sus andanzas en un ambiente pseudo tecnológico que era prácticamente inimaginable, donde ya se planteaban conceptos de Big Data e Inteligencia Artificial.

Heli Tiirmaa-Klaar[39] al referirse al ciberataque que sufrió Estonia en el año 2007 expresó lo siguiente:

39 Heli Tiirmaa-Klaar fuera Ciber-Embajadora de Estonia diplomática asesora del lado de la OTAN y encargada de montar la política europea en el ciberespacio y que en el año 2019 fue una de las 28 personalidades de Europa

> Los ciberataques no caen del cielo hay que colocarlos en un contexto político.... en 2007 no es que pasara algo en el ciberespacio, pasó algo en el mundo real, el elemento cyber será usado para ayudar los objetivos estratégicos de un conflicto político.... no habrá ninguna ciberguerra, habrá una guerra real con una faceta ciber siempre hay una razón política. (Tiirmaa-Klaar, 2019)

Las operaciones en el EEM se materializan en la totalidad de las plataformas de los sistemas de armas, control de teleprocesos, componentes de señales de telecomunicaciones y sistemas y subsistemas de sensores de telecontrol, cobrando cada vez más protagonismo el sector del EEM que incluye longitudes de ondas del orden del infrarrojo (ver ilustración).

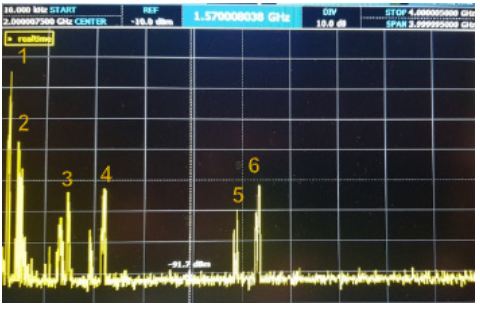
Encontramos un antecedente interesante en la última directiva del comandante de marines, General US Marine Corps David H. Berger donde expresa:

> El Mundo ha profundizado nuestra dependencia colectiva de la información en la medida en que una mínima vulnerabilidad en la forma en que manejamos, almacenamos o transmitimos información podría poner en peligro a los marines, sus familias y todo lo que hemos jurado defender. (United States Marine Corps, MCDP8, 2022)

Cabe destacar que cuando habla de transmisión de la información está sin duda destacando el protagonismo del EEM como medio por el cual la información se propaga mayormente.

Veremos de ordenarnos para describir a modo de ejemplos, las particularidades de lo que ocurre en cada uno de los sectores del EEM donde principalmente se desenvuelven las redes de telecomunicaciones; ello en función de la variación del parámetro principal del mismo, la *frecuencia*, o sea la velocidad en que esa variación a la que se refería Faraday se produce en la unidad de tiempo.

ILUSTRACIÓN 8 . **Analizador de espectro**



FUENTE: EL AUTOR.

En principio cada una de ellas, pueden verse representadas en un analizador de espectro, que cubre tan solo un rango entre los 10 megahertz (Mhz) y los 4 gigahertz (Ghz)

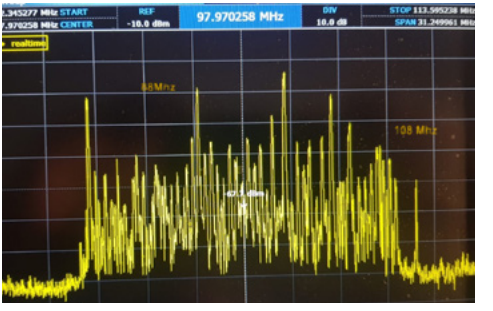
En el caso que mostramos en la ilustración anterior, vemos referenciado con el número 1, la banda para el servicio de emisoras de frecuencia modulada (FM), en frecuencias comprendidas entre 88 Mhz y 108 Mhz, se divide en 100 canales de 200 Khz cada uno (Reglamento General del Servicio de Radiodifusión Sonora

por Modulación de Frecuencia – FM – Resolución 142 SC/96)

Si entramos en el sector "1", veremos que cada elevación de la curva, marca la frecuencia portadora de una emisora de radiofonía comercial en FM.

Este ejemplo nos ilustra dándonos idea de cómo se vería la marcación de los distintos canales utilizados en cualquier tipo de punto de acceso de cualquier sistema de telecomunicaciones.

ILUSTRACIÓN 9 . **Frecuencia portadora de una emisora**



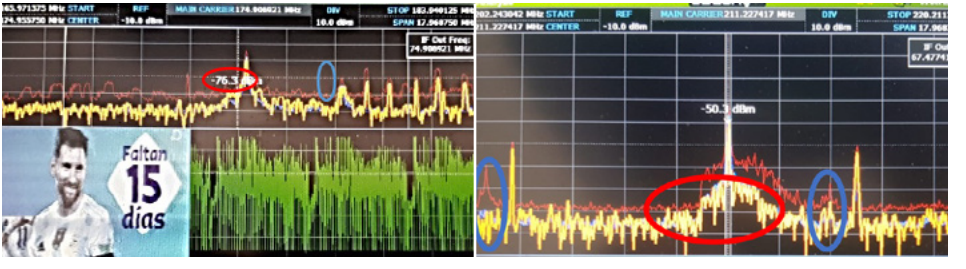
FUENTE: EL AUTOR.

En el caso referenciado "2", vemos las portadoras de los canales de televisión de aire del 7 al 13 denominada Banda II-VHF (Resolución 292 MOySP/81 y 3128 CNT/92).

En tal sentido cabe este ejemplo para reafirmar el concepto de lo que hemos mencionado anteriormente como ancho de banda y para ello centremos nuestra atención en la figura siguiente, donde habiendo sintonizado nuestro analizador de espectro en 174,906921 Mhz, para obtener una imagen razonablemente buena de un canal de televisión comercial, es necesario contar con un ancho de banda muy superior (marcado en rojo) al que es necesario para el ancho de banda por donde llega el audio (marcado en azul). Ello es debido a que para el caso de las señales de video nuestros sistemas necesitan transportar una cantidad muy superior de datos.

Este concepto que acabamos de mostrar, es absolutamente el mismo que rige por sobre todas las aplicaciones y funcionalidades en la EW.

ILUSTRACIÓN 10 . **Ancho de banda de un canal de televisión comercial**



FUENTE: EL AUTOR.

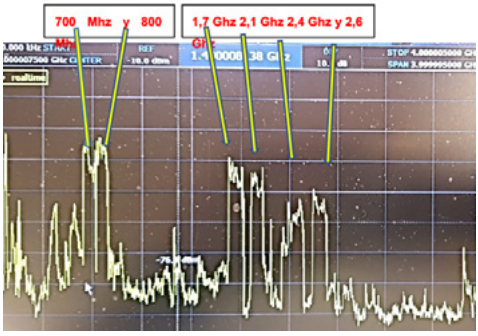
Volviendo a la ilustración inicial, las zonas identificadas con los números 3, 4, 5 y 6 nos muestran las emisiones presentes de radio bases de telefonía celular al momento y la zona geográfica en donde se concretaron las mediciones. Ellas en los órdenes de 700

Mhz, 800 Mhz, 1,8 Mhz y 2,1 Mhz respectivamente.

En la ilustración se puede observar lo que sucede cuando esas frecuencias son atacadas por energía electromagnética específicamente dirigida y por lo tanto interfiere toda información por ellas transportada.

Sirva este caso solo como un ejemplo que se cumple con similares características en cualquier plataforma de sistemas de armas, así como sobre las redes de telecomunicaciones.

ILUSTRACIÓN 11 . **Ancho de banda de un de radio bases de teléfonos celulares**



FUENTE: EL AUTOR.

4. **La competencia electromagnética**

En situaciones de competencia o conflicto multidominio entre estados, las acciones militares físicas y no físicas estarán presentes en el entorno operacional. Las operaciones electromagnéticas son acciones incorporadas al concepto de acción militar no física, considerando las capacidades especiales en el dominio de la información.

El análisis de los aspectos informativos, físicos y humanos del entorno operacional comprende cómo todas las formas de información o transmisión impactan en el medio ambiente e identifican cómo se pueden usar las operaciones electromagnéticas para afectar la relación cada vez más compleja y dinámica de los aspectos informativos, físicos y humanos (cognitivos) de una operación militar. Sin embargo, el análisis que utilizan los tres aspectos no separan los elementos del entorno en *contenedores* para el análisis individual, por el contrario, considera que el proceso debe integrarse en acciones físicas y no físicas (United States Joint Chiefs of Staff, JP 3-04, 2022).

Las operaciones electromagnéticas están en continua competencia, sea en un ambiente de paz o de guerra. La superioridad en el ciberespacio y las emisiones permiten a las fuerzas armadas la anticipación estratégica para realizar operaciones defensivas para lograr las metas y cumplir los objetivos que se les asignan. Las fuerzas armadas pueden realizar operaciones electromagnéticas durante situaciones que no involucren el conflicto armado, así como realizar operaciones de combate a gran escala durante un conflicto armado, las cuales son capacidades críticas para el poder de combate.

Las operaciones de gestión del espectro juegan un papel crucial en la construcción del entorno operacional de un campo de batalla multidominio extendido. En la competencia de múltiples dominios, el enemigo buscará emplear capacidades para crear efectos en múltiples dominios para impedir las operaciones amigas (United States Army, FM 3-12, 2021).

En una situación de conflicto armado, los actores de amenazas realizarán actividades en el entorno de la información, el espacio y el ciberespacio para influir en los

tomadores de decisiones e interrumpir el despliegue de fuerzas amigas. Corresponde a los comandos operacionales coordinar las capacidades especiales no físicas y su interrelación con las acciones físicas:

> La sincronización e integración general de operaciones en otros dominios también requeriría una arquitectura C2 habilitada para inteligencia artificial, también llamada sistema de gestión de batalla habilitado para IA integrado dentro de una internet de cosas militares capaz de presentar a un comandante una imagen operacional común en tiempo real que incluiría un ciber e imagen electromagnética. (NATO CCDCOE , 2020)

Las amenazas terrestres intentarán impedir la libertad de acción de las fuerzas conjuntas en los dominios aéreo, terrestre, marítimo, espacial y cibernético. Interrumpirán las emisiones electromagnéticas, sembrarán confusión y desafiarán la legitimidad de las acciones.

Existen numerosos requisitos técnicos, organizativos y doctrinarios necesarios para la integración eficaz de las capacidades electromagnéticas en operaciones multidominio en futuros escenarios de guerra de alta intensidad. Los avances tecnológicos y la facilidad con la que las personas y los sistemas automatizados pueden acceder y utilizar la información contribuyen a que las amenazas electromagnéticas actuales se vuelvan cada vez más transregionales, multidominio y multifuncionales. Las amenazas transregionales son capaces de explotar y utilizar la información en el nivel mundial para provocar múltiples crisis o conflictos simultáneos e interconectados que abarcan más de un área de responsabilidad o área funcional de un comando combatiente. Las amenazas de todos los dominios tienen acceso a capacidades avanzadas y aprovechan la tecnología durante las operaciones en todos los dominios físicos y el entorno de información para disputar las ventajas con oportunidad (United States Joint Chiefs of Staff, JP 3-04, 2022).

En el nivel tecnológico, se desea una red integrada de la capacidad electromagnética en combinación con una capacidad C2 habilitada para IA que permita la integración y sincronización de capacidades de ataque cibernético y cinético en operaciones de múltiples dominios. Una red integrada es una red o sistema de dispositivos informáticos interconectados que incluyen sensores, plataformas de armas y recursos de almacenamiento de datos, y las acciones electromagnéticas siempre estarán presentes. Por lo tanto, teóricamente recopilaría y crearía grandes cantidades de datos compartibles, que podrían convertirse en inteligencia electromagnética procesable para paquetes de ataques cibernéticos o electromagnéticos.

El espectro electromagnético permite la transferencia rápida de paquetes de ataques, por ejemplo, aeronaves para apuntar a sistemas enemigos con brechas de aire a través del espectro de radiofrecuencia (RF). La sincronización e integración general de operaciones en otros dominios también requeriría una arquitectura C2 habilitada para IA, también llamada sistema de gestión de batalla habilitado para IA inte-

grado dentro de una red capaz de presentar a un comandante una imagen operacional común en tiempo real que incluiría el ciber y las acciones electromagnéticas. En esencia, un sistema de gestión de batallas habilitado por IA en comparación con un sistema de gestión de batallas convencional se basa en algoritmos de aprendizaje automático para procesar grandes datos de múltiples fuentes para el apoyo de decisiones de C2 con el fin de acelerar el llamado observar, orientar, decidir, y actuar (OODA) (Schubert et al., 2018).

Comprender cómo se pueden presentar múltiples amenazas para las fuerzas conjuntas en todos los dominios puede ayudar a los comandantes a identificar, aprovechar y explotar sus oportunidades de combate no físico. La implementación de acciones electromagnéticas a la seguridad de las operaciones es una acción fundamental para proteger las infraestructuras de tecnología de la información, los sistemas de mando y control y los sistemas de selección de objetivos esenciales y fáciles de usar. La seguridad de operaciones electromagnéticas es una capacidad que identifica y controla información crítica, indicadores de las acciones de fuerzas amigas que sirven en operaciones militares e incorpora contramedidas para reducir el riesgo de que un adversario explote vulnerabilidades (United States Army, FM 3-12, 2021).

5. **Las acciones electromagnéticas militares**

Las actividades electromagnéticas militares se pueden dividir en acciones electromagnéticas de ataque, defensa y apoyo (United States Joint Chiefs of Staff, JP 3-85, 2020):

a. Acciones de ataque electromagnético (AAE): para llevar a cabo la planificación operacional, selección de objetivos, ejecución y evaluación, la fuerza conjunta requiere una comprensión clara de los efectos que puede crear la guerra electromagnética.

AAE puede llevarse a cabo tanto con fines ofensivos como defensivos. Dado que un sistema AAE transmite energía electromagnética como cualquier otro transmisor, también se puede utilizar para transmitir energía electromagnética para otros fines que no sean ataque electromagnético. Esto se hace más comúnmente para operaciones psicológicas o para crear efectos en el ciberespacio. En tales casos, es importante que esos efectos se creen usando las autoridades legales apropiadas y también que su uso cumpla con la ley de la guerra y las reglas de empeñamiento aplicables.

Los efectos que pueden crear los sistemas de acciones de ataque electromagnético incluyen *destrucción, degradación, interrupción y engaño.* Los tres primeros efectos son efectos de negación que se pueden colocar en un continuo de temporal a permanente y de parcial a completo. Por lo tanto, un efecto sobre una capacidad podría describirse como interrumpido durante un breve período de tiempo, destruido o degradado en diversos niveles durante diversos períodos de tiempo.

1) Destrucción: la destrucción hace que la condición de un objetivo esté tan dañada que no pueda funcionar ni restaurarse a una condición utilizable en un período de tiempo relevante para la operación actual. Cuando se usa en el contexto de guerra elec-

tromagnética, la destrucción es el uso de acciones electromagnéticas para afectar el personal, las instalaciones o el equipo del enemigo objetivo. Los sensores y los nodos C2 son objetivos lucrativos porque su destrucción influye fuertemente en las percepciones (en el cognitivo) y la capacidad del enemigo para coordinar acciones y tomar decisiones. Los activos espaciales en órbita, así como los servicios informáticos en el ciberespacio, también son objetivos potencialmente lucrativos para acciones de ataque electromagnético. La guerra electromagnética, a través de acciones electromagnéticas de apoyo, contribuyen a la destrucción al proporcionar información y/o ubicaciones de objetivos procesables. Si bien la destrucción del equipo enemigo es un medio efectivo para eliminar permanentemente aspectos de la capacidad de un enemigo, la duración del efecto en las operaciones dependerá de la capacidad del enemigo para reconstituirse.

2) Degradación: la degradación reduce la eficacia o la eficiencia de un sistema dependiente de sistemas electromagnéticos enemigos. El impacto de la degradación puede durar unos segundos o permanecer durante toda la operación. Por ejemplo, la degradación puede confundir o retrasar las acciones de un enemigo, pero un operador experto puede evitar los efectos para reducir o eliminar su impacto. La degradación se logra con la interferencia de acciones electromagnéticas, el engaño de acciones electromagnéticas y la intrusión de acciones electromagnéticas. La degradación puede ser la mejor opción para estimular al enemigo a determinar la respuesta del adversario o para el condicionamiento en el espectro electromagnético. La degradación puede ser adecuada para lograr el éxito general de la misión.

3) Interrupción: es interrumpir temporalmente el funcionamiento de un sistema dependiente de acciones electromagnéticas enemigas. La interrupción interfiere con el uso del sistema electromagnético por parte del enemigo para limitar sus capacidades de combate. Un operador enemigo capacitado puede frustrar la interrupción a través de acciones de protección electromagnética efectivas (por ejemplo, cambio de frecuencia, protección electromagnética). El objetivo de la interrupción es confundir o retrasar la acción del enemigo. Las técnicas avanzadas de acciones de ataque electromagnético ofrecen la oportunidad de interrumpir de forma no destructiva la infraestructura enemiga.

4) Engaño: las acciones de engaño están diseñadas para engañar al enemigo mediante la distorsión de la percepción para inducirlo a reaccionar de manera perjudicial para sus intereses. El engaño en un contexto de guerra electromagnética presenta a los operadores enemigos y funciones de procesamiento de nivel superior con entradas erróneas, ya sea directamente a través de los propios sensores o a través de redes basadas en sistemas electromagnéticos, como comunicaciones de voz o enlaces de datos. Mediante el uso de los sistemas electromagnéticos, la guerra electromagnética manipula el ciclo de decisión del enemigo, lo que dificulta establecer una percepción precisa de la realidad objetiva. El engaño a menudo se usa con fines defensivos para evitar ser el objetivo de un enemigo en un enfrentamiento táctico o mediante la inyección de señales falsas en un sensor como un radar. Esto no debe confundirse con operaciones

psicológicas, que a menudo se utilizan para presentar mensajes de propaganda a los responsables de la toma de decisiones, normalmente a un nivel superior. La distinción es importante porque las autoridades legales requeridas que rigen acciones electromagnéticas difieren de las que rigen operaciones psicológicas enemigas.

b. Acciones de protección electromagnética: la protección electromagnética se lleva a cabo para garantizar que las fuerzas puedan operar a pesar de los efectos potencialmente adversos de la radiación electromagnética enemiga. Proteger es cubrir o proteger de la exposición, el daño o la destrucción. En el contexto de las acciones de protección electromagnéticas, el efecto de la protección es poder continuar el uso de sistemas dependientes en rede a pesar de los efectos de la radiación electromagnética adversa.

Acciones de protección electromagnética no debe confundirse con acciones de ataque electromagnético defensivo. El ataque electromagnético defensivo se utiliza para proteger contra ataques físicos, mientras que las acciones de protección electromagnética garantizan la capacidad de operar en un ambiente multidominio congestionado y/o disputado.

c. Acciones de apoyo electromagnético: el apoyo electromagnético se lleva a cabo en sostener las operaciones y es crucial para apoyar otras actividades de la guerra electromagnética. Las acciones de apoyo electromagnético se pueden utilizar en apoyo de operaciones ofensivas o defensivas y puede proporcionar información general para alerta temprano o información más detallada en apoyo de la planificación o selección de objetivos. El apoyo electromagnético no debe confundirse con inteligencia de señales, que requiere diferentes autoridades y reglas de empeñamiento. Hay dos efectos que pueden ser creados por el apoyo electromagnético:

1) Detectar: La detección ocurre cuando se descubren e identifican emisiones electromagnéticas de amenazas potenciales mediante el uso de medidas de apoyo electromagnético. Es el primer paso esencial en cualquier actividad electromagnética de seguimiento.

2) Explotar: La explotación aprovecha al máximo cualquier información disponible con fines tácticos, operacionales o estratégicos. En un contexto de la guerra electromagnética, la explotación es apoyo electromagnético que aprovecha al máximo la energía electromagnética radiada para recolectar, caracterizar, ubicar y rastrear las fuentes de radiación electromagnética para respaldar las operaciones actuales y futuras. Las acciones electromagnéticas pueden mejorar o habilitar la explotación para estimular los sistemas dependientes de sistemas electromagnéticos o para guiar a un enemigo hacia el uso de sistemas explotables.

6. **Conclusiones**

Uno no puede imaginar actividades en el ciberespacio sin considerar prioritariamente la guerra electromagnética. El avance de la tecnología expandirá las acciones electromagnéticas en el ciberespacio.

En el ciberespacio, el electromagnetismo está presente en todos los sistemas de comunicación y los sistemas de comunicación militar estarán cada vez más interconectados. El grado de protección de los sistemas de comunicación determinará el grado de soberanía de un estado, debido a la existencia de una gran competencia militar en este ámbito.

En la competencia militar electromagnética, las características de cualquier plataforma de sistemas de armas, así como en las redes de telecomunicaciones, pueden verse afectadas por acciones electromagnéticas.

Las actividades electromagnéticas militares se pueden dividir en acciones electromagnéticas de ataque, defensa y apoyo, y la protección electromagnética se lleva a cabo para garantizar que las fuerzas puedan operar a pesar de los efectos potencialmente adversos de la radiación electromagnética enemiga.

Es posible decir, por lo tanto, que las acciones militares físicas y no físicas estarán presentes en el entorno operacional de las situaciones de competencia o conflicto multidominio entre estados.

Capítulo 3

La guerra cibernética

Por BM (R) Mg. Alejandro Moresi

1. **Introducción**

La naturaleza de la guerra ha permanecido invariable desde el principio de los tiempos hasta nuestros días; los cambios en los modos de hacer la guerra y la perspectiva estratégica que se visualizan en los conflictos del siglo XXI, en gran medida se encuentran impactados por un nuevo ambiente para la vida humana y social, como es el ciberespacio.

Este siglo introdujo consigo una "revolución Tecnológica", en la que el desarrollo de: robótica, biotecnología, computación cuántica e inteligencia artificial (IA), carga sobre el hombre común un desafío de proporciones, tanto en la gestión del conocimiento como en la toma de decisiones. Contar con una racionalidad casi perfecta como se prevé se alcanzaría con la IA en el evento llamado singularidad, estar a la altura del mismo, requiere contar con capacidades poco o nada desarrolladas en la humanidad.

Los avances en las neurociencias ofrecen una nueva perspectiva sobre las capacidades del cerebro y del desarrollo de la mente humana, ello se torna vital para los futuros decisores. La Big Data además de permitir contar con casi toda la información, podrá ser procesada en una infinidad de combinaciones a través de sistemas de IA, lo que abre el interrogante sobre ¿cuál será el aporte humano?

Ninguno de estos avances ha detenido el conflicto humano, sino que, muy por el contrario, este continúa en su eterno intento de imponer la propia voluntad sobre el adversario y, el ciberespacio como ambiente de operación, ha alcanzado una importancia tal que en muchos casos ha desplazado el acto cinético de la guerra a un segundo plano; la batalla se trasladó del campo de combate a la mente del individuo y de la sociedad.

Esta situación produce algunos interrogantes desde la perspectiva estratégica militar:

1. ¿La inclusión del ciberespacio implica una revisión de la Estrategia Militar?
2. ¿Cuáles son los alcances de la guerra cibernética?
3. ¿Cómo impacta la revolución tecnológica en la concepción estratégica militar para enfrentar el conflicto futuro?

En este capítulo nos introduciremos en la problemática de la naturaleza de la guerra y en los conflictos del Siglo XXI, desde la perspectiva del dominio CIBERESPACIAL, intentando comprender como actúan las diferentes culturas estratégicas (occidental, soviética y oriental) a fin de responder a las preguntas formuladas, explorando cómo ellas limitan o extienden la libertad de acción de quienes deben formular propuestas para la Defensa Nacional ante un Conflicto.

1.1. **Reflexionando acerca de la Naturaleza de la Guerra**

La naturaleza de la guerra no ha ariado desde el principio de los tiempos dado que el objetivo siempre fue doblegar la voluntad del enemigo e imponer la propia.

Sin embargo, los modos de la guerra han mutado, las nuevas formas en general se asociaron con las ventajas que dan los desarrollos tecnológicos, los nuevos procesos, tácticas o procedimientos que permiten adquirir un diferencial ventajoso sobre el enemigo.

Los conflictos, se dirimían en la tierra, luego se extendieron al mar y ya en el siglo XX a la atmósfera con soporte en el espacio exterior; pero en el siglo XXI el espacio y el ciberespacio se encuentran completamente integrados a los clásicos, como ámbitos de la guerra.

Más allá de todo estudio, la ejecución de la guerra en el campo de batalla se ha caracterizado por la irracionalidad, por de sus altos niveles de violencia, heroísmo, cobardía y entrega que van más allá de la comprensión. La guerra puede analizarse desde una perspectiva lógica, puede intentar humanizarse a través de leyes y acuerdos, pero en su ejecución siempre será difícil de comprender esa violencia extrema más allá de lo razonable.

El siglo XXI, trae nuevos pensadores estratégicos que excluyen el concepto de paz y guerra, en una suerte de blanco y negro, cambiándolo por una idea de conflicto permanente (Mc Fate, 2019, pág. 27).

Una cuestión similar, sucede con la capacidad humana, donde se ha ensalzado la racionalidad como fuente casi exclusiva de conocimiento, llegando a excluir o considerar otras áreas como la intuición de significativas proporciones en las decisiones profunda de los seres humanos.

Sin embargo, volviendo a la problemática del conflicto, el imponer la propia *voluntad*, (naturaleza de la guerra), implica aspectos relacionados con el deseo, el *compromiso* y la *determinación*.

La primacía de la voluntad sobre el adversario implica el manejo de factores

como: *poder, libertad*[40] *y seguridad,* tres pilares del *desarrollo humano* y que a su vez no son estables, sino que la presencia de uno siempre modifica a los restantes y los condiciona.

A través del tiempo los seres humanos han considerado que el control de todos estos aspectos y factores, dependían del accionar en el campo de batalla. El efecto cinético, horroroso e irracional de la contienda domina la voluntad del adversario por el miedo e incluso el terror que infunde el dolor físico, aspecto que no sucede en el ciberespacio. Las tecnologías de la información y las comunicaciones (TICs) como parte del conflicto, están trasladando lentamente la batalla del campo de combate a la mente de la sociedad de los individuos que la componen. Su influencia en los decisores está cambiando la forma de dominio de la voluntad.

La tendencia del conflicto actual es coincidente con el planteo de filósofos como Byung-Chul Han, donde no es la acción punitiva, sino la convicción propia la que se impone para cumplir con los deseos del adversario (Han B. C., 2016). Paradójicamente más de 2000 años después, se alcanza lo consignado por Sun Tzu, en *"El arte de la guerra" donde predica "lograr cien victorias en cien batallas, no es el pináculo de la excelencia. Sojuzgar al enemigo sin luchar es el verdadero pináculo de la excelencia"* (Tzu, 2015, pág. 38).

La Guerra, un hecho eminentemente fáctico, paradojalmente busca controlar aspectos intangibles del ser humano, su voluntad, imponiendo el miedo sobre la materia y en el espíritu, allí donde se debate la naturaleza de la guerra. En este contexto, el ciberespacio alcanza la dimensión exacta de su realización como ambiente primario en el conflicto moderno, intentando alterar la naturaleza humana cambiando la espiritualidad por virtualidad y controlando la voluntad a partir de la aceptación inconsciente del deseo del adversario.

Así las nuevas guerras no serán, ni parecerán las clásicas, como explican Qiao y Wang: "El objetivo de este tipo de guerra abarcará más que simplemente usar medios que involucren la fuerza de las armas para obligar al enemigo a aceptar la propia voluntad». (Qiao & Wang,, 1999, pág. 37).

La naturaleza de la guerra es desde una perspectiva humana, casi inmutable. Siempre en una relación de más de uno existe naturalmente la imposición de la voluntad de uno sobre el otro, los modos en que ello se produce son innumerables y el objeto de éstas líneas es discurrir acerca *"del conflicto"*, en lo que se ha dado a llamar el *quinto dominio,* el ciberespacio.

1.2 Breve síntesis de la evolución de la guerra hasta nuestros días

La seguridad del individuo y su supervivencia, desde la perspectiva individual o como miembro de una comunidad, ha sido el tema esencial desde el principio de los tiempos. La necesidad de defenderse es naturalmente el origen de los sistemas defensivos.

---

40 El concepto aquí empleado de libertad es el aristotélico entendido como "preferencia reflexiva de lo mejor", un acto de la voluntad que a través de la inteligencia permite seleccionar el bien mayor, en tanto el entorno lo permita, el mismo depende de cómo se amordaza la voluntad.

A lo largo de la historia existió cierta convicción tácita acerca de que la violencia ejercida sobre otro a través del empleo de la fuerza era el medio para la solución de problemas imponiendo la voluntad de una parte sobre la otra. Así vemos que, desde la Edad de Piedra, aquellos que descubrieron una fuente esencial de riquezas como la agricultura que dio origen a los pueblos sedentarios, debieron generar estructuras defensivas que los protegieran de aquellos que deseaban hacerse con sus riquezas.

De esta manera, se fue gestando una relación extraña entre la fuerza y el conocimiento tecnológico. La primera parecía la herramienta adecuada y más preciada para acceder a la segunda. La fuerza se convirtió en sinónimo de poder que permitía alcanzar todo lo deseado. De esta forma, la tecnología y la guerra se asociaron de tal fuerza, que la civilización que obtuvo el bronce fue vencida por la del hierro y ésta por la del acero, convirtiendo la carrera del conocimiento para el desarrollo de nuevas armas en la esencia de las nuevas ciudades-estados, reinos e imperios.

La utopía humana era la paz, pero el camino escogido no ofrecía otra solución que el conflicto. Las sociedades entonces comienzan a encontrar personas que se dediquen a su protección y así comienza a nacer una "estirpe" que en la antigüedad se denominaron guerreros. Al respecto, Platón al comparar el trabajo del teñido de telas con la formación del guerrero nos dice:

> ...escogiendo nuestros guerreros con las mayores precauciones y prepa–rándolos mediante la música y la gimnasia. Nuestra intención al obrar así, es que tomen una tintura sólida de las leyes; que su alma bien nacida y bien educada, se penetre de tal manera de la idea de las cosas que son de temer, lo mismo que todas las demás, que ninguna clase de loción pueda borrarla; ni la del placer, que para este efecto tiene otra virtud distinta que la cal y los lavados, ni el dolor, ni el temor, ni el deseo. Esta idea justa y legítima de lo que es de temer y de lo que no lo es; esta idea, que nada puede borrar, es a lo que yo llamo valor... (Platón, 1872, pág. 212)

Luego de fracaso de la *pax romana,* nacida en el imperio homónimo, devino la era feudal y el fracaso de ésta devino en el estado moderno. La formación de los primeros ejércitos estatales, fue una época donde el desorden y la violencia estaban en manos de quien podía ejercerla, y así se llega a la llamada *Paz de Westfalia*[41]*,* que será el elemento que convierte a los estados en su configuración actual. Sus tres pilares son:

1) El príncipe (ejecutivo, presidente primer ministro o autoridad a cargo del estado), es quien y donde se conciben las políticas del estado.
2) El ejército (fuerzas Armadas) donde descansa el monopolio de la fuerza por

41 Se refiere a los dos tratados de paz firmados el 24 de octubre de 1648 en Osnabrück y Münster, en la región histórica de Westfalia, evento que determinó el fin de la guerra de los Ochenta Años entre España y los Países Bajos así como la guerra de los Treinta Años en Alemania. Para este trabajo se considera este evento como el origen del estado moderno, caracterizado por el concepto de soberanía nacional e integridad territorial. (Martin G. , 2015)

parte del estado, y a través de ellas se ejecuta la política exterior apoyado sobre su fortaleza, que puede incluir el conflicto armado.

3) El pueblo (la sociedad): es quien afronta los costos y las consecuencias de estas acciones. Sin embargo, la falta de fondos en las arcas del estado para sostener sus políticas obligó muchas veces al ejecutivo a recurrir a los préstamos de la burguesía, ingresando esta clase social en la órbita del gobierno, lo cual comienza a ampliar las bases de este pilar, que en la actualidad han crecido de tal manera que su opinión muchas veces dirige las decisiones de la política.

Desde Westfalia, la violencia ha sido un monopolio del estado. Sin embargo, es en este período donde las guerras han sido las más virulentas y la humanidad se ha visto expuesta a los mayores niveles de violencia no solo física, sino también psicológica (Mc Fate, 2019, pág. 192).

Así, los conflictos actuales, comienzan a adquirir características distintivas que difieren de los que llamamos convencionales. La asimetría deja de ser una ventaja del fuerte y la estrategia del débil en varias oportunidades ha terminado en la derrota del fuerte, no en el plano militar propiamente dicho, sino que pese a su superioridad este no logra alcanzar el objetivo final de imponer la voluntad propia sobre el adversario.

> Desde la Segunda Guerra Mundial, milicias indigentes sin entrenamiento, de baja tecnología y armadas con armamento primitivo, han frustrado los planes de monstruos militares, de forma rutinaria. Francia fue derrotada en Argelia e Indochina, Gran Bretaña en Palestina y Chipre, URSS en Afganistán, Israel en el Líbano y Estados Unidos en Vietnam, Somalia, Iraq, Afganistán. Hacer la guerra de la misma manera en el futuro, no es la respuesta. (Mc Fate, 2019, pág. 9)

Conclusiones como las expuestas dieron origen a muchos estudios sobre el conflicto moderno y sus características: el primero fue el artículo de Lind y otros, denominado "El rostro cambiante de la Guerra" (Lind, Nightengale, Schimtt, Sutton, & Wilson, 1989, págs. 2-11) y en 1991, Martin Van Creveld escribe "La transformación de la Guerra" (Van Creveld, 1991). Este autor realiza un compendio de los conflictos modernos y propone al lector una serie de reflexiones acerca del drama humano de la guerra donde trata los problemas de la guerra convencional, la nuclear y la que él llama de baja intensidad, considerando el surgimiento de esta última, como el adalid del conflicto moderno. En sus capítulos, el libro plantea todos los aspectos filosóficos acerca de "qué se trata la guerra, cómo se pelea y porqué". Para finalizar revisando lo que él ve como la guerra del futuro.

Pocos años después, Toffler escribiría acerca de "Las guerras del futuro" (Toffler A. &., 1994, pág. 111), donde desarrolla, a partir de las ideas expuestas en "La Tercera Ola", todo un planteo acerca del valor de la información, su empleo en la guerra y las características del futuro "cuerpo de oficiales". El libro parte de los éxitos de la Batalla Aeroterrestre contra IRAK en 1991, y es tomado como el modelo de la batalla "inteligente". Sin embargo, sus líneas advierten que ni las fuerzas, ni

la política se encuentran preparadas para el conflicto. Estaba bien para la era del conocimiento, pero dejaba abierta una serie de reflexiones que hoy son parte inexorable del conflicto moderno.

La evolución del conflicto no puede ser separada de la evolución del conocimiento humano y el pasaje del tiempo. A modo de síntesis se presentan ciertos hitos que son representativos de cambios trascendentales, para la vida de Occidente.

En el siglo V AC, aparece la filosofía como ciencia de ciencias, definiendo al "hombre como animal racional", frase atribuida a Aristóteles. El nacimiento de Cristo establece un cambio en la medición del tiempo aceptado de manera general. La *Revolución Francesa* y su impronta no solo afecta en el desarrollo de los conflictos a partir de los conceptos napoleónicos, sino que también altera las perspectivas y creencias de la humanidad, la deidad deja de ser el eje de la noción de trascendencia humana. El centro de la escena deja de lado la figura divina en la vida del hombre y se debilita la familia donde el vínculo espiritual se desarrolla.

La Revolución Francesa marca un quiebre para esta visión humana, más allá que Nietzsche tardará algunos años (Siglo XIX) en expresar su frase "Dios ha Muerto" (Nietzstche, 2011, pág. &125)[42]. El ateísmo que se inicia en este proceso revolucionario inicia su madurez en el siglo XVIII con el nacimiento de la Ilustración, donde la ciencia, la razón y el progreso florecen entre los intelectuales y el ateísmo más que una moda se constituye en un elemento que destaca el saber científico.

La religión y la idea de Dios concebida y ya estructurada en Occidente, iniciada con la filosofía platónica, socrática y consolidada por San Agustín, se van destruyendo sistemáticamente. En este período, estos conceptos filosóficos, son resquebrajados en sus cimientos y el sentido de trascendencia desgarrado, apreciándose como falsa la cultura consolidada en dos milenios de historia para concluir "Nuestra existencia no es más que un cortocircuito de luz entre dos eternidades de oscuridad" (Nabokov, s.f.).

Más allá de las declaraciones del ateísmo moderno, el hombre sigue siendo un ser espiritual y necesita de esta conexión. Sin embargo, este naciente período sacude en forma trascendente los cimientos de Occidente y ya nada puede volver a ser lo mismo. La filosofía busca en la propia vida del hombre la plenitud, razón de ser y la realización sobre sí mismo. El mundo cambia de una visión teocéntrica a una completamente antropocéntrica centrada en el hombre. La idea de pertenencia ya deja el concepto de patria (nación) y pasa a ser el estado consolidado en la llamada *Paz de Westfalia,* sobre una base trinitaria (Príncipe, Ejército y Pueblo): esta organización es

42 Entender la muerte de Dios, como la incapacidad de actuar como fuente del código moral o teleológico, al menos como parte, del progreso del conocimiento científico. Para el hombre del siglo XIX ya no resulta posible creer honesta y razonablemente en Dios, (parece que Nietzsche se está haciendo cargo de la expansión del ateísmo entre la intelectualidad moderna, que lo interpreta como un fenómeno irreversible, que no tiene vuelta atrás). Es en Aforismo 357 donde plantea el problema de la existencia y el nihilismo cuando expresa "tan pronto como rechazamos lejos de nosotros la interpretación cristiana y consideramos su "significado" como moneda falsa, nos asalta la pregunta de Schopenhauer de la manera más terrible: ¿tiene la existencia algún sentido? Cuestión que necesitará varios siglos para ser percibida en toda su profundidad., estos varios siglos ¿nos han alcanzado? (Nietzstche, 2011, pág. &357)

el eje de la vida ciudadana, la familia comienza a dejar su concepto ampliado para migrar a un concepto de *familia nuclear* como expresa Toffler en su libro *La tercera Ola* (Toffler A., 1980).

Así transcurre el desarrollo humano donde la muerte de Dios ha puesto su mirada sobre el hombre como nuevo sol que ilumina la vida humana. El mismo Nietzsche habla del superhombre (Nietzsche, 2012), como el hombre sin barreras que se desarrolla ya sin Dios en completa plenitud. En este período, las ideas, el conocimiento y la tecnología avanzan a pasos rápidos. Podríamos decir que hoy estamos transcurriendo la última inflexión en una curva de crecimiento exponencial del conocimiento y el desarrollo tecnológico.

Es en este punto exactamente donde se detiene el análisis. Han pasado más de 300 años desde la Revolución Francesa y se podría asumir que la concepción antropocéntrica del hombre como nuevo dios de la existencia se encuentra consolidada, por sus obras y sus promesas. El siglo XXI inicia con un nuevo ambiente de vida, el ciberespacio, la promesa de un futuro cada día mejor asoma con la nueva revolución tecnológica, donde la robótica, la inteligencia artificial y la computación cuántica prometen un nuevo[43] paraíso, en un transhumanismo[44] que no logra consolidarse.

El ciberespacio como un nuevo ambiente virtual, se concibe a partir de la interconectividad de sistemas informáticos: software, redes de comunicación de todo tipo, cuya existencia concreta surge de la disponibilidad de tiempo que el ser humano le otorga. Desde su origen a la actualidad, en el ciberespacio se han ido desarrollando todas las facetas de la vida humana desde el contacto más sencillo hasta las transacciones más complejas, pasando por la actividad creativa, lúdica, educativa, investigativa y toda actividad que el ser humano realice y que sea posible de ser llevada a cabo en este nuevo ambiente que constituye un mundo virtual, del cual *metaverso*[45], hoy es su expresión más audaz.

La virtualidad es un elemento inmaterial. La era del *dataismo*[46] está dada por la capacidad de procesamiento de información y los softwares asociados. El ciberespacio es un ambiente nuevo adonde las personas se sienten muy cómodas y cuyas características son:

---

43 El concepto de nuevo obedece al fracaso de la globalización como promesa de un mundo mucho mejor y más perfecto. Se entiende por globalización, en ocasiones denominada mundialización, al proceso económico, tecnológico, político, social y cultural a escala mundial que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo, uniendo sus mercados sociales a través de una serie de transformaciones sociales y políticas que les brindan un carácter global.

44 Trashumanismo: es un movimiento cultural e intelectual internacional que tiene como objetivo final transformar la condición humana mediante el desarrollo y fabricación de tecnologías ampliamente disponibles, que mejoren las capacidades humanas, tanto a nivel físico como psicológico o intelectual.

45 Metaverso: entornos donde los humanos interactúan e intercambian experiencias virtuales mediante uso de avatares, a través de un soporte lógico en un ciberespacio, el cual actúa como una metáfora del mundo real, pero sin tener necesariamente sus limitaciones.

46 Dataísmo término empleado para describir a partir de los datos una filosofía, creada por el significado emergente del big data, la inteligencia artificial y el internet de las cosas. (Brooks, 2018)

1. La privacidad no existe. Mientras que no poseer redes sociales, cuentas de correo, etc. pareciera convertir a una persona en sospechosa, por otra parte, el exponerse ampliamente en las redes abre la posibilidad de ser observado por un tercero no deseado, actividad que con diferentes fines realiza un individuo vulgarmente denominado hacker, aunque verdaderamente es un delincuente.
2. La virtualidad ha invadido todos los ámbitos de la vida. Prácticamente no existe actividad, incluso las más íntimas, que no puedan ser realizadas en el mundo virtual. Hasta el deporte se ha virtualizado y los llamados *gamers*, constituyen una nueva forma de ídolo.
3. Es un ambiente agradable donde el individuo se siente bien porque en el espacio virtual no existe el rozamiento, puede realizarse e ir más allá de sus propias limitaciones.
4. Es fuente de peligros, desenvolverse en un nuevo ambiente requiere un proceso de aprendizaje. Así, por ejemplo, antes de salir al mundo terrestre los niños aprenden a caminar, se les enseña a cruzar la calle, se los advierte ante el peligro de tratar con desconocidos; antes de ir al mar, se aprende acerca de los riesgos que ello implica, se desarrollan destrezas como nadar, se determinan ciertas reglas que regirán de alguna manera la interacción en el agua; cuanto más severo y complejo se vuelven las exigencias, si lo que se pretende es desenvolver su actividad en el aire, donde ya no resulta posible hacerlo sin una preparación física, intelectual y las certificaciones correspondientes; más exigencias, reglas y pruebas si se trata es la actividad espacial la más compleja y selectiva. Nada de esto sucede para ingresar al ciberespacio, ello se debe a 2 razones: la primera, lo ignoramos "nadie puede dar lo que no tiene", la segunda es que ello demanda tiempo que el mismo ciberespacio consume.

Podríamos entonces llegar a concluir que: la ignorancia es la base de la derrota, mientras que la victoria es sinónimo de conocimiento.

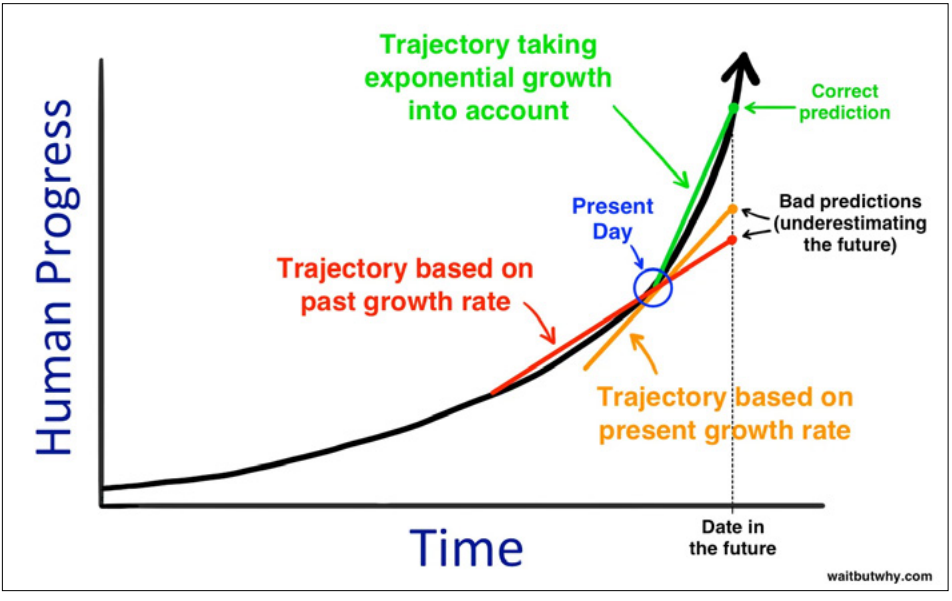
En la actualidad, podríamos afirmar con baja probabilidad de error que el conocimiento de la humanidad ha crecido y crece a una velocidad que resulta difícil de explicar. En gran parte es porque la globalización ha puesto los conocimientos al alcance de la mano de todo aquél que pueda acceder al mundo virtual. Ello produce un efecto sinérgico donde el conocimiento florece desde diferentes perspectivas en distintas partes del mundo (Zavaleta Mercado, 2014).

Hechos como el posible empleo de la inteligencia artificial (IA) para cambiar el humor de una población hasta incluso influir para llegar a dar vuelta una votación (Confessore, 2018) han expuesto 2 aspectos para analizar:

1) El potencial de la inteligencia artificial (IA) para influir en el ser humano.
2) La falta de capacidad del ser humano para hacer uso de su libertad en las decisiones.

La capacidad de la IA se encuentra recién en sus primeras fases de desarrollo. La ilustración permite observar un detalle de cómo crece el conocimiento[47] y habla de la denominada singularidad tecnológica[48], de acuerdo con el libro *The Tecnological Singularity* de Shanahan.

ILUSTRACIÓN 12 . **Progresión Humana X Tiempo**



FUENTE: (URBAN, 2015).

La idea de que la historia de la humanidad se está acercando a una *singularidad* —donde algún día los seres humanos comunes serán superados por máquinas artificialmente inteligentes o inteligencia biológica mejorada cognitivamente, o ambas— ha pasado del ámbito de la ciencia ficción al debate serio. Algunos teóricos de la singularidad predicen que si el campo de la inteligencia artificial (IA) continúa desarrollándose al ritmo actual, la singularidad podría surgir a mediados del presente siglo (Shanahan, 2020).

De hecho, el concepto de singularidad tecnológica ya cuenta con su propia universidad (Singularity Group, 2022),la cual da notables muestras de las ventajas que este

47 Otras similares gráficas con información adicional pueden encontrarse en: http://www.edwinhrydberg.com/what-is-the-technological-singularity-and-why-should-you-care/ o en https://www.newworldai.com/what-is-technological-singularity/

48 Singularidad Tecnológica: es el momento en que la inteligencia artificial y la robótica alancen capacidades similares a las humanas. En otros ámbitos se pueden encontrar definiciones como “Es la noción de que las máquinas pueden llegar a ser más inteligentes que los humanos” (Polansky, 1965).

hito traerá a la humanidad. No hace más de 30 años, la globalización y sus efectos también fueron pintados como el paraíso en la tierra. El concepto de Nietzsche del superhombre pareció alcanzarse y en gran medida así fue, pero de su mano también llegaron grandes miserias y nuevos problemas, formas y métodos de conflictos. En este caso la IA ya ha mostrado los primeros vestigios de su capacidad, con desarrollos que permiten perfilar la personalidad de un individuo y a partir de ella inducirla o influenciarla para que se oriente en una determinada dirección.

Quizás el caso más resonante en este sentido sea el denominado *Cambridge Analityca,* donde se discute la posibilidad de haber influenciado en el humor popular de la sociedad de los EE.UU. (50 millones de usuarios), hasta el punto de haber sido explicado como uno de los factores determinantes del triunfo del expresidente Donald Trump. Pero el caso no se agota allí, sino que pareciera también tener ciertas implicancias en el Brexit del Reino Unido (Rosenberg, Confessore, & Cadwalladr, 2018)[49].

¿Cómo funciona? de acuerdo con el Dr Uzal, perfilar una persona requiere aproximadamente unos 15.000 data items[50] (UZAL, 2021). Más allá de su definición y en simples palabras: un data ítem es un acceso al ciberespacio para ejecutar una transacción cualquiera. Así cuando se da un *like* en Facebook, ingresa al banco, o se mira determinadas noticias, se asiente a la opinión de un amigo en una red social, se está construyendo un *data ítem.* En el resonante caso mencionado esto se consiguió en gran medida a partir de los datos obtenidos de Facebook. Un desarrollo interesante acerca de la forma de recolección puede ser accedido en el artículo del New York Times *You Are the Product': Targeted by Cambridge Analytica on Facebook* (Dance & Rosenberg, 2018) que explica cómo funcionaba la recolección de datos por parte de *Cambridge Analytica* en Facebook (Gonzáles, 2018).

Lo aportado hasta ahora permite explicar el potencial de la IA para influir en el ser humano. Si volvemos a la temática del conflicto, el ambiente operacional donde se desarrolla es el cibernético y el objetivo es el hombre. El *Global Trend* 2040, explica que:

> ...la IA del futuro requerirá cantidades masivas de datos para operar de manera eficiente y competitiva. Las instituciones, las empresas y los países que ya invierten en formas de adquirir, clasificar, almacenar y monetizar datos tendrán ventajas. Las cantidades sin precedentes de datos disponibles en 2040 proporcionarán información y capacidades valiosas, pero también abrirán el acceso, la privacidad, la propiedad y el control de los datos como áreas de competencia y con-

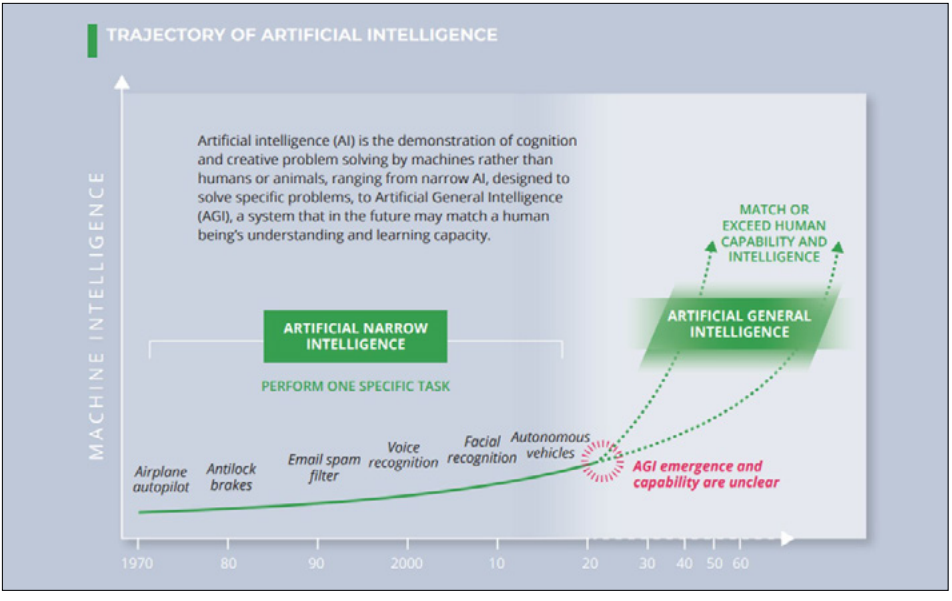
49 Algunos detalles pueden encontrarse en el artículo del New York Times: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Confessore, 2018).

50 Data Ítem: es una sola unidad de datos en un registro de almacenamiento. Este término puede referirse específicamente a la unidad de información más pequeña posible o, de manera más general, a una sola entrada o campo. El contexto suele proporcionar información sobre el significado. Los elementos de datos se almacenan en bases de datos informáticas de diversas formas y pueden protegerse para restringir el acceso o dejarse sin protección para que estén fácilmente disponibles para cualquiera que desee acceder a ellos. (McMahon, 2006)

> flicto crecientes. Las nociones actuales de privacidad seguirán evolucionando, ya que las personas necesitarán compartir más información personal para acceder a las aplicaciones y el seguimiento se volverá omnipresente. Es probable que los gobiernos autoritarios exploten el aumento de datos para monitorear e incluso controlar a sus poblaciones. Además, muchas empresas y organizaciones también tendrán herramientas poderosas, como la manipulación de videos o falsificaciones profundas, para mejorar el marketing personalizado o avanzar en una narrativa particular. Las aplicaciones emergentes de IA también pueden convertirse en objetivos potenciales para la manipulación de datos para sesgar su salida. (DNI, 2021, págs. 59-60)

Es aquí donde se plantea el inicio de una crisis acerca de la visión, hoy antropocéntrica del hombre, debido a que de manera no perceptible se encuentra nuevamente en una dimensión completamente intangible como es el ciberespacio y con un ser cibernético que es la IA que prácticamente sabe todo de nosotros y nos atiende como seres únicos e irrepetibles a quienes está consagrada. Luego de poco más de 500 años de reinado del hombre como dios, donde la familia nuclear tiene su relevos en el individuo aislado (Amoroso, 2018) y el concepto de estado se diluye en las nuevas generaciones X, Y y milenials donde prima lo internacionalista y la economía del individuo (Ney Fajardo, S/F), parece que la humanidad en su necesidad de espiritualidad y atención divina, está encontrando como resultado de su propia invención un reemplazo de la espiritualidad

ILUSTRACIÓN 13 . **Trayectoria de la Inteligencia Artificial**



FUENTE: (DNI, 2021, PÁG. 58).

en la virtualidad. Sin embargo, el reemplazo de Dios por la IA tiene objetivos muy diferentes: el primero nos otorga y respeta nuestro libre albedrío, mientras que el segundo tiene por objeto controlar nuestras vidas y orientar las decisiones.

A modo de conclusión se puede expresar que: la capacidad que posee la IA de poder perfilar al ser humano adecuadamente permitirá influir y llegar incluso a controlar sus decisiones.

2. **El ciberespacio y las áreas de acción**

Para el desarrollo de este título se tomará como definición del ciberespacio la que presenta el proyecto de Glosario de Términos de Empleo Militar para la Acción Militar Conjunta de 2015:

> Ámbito virtual en el que se desarrollan actividades de procesamiento, almacenamiento y explotación relacionadas con los datos e información digital, a través de redes interdependientes e interconectadas, software, firmware de dispositivos, cuyo carácter distintivo está dado por el empleo de las tecnologías de información y comunicaciones. (EMCO , 2015, pág. 42)

2.1. **Normas Legales y Organizacionales de la República Argentina relacionadas con el Ciberespacio**

Bajo este título se concentra diferentes aspectos normativos que ya rigen en nuestro país en relación con las actividades en el ciberespacio

2.1.1. Directiva Política de Defensa Nacional (DPDN)

Por medio del decreto 457 de 2021 se dictó directiva política de máximo nivel de la República Argentina, la cual que contiene una serie de aspectos relacionados con la cuestión ciberespacial centrados en la ciberdefensa. Al respecto, se destacan algunas precisiones de interés.

> El Ministerio de Defensa deberá incluir el desarrollo doctrinario, planeamiento, diseño y elaboración de la política de ciberdefensa en el nuevo "Ciclo de Planeamiento de la Defensa Nacional. Fortalecer el Sistema de Ciberdefensa. ... Fortalecer los vínculos internacionales y en la región, para el desarrollo de una capacidad soberana en materia de infraestructura de comunicaciones y ciberdefensa…Participar en ámbitos de discusión institucionales referidos al derecho internacional aplicado al ciberespacio…Desarrollar el objetivo operacional del Sistema de Ciberdefensa, consistente en la observación, vigilancia y control de la actividad que acontece en la infraestructura de tecnología informática de las redes del Sistema de Defensa Nacional y de las infraestructuras de la información que le sean asignadas, con el fin de prevenir y contrarrestar incidentes provenientes del ciberespacio…Deberán desarrollar los componentes sistémicos que contribuyan al logro de ese objetivo primario. (PEN Dto457/2021DPDN, 2021)

2.1.2. Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional con el consenso del conjunto de la sociedad en forma multidisciplinaria y multisectorial, sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio. Su finalidad es brindar un contexto seguro para su aprovechamiento por parte de las personas y organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo acorde (Comité de Ciberseguridad, 2019).

2.1.3. Organismos de ciberdefensa y ciberseguridad

Los organismos que se han creado hasta el momento en relación con el ciberespacio y sus misiones son:

> Comité de Ciberseguridad: Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional. Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad. Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado. Impulsar el dictado de un marco normativo en materia de Ciberseguridad. Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales. Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden. (PEN Dto 577/2017, 2017)

> Comando Conjunto de Ciberdefensa: Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar. (Cdo Cjto de Ciberdefensa, S.f.)

> Dirección Nacional de Ciberseguridad: Diseñar políticas que brinden protección a las infraestructuras críticas de información, generando y mejorando las capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática en el nivel nacional. Esta Dirección ha generado un Centro de Respuesta ante emergencias informáticas(CERT). (D.N. de Ciberseguridad, S.F.)

2.1.4. Legislación Argentina en ciberdefensa y/o Ciberseguridad

> Ley 26.388 de Delito informático: esta norma amplia el código penal incluyendo el concepto de delito informático en varios artículos. (PEN Ley 26.388, 2008)

Ley 25.326 de Protección de Datos Personales: trata sobre los derechos de la persona sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. (PEN Ley 25.326, 2000)

Decreto Reglamentario N° 1558/2001: Reglamentación de la protección de los datos personales (PEN dto 1558/2001, 2001)

Ley 25.506 de Firma Digital: Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina (PEN Ley 25.506, 2001)

Decreto Reglamentario N° 2628/2002: Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional. (PEN Dto 2628/2002, 2002)

Ley 26.904 de Grooming: es un delito de una persona adulta contra una niña, niño o adolescente. Hay grooming cuando una persona adulta acosa por internet a una niña, niño o adolescente para cometer delitos sexuales. Acosar es perseguir y molestar de manera repetida a una persona. (Ley 26.904, 2013)

2.1.5. Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad

Decisión Administrativa 641/2021: requisitos seguridad de la información para organismos públicos (JGM Dec Adm 641/2021, 2021)

Resolución 1107-E2017: Comité de Respuesta de Incidentes de Seguridad Informática del Ministerio de Seguridad (MS Res 1107-E/, 2017)

Resolución 580/2011: Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad. (JGM Res 580/2011, 2011)

Disposición ONTI 3/2013. Política Modelo de Seguridad de la Información. (ONTI Dispo 3/2013, 2013)

Resolución 1523/2019: Definición de Infraestructuras Críticas. (JGM Res 1523/2019, 2019)

2.1.6. Otras normativas relacionadas a la ciberseguridad

Resolución 829/2019: La Estrategia de Ciberseguridad sienta principios básicos y objetivos fundamentales para el desarrollo de previsiones (normas, planes, políticas y acciones concretas) en materia de protección del Ciberespacio en el nivel nacional y en beneficio de la Nación, tendientes a brindar un contexto seguro para su aprovechamiento. (JGM Res 829/2019, 2019)

2.2. La estrategia Militar y las operaciones cibernéticas

En el ciberespacio encontramos tres (3) dimensiones: la *material* integrada por la geografía, los sistemas de infraestructuras, hardware, computadoras, conectores, *routers*, entre otros. La lógica que es, básicamente, la interconexión de los componentes físicos mediante protocolos específicos de funcionamiento que obedecen al diseño algorítmico empleado y software con fines de procesamientos de datos e información. Finalmente, la *humana*, real y a la vez abstracta. Debería entenderse que la palabra correcta es virtual, entendiendo por tal a la persona que dispensa su tiempo y atención y da vida real al ciberespacio haciendo de este un ámbito propio del proceso cognitivo del ser humano.

Estas dimensiones, que permiten que en el ciberespacio interactúen la energía eléctrica, infraestructuras, software, transporte, información y personas (JID, 2020, pág. 17), constituyen el ámbito donde se desenvuelve la guerra cibernética, que para su adecuada acción requiere:

1. Una clara comprensión de la composición de las redes de información y comunicación, así como la interacción de éstas en los diferentes niveles: interno, local, metropolitano y global, identificando las vulnerabilidades para desarrollar las herramientas que permitan anular, mitigar, reducir o al menos advertir la posibilidad de que sean explotadas por alguien. En términos generales, podemos ubicar aquí las acciones de la ciberseguridad
2. Desarrollar y operar sistemas que permitan la vigilancia y control[51], de sistemas basados en Tecnologías de la Información (TI /IT), como en Tecnologías de la Operación (TO/OT)[52]. En este sentido lo relacionado con:

---

51 Se entiende por vigilancia la capacidad de poder advertir cualquier anormalidad en el flujo de datos e información ya sea por razones de tipo física (operaciones electromagnéticas) o lógicas (programas de los denominados *malware*). El control es la capacidad del sistema para normalizar la situación detectada. Se puede lograr a partir de una situación de supremacía, superioridad, paridad, por degradación y/o incapacitación. La capacidad de Vigilancia y Control en los sistemas cibernéticos es función de la resiliencia de los mismos a las agresiones a los que son sometidos.

52 La Tecnología de la Información se caracteriza por la aplicación de equipos de telecomunicación como ordenadores para tratar datos. IT Suele utilizarse en el ámbito de los negocios y las empresas. En cambio, la Tecnología de las Operaciones está dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas. (oasys, 2022)

a. TI /IT: permiten las acciones y tareas para generar o evitar los efectos de la *comunicación estratégica enemiga*[53].
b. TO/OT: desde la perspectiva estratégica se encuentran relacionadas de manera directa con las infraestructuras críticas. Permiten operaciones Defensivas (pasivas y activas), de Explotación (pasivas en ámbito propio y activas en ámbitos adversarios) y Ofensivas de respuesta y preventivas. Todas son consideradas en occidente en el marco de un conflicto declarado.

3. En el ambiente operacional, en tal sentido la Guía de Ciberdefensa de la Junta Interamericana de Defensa dice: "Un ámbito de operaciones es el entorno de interés e influencia en el que se llevan a cabo actividades, funciones y operaciones para cumplir la misión y ejercer control sobre un oponente con el fin de lograr los efectos deseado". Que cumple con los criterios: (1). Requiere capacidades únicas para operar en ese ámbito. (2). No está totalmente abarcado por ningún otro ámbito (tierra, mar, aire, espacio). (3). Se caracteriza por una presencia compartida de capacidades aliadas y adversarias. (4). Es capaz de ejercer control sobre un oponente a través de la influencia y el dominio. (5). Brinda oportunidades de sinergia con otros ámbitos. (6). Proporciona oportunidades asimétricas entre todos los ámbitos. (JID, 2020, pág. 23)

La Estrategia Militar (EM) se ve impactada por la TI/IT en lo referente a operaciones del ámbito cognitivo, de información e influencia. Mientras que el aspecto operacional se ha desarrollado una gran dependencia de las TO/OT, particularmente para cuestiones como: (1) Comando y Control, (2) Inteligencia Vigilancia y reconocimiento, (3) Logística, (4) operación conectividad entre los diferentes sistemas de armas, operadores y decisores, llevando las necesidades de ciberdefensa en la guerra a una dimensión de tiempo real que asegure a las TI/IT, trabajar con una perspectiva con ciertos niveles de seguridad en los sistemas.

Un ejemplo más emblemático de esta capacidad, es la operación "Lanza de Neptuno" (9/11 memorial, S.F.) , que acabó con la muerte de Osama de Bin Laden[54], donde la estrategia nacional se encontraba en directa conexión con el operador táctico. Esto también despierta ciertos interrogantes sobre las responsabilidades que la EM debe delegar en el nivel operacional.

---

53 Comunicación estratégica militar enemiga, es la acción que realiza un adversario sobre el sistema propio producto de un planeamiento no lineal, ni secuencial, con un diseño y planificación basados en estudios detallados de los intereses nacionales que se fijen (*targeting*) y de las características del objetivo seleccionado o área de poder o componente que se desea afectar (*weaponeering*), sobre las que se aplicarán diferentes combinaciones de actividades relacionadas con la dimensión la información, la capacidad de incidir toma de decisiones, la manera en que el elemento afectado enemigo absorbe esa información, en el entorno electromagnético, todas dimensiones propias de la Comunicación Estratégica, que son coordinadas sinérgicamente para el logro de objetivo político

54 Esta operación se la conoce también como "Gerónimo" que fue el código para informar la muerte en acción del líder terrorista.

Asociados con las ventajas que otorgan las TICs, se identifica la interconexión de miles de dispositivos en el ámbito cibernético, donde, según Javier M. Gil, se aprecia que: (1) se dificulta sostener y actualizar los sistemas de cibernéticos; (2) surgen problemas en el análisis de las posibles vulnerabilidades; (3) los nuevos dispositivos amplían la posibilidad de nuevas focos de infección; (4) existencia de daños colaterales como consecuencia del empleo de dispositivos cibernéticos (ej.: alteración de las señales de posicionamiento), (5) hay una necesidad de desarrollo permanente de nuevos algoritmos y dispositivos (Gil, 2017). Al respecto:

> Los ataques son constantes y están creciendo en frecuencia e intensidad. Pueden destruir estructuras físicas y sistemas operacionales, paralizar ciudades y generar millonarias pérdidas, inclusive costar vidas. Pero los instrumentos de todo este caos no son balas, bombas o tanques; son «bits y bytes»... «Los ataques cibernéticos serán un componente significativo de cualquier conflicto futuro, ya sea que involucren naciones principales, estados paria o grupos terroristas». (Lynn III, 2011).

> Los gobiernos occidentales no han logrado comprender completamente la vulnerabilidad de las comunicaciones electrónicas y los enormes riesgos que esto representa para la infraestructura crítica, el transporte y la protección de civiles. (Stupples, 2015)

Una adecuada comprensión del ámbito ciberespacial y sus características y permitirá definir con las actuales capacidades militares en otros dominios y las restricciones legales que imponga el estado para la dimensión operacional poder determinar los efectos a alcanzar como: dominio superioridad, vigilancia control, exploración, explotación entre otras que puedan definirse.

Para el caso de nuestro país el problema de la ciberguerra en el ámbito de la estrategia militar y en tiempo de paz se limita a las acciones de ciberdefensa relacionadas con las infraestructuras críticas del sistema de Defensa Nacional.

Aquí es importante notar las diferencias culturales entre oriente, los soviéticos y occidente, según diferentes autores:

1. Para los orientales, el conflicto es permanente y no posee limitaciones, esto es expresado claramente a lo largo de todo el libro de los coroneles Qiao Liang y Wang Xiangsui La guerra más allá de los límites. (Qiao & Wang,, 1999).
2. En el caso de los soviéticos y occidentales:

   > La entrada de «guerra de información» (informatsionnaya voyna) en un glosario de términos clave de seguridad de la información, producido por la Academia Militar del Estado Mayor General, hace una clara distinción entre la definición rusa –amplia, y no limitada a los tiempos de guerra– y la occidental –que la describe como limitada a operaciones de información tácticas llevadas a cabo durante las hostilidades. (Gil, 2017, pág. 13).

3. Para el caso de occidente: "Las ciber-operaciones ofensivas son aquellas ejecutadas, en el marco de un conflicto declarado, en las redes de adversarios o de terceros con la finalidad de causar un ciber-efecto o un efecto físico" (JID, 2020, pág. 43). Nótese que occidente considera una clara diferencia entre tiempo de paz y de guerra donde la crisis debe definirse en una contienda establecida para hacer efectivas las operaciones cibernéticas de explotación ofensiva o de orden ofensivo propiamente dicho.

En tal sentido cabe la pregunta ¿en este nuevo dominio, caben los principios tradicionales de la guerra o deben ser definidos nuevos principios, propios de él?

En razón de ser el ciberespacio un dominio virtual, creado por el hombre, bajo un concepto bastante caótico, particularmente si se considera la "Declaración de Independencia del Ciberespacio"[55] (Barlow, 2018), no posee fronteras físicas o políticas y, además, muta y se transforma; esta condición demanda la constante evaluación y supervisión de las capacidades a fin de determinar los niveles de eficiencia necesarios y suficientes para decidir, si los principios aplicados tienen vigencia o no, de acuerdo con el ambiente cambiante y las múltiples posibilidades defensivas u ofensivas que se pueden generar. Consecuentemente, el concepto de dominio capacidad para ejercer superioridad, control, influencia y competencia, podría obedecer a principios de la guerra diferentes de los fijados para las fuerzas tradicionales.

Otro aspecto a considerar por la estrategia militar es el grado de participación del sector privado que cuenta con una amplia gama de recursos materiales, humanos y financieros necesarios para monitorear una porción de lo que acontece en este ambiente. Parte de las infraestructuras críticas se encuentran bajo el control privado[56], por lo cual la coordinación y la sinergia con este sector resulta esencial. (CEEP Think Tank Ejército del Perú, 2019). En tal sentido la Guía de Ciberdefensa producida por la Junta Interamericana de Defensa dice: "Una significativa cooperación regional e internacional ha surgido en torno a la ciberseguridad entre los gobiernos de las Américas durante la última década, sin embargo, gran parte del progreso se ha centrado principalmente en las instituciones civiles" (JID, 2020, pág. 5).

Una posibilidad a explorar como estrategia de integración civil-militar es desarrollar un concepto de Poder Ciberespacial Nacional, que involucre y coordine esfuerzos sinérgicos de todas las áreas.

---

55 La Declaración de independencia del ciberespacio es un texto presentado en Davos, Suiza el 8 de febrero de 1996 por John Perry Barlow, fundador de la Electronic Frontier Foundation (EFF).

56 Ejemplo: Las estaciones de amarre de los cables submarinos por donde llega el grueso del tráfico de internet a la RA se encuentra en Las Toninas: el Atlantis II, manejado por un conglomerado de más de 15 empresas, atraviesa el Atlántico hacia África y Europa. Por último, el Unisur (también de Telxius) nos conecta con Brasil y Uruguay, y el Bicentenario (de Antel Uruguay y Telecom Argentina) solamente se dirige hacia este último. Por fuera del anclaje de Las Toninas, ARSAT tendió una fibra óptica submarina para atravesar el Estrecho de Magallanes y conectar Tierra del Fuego. (nic.ar, 2018)

La estrategia militar, debe considerar en su enfoque el alcanzar una alta capacidad de conciencia situacional[57], que le permita coordinar las operaciones defensivas, de explotación y con el sector privado, minimizar la ofensiva adversaria que intentará explotar las debilidades de la base tecnológica y las infraestructuras críticas de orden energético, transporte, logístico, financiero, propios (JID, 2020, pág. 88).

En este sentido, la definición de las operaciones en el ciberespacio, constituyen un punto inicial de apoyo para definir la doctrina de empleo del poder militar, insumo crítico para que el nivel político del Estado responsable determine el marco legal que le dará la legalidad para que se pueda definir la estructura, organización y funciones militares en este espacio; este es un trabajo conjunto entre los expertos militares, el sector privado y los poderes ejecutivo y legislativo, aspecto que otorga legitimidad.

En el caso argentino, se ha avanzado en diferentes normas legales y organizacionales, que resultan una base para la formulación de una doctrina para acción militar conjunta en el ciberespacio.

La Estrategia Militar en el ciberespacio podría ser diseñada considerando como base algunas líneas de líneas de trabajo, como:

1. Propósito: Asegurar la capacidad de operación de los sistemas propios, contra cualquier intrusión, así como la calidad claridad y oportunidad de los datos y la información que en ellos circula cerrando las brechas existentes, facilitar la adecuada explotación de la información entre los diferentes ambientes y la capacitación de los RR.HH. que componen el sistema.
2. Ambiente: el ciberespacio de operación propio debe ser gestionado para alcanzar un adecuado nivel de resiliencia, los diferentes niveles ciberespaciales, debe ser seguro a las acciones sobre los datos o la información que dispone en todo el complejo dominio, cerrando las brechas existentes entre los distintos niveles y tipo de redes que lo componen, permitiendo alto niveles de interoperabilidad entre sus capas asumiendo niveles de riesgo aceptable.
3. Capacidades: la estrategia de ciberdefensa debe tender a sistemas que permitan altos niveles de Conciencia Situacional, robustos ágiles, que permitan ser proactivos, resistir ataques (resiliencia), generando modelos que permitan la adecuada toma de decisiones sobre datos e información confiables y seguros.
4. Convergencia: esta estrategia debe ser convergente con el estado del arte considerando las tecnologías emergentes en el ciberespacio, como la Inteligencia artificial, la computación cuántica, los cambios que se producen tanto en los servicios de comunicaciones como en las características de las tecnologías de la información, tanto en el ámbito local como global
5. Amenazas: la estrategia militar de ciberdefensa debe generar una agenda que

57 Conciencia Situacional ciberespacial: Representación de los elementos y eventos del ciberespacio, en un tiempo, lugar y misión determinados, la explicación de su significado y la proyección de su estado futuro. (JID, 2020, pág. 15)

considere riesgos y amenazas configurando los diferentes perfiles de ataque y posibles acciones de respuesta empleando el Poder Ciberespacial Nacional.

6. Cultura: es un campo propio de la estrategia nacional, donde la estrategia militar, posee acciones concretas tanto en el nivel operacional como en el estratégico militar para la protección de sus Recursos Humanos los cuales deben ser e preparados con altos niveles de educación técnico profesional y ético-militar, que le permitan alcanzar confianza en la propia conducción y poder ignorar los intentos de influencia del adversario

2.3. **Interoperabilidad en el ciberespacio**

El ejército de los EE.UU., en su Concepto de Ciber-operaciones Plan de Capacidades 2016-2028, plantea la visión de tres capas, la física, la lógica y la social de las cuales destaca 5 componentes. En la física los componentes geográficos y las redes físicas, en la lógica los componentes de redes lógicos y en la social a las personas y a los componentes que denomina ciber-personas (avatares[58]) (US army, 2010, pág. 8).

Modelizar el ciberespacio en capas permitirá mejorar los estudios que aplique la estrategia militar para determinar aspectos éticos, estándares, gobernanza, políticas, procedimientos y comportamiento humano en cada capa y la interoperabilidad entre ellas.

La interoperabilidad, en este tipo de modelos, presenta en las capas más bajas criterios y limitaciones técnicas que provienen tanto de los servicios de redes de transporte de datos como de los servicios que proveen información, que se contraponen con las necesidades interoperabilidad de la organización ello implica la necesidad de crear capas de interacción.

Pensar un proceso de guerra cibernética desde la perspectiva ciberespacial requiere asegurar la calidad de los datos, la información, conciencia situacional y el conocimiento que permita la mejor toma de decisiones, alcanzando de esta manera una superioridad militar a partir de la superioridad de la información, un proceso que a principio del milenio se denominó como la guerra centrada en redes (*network centric warfare*[59]). En este punto se plantea la diatriba de lo seguro y lo práctico, esencia de la interoperabilidad cibernética debido a que lo muy seguro es poco práctico y lo muy práctico es poco seguro, ecuación que debe ser resuelta en el nivel técnico e implementada por la decisión estratégica en una adecuada evaluación de las fortalezas propias, las vulnerabilidades del adversario, las debilidades propias y las oportunidades

---

58 Más Información en: https://www.rd.ntt/e/ai/0004.html y https://www.researchgate.net/publication/351749807_Is_Human_Digital_Twin_Possible

59 Netwok Centric Warfare es un concepto que reside en el valor de la información y la superioridad que puede obtenerse al disponer de información precisa y relevante en el momento oportuno. Como medio para lograr dicha superioridad se plantea el uso extensivo de las tecnologías de la información y las comunicaciones, con objeto de conectar en una red común a todos los sistemas y fuerzas propias que participan en las operaciones, de forma que cada usuario pueda conocer, aprovechar y difundir la información que pueda resultar de interés en cada momento. (McConoly, 2021).

que ellas dejan para la acción del oponente, determinando claramente lo riesgos y amenazas que esa decisión involucra.

> El desafío para las fuerzas armadas transformadas y seguras es utilizar las tecnologías de la información para construir una infraestructura de sistema altamente adaptable, de alto rendimiento e interoperable que sea resistente, se degrade lentamente bajo ataque, y se reconstituya en un modo seguro mientras está bajo ataque. Para lograr este desafío, este ejército transformado necesita una mejor comprensión del ciclo de vida vulnerabilidades de las tecnologías de la información. (Richarson, 2012, pág. 28)

2.4. **Una perspectiva de modelización de la estrategia Militar**

Actualmente el Estado Mayor Conjunto, se encuentra trabajando en un concepto que se ha denominado *multicapa* y que se concentra de manera particular en el desarrollo futuro de una estrategia que finalmente se espera decante en una doctrina, que por las características del concepto expresado hasta el momento la misma es completamente afín con una actitud estratégica defensiva, llevada a cabo desde la posición del débil, en el cual los aspectos asimétricos adecuadamente conducidos pueden jugar a favor de este último.

En tal sentido en relación las capas propias del poder militar, de alguna manera pueden ser modelizadas a partir de comprender que las posibilidades del accionar militar se encuentran asociadas con los conceptos de alerta estratégica del Estado y la capacidad de alerta táctica de las fuerzas propias, en función de las capacidades y tiempos de alistamiento para actuar.

Una analogía del ser humano con adecuada capacidad de alerta, se da cuando los sentidos del individuo se encuentran desarrollados, su percepción de la realidad es óptima y, en consecuencia, le permiten una reacción oportuna y consistente. En el caso del Estado, sus sentidos están constituidos por un sinnúmero de sistemas (servicio exterior, agencias de inteligencia, agencias de noticias, agencias de estrategia, Fuerzas Armadas, Fuerzas de Seguridad y otros, con elementos como sensores espaciales, sensores electrónicos, Internet, vigilancia tecnológica, por citar algunos) que, de acuerdo con el desarrollo de su capacidad y sensibilidad, determinarán dentro del Sistema de Inteligencia y Estrategia Nacional el tiempo de aviso para la reacción del Estado a un evento determinado.

A los efectos de encontrar cuáles son las mejores soluciones para un sistema con las características del expuesto, se recurrió a la ayuda de un modelo sistémico defensivo simplificado y su funcionamiento en relación con los esfuerzos que el instrumento militar puede ejecutar. La intención es efectuar conclusiones acerca del diseño adecuado de la fuerza futura a través de modelizar de manera simplificada y la elaboración de un camino crítico contribuyente a esbozar una idea de los esfuerzos permanentes en tiempos de paz y cuáles serían los esfuerzos intensivos a realizar en periodos de conflicto. El *tiempo de reacción* constituye el insumo crítico del Servicio de la Defensa adonde las condiciones del entorno establecidas para una actitud

defensiva serán consecuencia de: (1) Un Ambiente operacional bien interpretado; (2) Lograr posiciones relativas Favorables de los medios propios; (3) Poseer un adiestramiento óptimo de los recursos humanos y (4) buscar y desarrollar la capacidad de Sorpresa. Todos ellos permiten optimizar o desmejorar el *tiempo de reacción,* factor determinante para la toma de decisiones durante el manejo de crisis.

Por otra parte, las características de los medios tendrán influencia directa para: (1) dar soporte a la diplomacia, constituyéndose en un punto de apoyo de las decisiones políticas durante los periodos de crisis y negociación, de aspectos que pudieran afectar la soberanía nacional; (2) disuadir sobre las posibilidades reales del agresor para ocupar territorio propio y (3) en caso de encontrarse ante el hecho consumado de una pérdida de soberanía dar factibilidad a la decisión política para la reconstitución de la soberanía afectada.

Como corolario de este modelo la libertad de acción del poder político será una variable con la siguiente tendencia: "A mayor inversión en medios adecuados[60] menor probabilidad de pérdida de soberanía, y mejor punto de apoyo en el ejercicio de la soberanía." (Moresi A. , 2018)

De lo expuesto hasta aquí se pueden extraer las siguientes conclusiones:

1. El tiempo de reacción requiere capacidad de penetración estratégica[61], que depende nuevamente de la característica de los medios.
2. Es necesario perfeccionar los tiempos de reacción y optimizar la alerta estratégica, desarrollando la capacidad de la defensa a través de medios Inteligencia, Vigilancia y Recogimiento (Área de Capacidad ISR) y una permanente y continua observación de los ámbitos ciberespaciales, aeroespaciales, marítimos y terrestres, optimizando los medios que constituyan la opción más rápida y procedente para conjurar cualquier intento de violación de la soberanía.
3. Los modelos sistémicos a diseñar por la estrategia militar para optimizar la Alerta Estratégica consisten en un:
   - Modelo operacional que se compone con los elementos del instrumento militar propios del nivel operacional. Si bien este elemento puede ser afectado por la guerra electromagnética y requiere protección cibernética, no constituye un aspecto propio de la presente investigación y que no es propósito de este trabajo
   - Modelo de Inteligencia, Vigilancia y Reconocimiento (ISR), es decir, al compuesto por los sensores electromagnéticos, electrópticos, infrarrojos, sonoros u otras tecnologías que permiten desde diferentes plataformas ejercer la vigilancia (no es especifico de este trabajo).
   - Modelo ciberespacial. es el objeto de trabajo, en la guerra cibernética se desarrolla en este ambiente operacional de características particulares,

60 Medios adecuados son aquellos que mejor responden a obtener un óptimo Servicio de Alerta Estratégica que se traduce en mayor tiempo disponible para la reacción para todos los sistemas.

61 Capacidad de Penetración Estratégica es la posibilidad de accionar en la profundidad del sistema adversario, sobre blancos que constituyen parte esencial a sus intereses vitales y/o nacionales

tanto en la preparación de los recursos humanos para combatir en él, como así también en las cuestiones legales, doctrinarias y los recursos materiales. Las operaciones que se ejecutan en el ciberespacio tienen capacidad proteger, de afectar directa e indirectamente la capacidad del sistema de defensa nacional propio, a la vez que permite afectar el del adversario.

4. El Sistema de Comando y Control (CyC), es donde confluyen estos modelos produciendo información clara precisa, oportuna y segura de todos los ambientes operacionales para la toma de decisiones en todos los niveles. Para el modelo operacional e ISR serán insumo del nivel estratégico operacional y táctico, mientras que los del modelo ciberespacial serán del nivel estratégico nacional y estratégico operacional. Es por ello que los Sistemas de CyC deben ser integrales horizontalmente e integrados verticalmente desde los niveles tácticos inferiores hasta los estratégicos nacionales. Esto se concibe como un sistema de Comando y Control que integra todos los ambientes.

3. **Acerca del conflicto cibernético futuro**

Los estados modernos modelados durante la *Paz de Westfalia,* mantienen el formato básico, pero las circunstancias fueron introduciendo cambios en la preeminencia de los pilares que lo sostienen; así en su principio, el mayor peso se encontraba en el príncipe y podemos decir que aún hoy continúa siendo un factor determinante la política.

En el período napoleónico y post napoleónico gran parte del peso se trasladó al ejército con derivaciones en el concepto de los estados mayores y de un cuerpo de oficiales profesionales colectivamente competente, a partir de un entrenamiento superior, conocimiento, organización y consagración al deber, definido en los escritos de Von Moltke[62]. Trae aparejado el concepto de la *nación en armas,* donde se impone en muchos estados el servicio de armas obligatorio, dirigido por un cuerpo profesional militar:

> En el siglo XIX los hombres enrolados se convirtieron en una sección entremezclada de la población nacional -ciudadanos de corazón- y los oficiales pasaron a ser un grupo profesional separado que vivía en un mundo propio... (Huntington, 1995, pág. 48)

El ejército, ya devenido en fuerzas armadas, que a través de un período de transformaciones termina convirtiéndose en lo que Huntington llama un cuerpo *profesional militar*, donde:

62 Graf Helmuth Karl Bernhard von Moltke (apodado el viejo) fue un mariscal de campo prusiano. Jefe de estado mayor del ejército prusiano durante treinta años, se lo considera el creador de un método nuevo y moderno de dirigir ejércitos en el campo de batalla

> La línea es trazada entre militares y civiles más que entre burgueses y nobles. La aristocracia del origen había sido reemplazada por la aristocracia de la educación y el logro. El oficial prusiano era pobre, experto, disciplinado y devoto. Parte Integral de una comunidad de tejido cerrado. El resultado era un sprit corporativo único en Europa. En palabras de la Comisión Educativa Militar Británica, [Huntington transcribe del Military Education (pag 168): "totalidad de los oficiales del ejército prusiano, se consideran un solo cuerpo –el cuerpo de oficiales–, unidos por vínculos y simpatías comunes y el ingreso a este cuerpo se considera a la vez algo que confiere aspectos distintivos e impone deberes peculiares". (Huntington, 1995, pág. 62)

Para cerrar y comprender esta particularidad de la profesión militar que se consolida entre fines de XIX como se la conoce actualmente, es un movimiento que se da prácticamente en todo el mundo. Huntington transcribe el informe del Gral. Upton, enviado del Gral. Sherman y el Secretario Belknap de los EEUU para estudiar la organización, táctica y disciplina de los ejércitos de Europa y Asia y particularmente del sistema alemán. Al respecto, Upton subraya en su informe que este sistema se encontraba arraigado en Europa e instaba a su inmediata incorporación en el ejército de los EE.UU. Dicho informe establece:

1. El ingreso en el cuerpo de oficiales sólo se daba por graduación de una escuela militar o por promoción desde los rangos después de seguir un curso de estudio profesional y pasar un examen de calificación.
2. La academia de guerra educaba a oficiales en la ciencia avanzada de la guerra, preparándolo para posiciones en el estado mayor y altos cargos de mandos.
3. El Estado Mayor General exigía oficiales con "el más alto entrenamiento profesional". Los oficiales rotaban entre cargos en el estado mayor y cargos de línea.
4. Para permitir al gobierno aprovechar los mejores talentos en el ejército, con la promoción rápida, sea entrando en el cuerpo del estado mayor o por selección, donde se les ofrece a todos los oficiales que manifiesten un notorio celo y capacidad profesional.
5. Para que el gobierno conozca las calificaciones de los oficiales, se exigían informes anuales o bianuales por parte de los oficiales al mando que mostraran "el celo, aptitud, calificaciones especiales y carácter personal" de sus subordinados.
6. Los oficiales se mantenían para el sólo beneficio del Estado. Si, en consecuencia, un oficial es ignorante o incompetente, el gobierno, por medio de informes personales y exámenes especiales, puede detener su promoción y así impedir daños al servicio... (Upton, 1878, págs. 319-320)

Este concepto de FFAA, en los conflictos actuales se encuentra en crisis por las siguientes razones:

a. **La base humana de conformación de las fuerzas ha cambiado:** no sólo se ha ampliado en sus conocimientos técnicos profesionales, sino también en su composición social. En principio, de acuerdo con los estudios de Morris Janowitz[63], gran parte de la sociedad de los EE.UU., si bien declara que no ve a la profesión militar a la altura de la medicina o la investigación, también "la considera una posibilidad más en hacer carrera y como una oportunidad de ascenso social para todos los sectores" (Janowitz, 1960, pág. 18). Si a estos conceptos se suma los expuestos en su tercera hipótesis: "Modificación del reclutamiento de oficiales", donde plantea la ampliación de la base de reclutamiento en función de la necesidad de nuevos especialistas adiestrados, así como el surgimiento de nuevas armas como la Fuerza Aérea a la que destaca por su creciente necesidad de técnicos especializados y su gran expansión en lapsos breves, ofreciendo una creciente oportunidad de promociones. (Janowitz, 1960, pág. 24)
b. **Las relaciones cívico-militares han evolucionado.** La quinta hipótesis de Janowitz desarrollada en su libro "El soldado Profesional", se expresa en las "Tendencias en la esfera del adoctrinamiento político", adonde se plantea que a partir del mayor desarrollo de la estructura organizativa, la imagen tradicional del soldado se pone a prueba y se expande de la función técnico militar a la conducción estratégica de su ámbito, debiendo desarrollar una ética que le permita, de acuerdo con el autor, dos diferentes comportamientos: uno *interno* en relación con los programas y proyectos, así como la administración relacionada con la seguridad internacional y otro *externo* relacionado con las consecuencias de los actos militares en el equilibrio internacional de poder y en la conducta con otros estados. Pareciera que en las nuevas relaciones cívico- militares estos últimos debieran elaborar opiniones sobre cuestiones que en el pasado podrían mostrarse indiferentes, quedando indefinido si esto es positivo o negativo, pero sí puede decirse que es un aspecto que convive en la relación cívico-militar con ambivalencia entre ambos resultados, dependiendo de la situación y el momento. En occidente la subordinación de las fuerzas armadas al poder político, más allá de sus matices, es un hecho indiscutible en la actualidad.
c. **La ética de la guerra se encuentra en crisis:** si bien hablar de la ética de la guerra es difícil, ya que constituye un acto humano de mayor irracionalidad, desde Westfalia hasta la actualidad, particularmente desde la batalla de Solferino[64], se ha tratado de establecer ciertas pautas de humanización a través del derecho "*Jus*

---

63 Morris Janowitz es un sociólogo y profesor estadounidense que hizo importantes contribuciones a la teoría sociológica, el estudio de los prejuicios, los problemas urbanos y el patriotismo. Fue uno de los fundadores de la sociología militar e hizo importantes contribuciones, junto con Samuel P. Huntington, al establecimiento de las relaciones cívico-militares contemporáneas.

64 Esta batalla por la reunificación italiana, dio origen al libro de Henry Dunant, "Recuerdo de Solferino", ello lleva al autor en 1863 a fundar el Comité Internacional de la Cruz Roja, organismo que ha sido mentor de diferentes modos de humanizar el conflicto bélico https://www.icrc.org/es/publication/recuerdo-de-solferino

in bello" (Derecho en Guerra) que fija un conjunto de normas que rige la forma en que se conduce la guerra, dando origen a los "Tratados de Ginebra y al Derecho Internacional Humanitario". Este concepto es independiente acerca de si la guerra es justa, objetable o no y que trata sobre las razones de la guerra, o su prevención, cubiertas por el *"jus ad bellum"* (derecho sobre la prevención de la guerra). En la actualidad, los conflictos no llegan a constituirse en guerras en el sentido clásico sino que pareciera se mantienen en las denominadas zonas grises o guerras híbridas, donde todo el andamiaje del Derecho Internacional Humanitario (DIH), posee poca o relativa aplicación. En estas situaciones el sufrimiento de civiles y la violencia aplicada es mayor que en los conflictos convencionales, pero su estatus se encuentra por fuera de estos acuerdos. Hoy estados y organizaciones transnacionales como el Estado Islámico[65] emplean este tipo de conflictos, donde se mezcla la guerra de la información, con la criminalidad, donde lo civil y lo militar no poseen una clara diferenciación.

d. Las Amenazas Híbridas[66] o Zonas grises[67]: es el tipo de conflicto que pareciera dominar la actualidad tanto por actores estatales como no estatales. Ellos poseen un formato transnacional y/o intra-estatal, cuando en realidad también se trata de una forma de confrontación de terceros por la hegemonía de poder a través del sistema denominado "guerra proxy"[68]. Lo importante es que las FFAA como tales poco o nada pueden hacer, ya que no cabe su empleo desde una perspectiva legal. En las actuales condiciones cuando los Estados-Nación a través de sus líderes políticos advierten el deterioro de la situación, en general se constituye una solución tardía para llevarla a un punto inicial aceptable.

e. El monopolio de la fuerza pareciera dejar de ser propio del Estado Nación: aparecen nuevos actores con capacidad de empleo de la violencia que en principio no poseen nacionalidad definida; se puede tratar de compañías privadas contratadas por el propio estado o terceros que permitirían pensar que ha perdido vigencia el con-

---

65 *"África: yihadismo, demografía y género":* https://elpais.com/opinion/2021-04-14/africa-yihadismo-demografia-y-genero.htmlhttps:/elpais.com/opinion/2021-04-14/africa-yihadismo-demografia-y-genero.htmlhttps:/elpais.com/opinion/2021-04-14/africa-yihadismo-demografia-y-genero.html

66 Amenazas Híbrida: amenazas que incorporan una gama completa de diferentes modos de guerra, incluidas capacidades convencionales, tácticas y formaciones irregulares, actos terroristas que incluyen violencia y coerción indiscriminadas, y desorden criminal, llevados a cabo tanto por los estados como por una variedad de actores no estatales. (GAO, 2010).

67 Zonas Grises: para el presente capítulo, se considera un informe fechado en 1992 de la Comisión de la Defensa se puede leer una definición de zonas grises: estas serían "regiones que se han vuelto inaccesibles y hostiles a todo penetración, y en las que ningún gobierno tiene la capacidad de hacer respetar las normas mínimas del derecho" (Torres Buelvas, 2019)

68 Guerra *Proxy* Las guerras subsidiarias o"proxy" son un tipo de conflictos en los que se distingue un conflicto interno entre distintos bandos o actores que se engloban como parte de otra rivalidad entre potencias o actores externos. A pesar de que las guerras proxy se han dado a lo largo de la historia, conocerlas resulta revelador acerca de la naturaleza en el mundo en el que vivimos y la situación geopolítica de la región donde ocurren. https://elordenmundial.com/guerra-proxy/

cepto de que *"la violencia es un monopolio del estado"*[69]. En este punto es interesante lo que comenta McFate:

> ... los súper ricos se convertirán en un nuevo tipo de súper poder y esto cambiará todo. A medida que los Estados se retiran, el vacío de autoridad ha engendrado una nueva clase de potencias mundiales, desde corporaciones multinacionales hasta los supe-señores de la guerra y a los multimillonarios. Ahora estas potencias pueden alquilar ejércitos privados, así se esperan guerras sin estados. Esta tendencia crecerá impulsada por un libre mercado de la fuerza que genera la guerra, pero no puede regularla. Los militares de hoy han olvidado cómo luchar en guerras privadas dejándonos a todos expuestos. Para el guerrero convencional todo esto parece desorden e infunde pánico. El mundo está ardiendo sin manera de apagar el fuego. Pero el nuevo guerrero ve algo diferente. (Mc Fate, 2019, pág. 191)

Todos estos aspectos aparentemente propios del siglo XXI de ninguna manera son novedosos. Seguramente una lectura entre líneas del "Arte de la Guerra" permitirá asomarse a muchas de las cuestiones aquí planteadas. En la historia de la guerra encontraremos ejemplos de empleos parecidos o similares a los comentados, pero lo interesante es cómo las tecnologías y el ciberespacio como ambiente operacional han impactado en ellos, para sistematizarlos y particularmente para dar nacimiento a toda una pléyade de autores que comienzan a desgranarse a partir del artículo de Lindt que exponen de manera contundente muchos de los aspectos que devendrán en los conflictos presentes.

Muchos autores han escrito artículos, libros, han realizado investigaciones en diferentes centros de pensamiento con distintos enfoques. Resultaría titánica la tarea de enumerarlos a todos sin cometer la injusticia de olvidar alguno, la idea es comentar algunos de particular interés y que, por sus características, de una u otra forma, representan las partes en disputa según sus preferencias políticas, de las grandes fuerzas en pugna, para que el lector pueda ampliar su visión integral de los contenidos.

f. La evolución del pensamiento estratégico: el General de División en este ensayo, se orienta a los profesionales del conflicto del siglo XXI y apunta a permitir de manera breve y didáctica reflexionar y obtener conclusiones sobre la naturaleza, el propósito y la forma de conducir la guerra, desde Napoleón hasta Van Creveld, comprender el conflicto abordando a estrategas como: Napoleón, Jomini, Clausewitz; Foch, Lee, Hart, Dohuet, Mahan, Churchill, Nimitz, Arnold, Ridgeway, Mao Tse Tung, Vo Nguyen Giap, para finalizar en Van Creveld, a lo largo de su ensayo

---

69 RFI (Radio France Internationale); "Cientos de mercenarios rusos siembran el terror en la República Centroafricana"https://www.rfi.fr/es/africa/20210503-centroafrica-mercenarios-rusos-investigacion-terror-violacion-derechos-humanos

toca aspectos de la disuasión nuclear, la guerra revolucionaria e incursiona en la *"guerra del golfo",* dando una perspectiva de las guerras asimétricas presentando a Afganistán e Irak (de Vergara, El estudio de la historia, evolución del pensamineto estratégico, 2010):

Los nuevos autores estratégicos, más allá de permitir diferentes aproximaciones a los conflictos del presente, tanto en el plano regional como en el internacional, dejan entrever que el conflicto actual, no presenta las condiciones de los escenarios de guerra del siglo XX, en principio algunos aspectos a destacar son:

1. La violencia crece, los conflictos se vuelven más cruentos, sin embargo, desde una perspectiva formal siempre se encuentran en un estado de sub-guerra lo que hace poco aplicable las convenciones vigentes. Parte de ello obedece al empleo de la criminalidad como vector de ejercicio de la violencia
2. Existe una clara coincidencia, más allá de las ideologías que se defiendan, unas y otras dicen los mismo, sólo que las acciones son ubicadas en el lado opuesto. La forma de hacer la guerra en los comienzos del milenio contiene un fuerte contenido de trabajo en el plano ciberespacial, donde la conducta

ILUSTRACIÓN 14 . **Datos obtenidos del foro económico mundial**

El lado malo (HARD)	El lado bueno (SOFT)
Estrategias ciberespaciales duras Ataques a infraestructuras críticas	Busca capturar la mente de la sociedad
Fraude electoral Comunicaciones y TICs Cadena de suministro y transporte Banca y mercado de capitales Seguridad nuclear Provocar derrames intencionados de petróleo Toma del control de un proceso de fabricación Ciudades y urbanización Aviación Corte de energía, etc	1. Convulsionar redes sociales 2. Identidad digital 3. Gobernanza y corrupción 4. Generar fake news 5. Viajes y turismo 6. Ranomsware 7. Desconfianza de las IoT 8. Ataques de colapso en las redes 9. Desinformación e incertidumbres

Usados manera coordinada, efectiva y direccionadas estratégicamente, junto a otros elementos del poder constituyen un factor coadyuvante de importancia en minar la voluntad de la sociedad. Crear el mito de que el poder ciber lo logra por sí, es un error como lo fue en la HWM, creer que el poder aéreo era la forma de doblegar el pueblo inglés primero y el alemán después y sólo trajo terrible destrucción y pocos éxitos.

La fuente para la mayoría de las hipótesis de conflicto provienen de:
https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

FUENTE: (CARNEGIE MELLON UNIVERSITY, 2022).

que asume la sociedad constituye un hito relevante, ya que no importa cuál sea la realidad, sino que la gente cree que la realidad es[70].

3. Acciones cibernéticas enemigas por medios ciberespaciales es la punta de lanza de todo conflicto, apoyada sobre diferentes tipos de operaciones contra estructuras críticas (el lado duro HARD) o en cuestiones propias de la creencia social (el lado blando SOFT). Coordinadas de manera adecuada resultan en una degradación de la sociedad que es base para otras operaciones. Sobre este punto es interesante ver que para occidente estas operaciones sólo serían aplicables en un estado de conflicto abierto, mientras que, para los orientales y soviéticos, estas son de carácter permanente.
4. Los estados occidentales se encuentran con una preparación deficiente para este tipo de conflicto, en áreas como:
   a. Militar: no hay actualización de doctrina, se mantienen esquemas cerrados y estancos donde la comunicación estratégica no se desarrolla en el nivel de la EM y por ende no se orienta de manera adecuada ni genera doctrina para el nivel operacional, si esto es prohibido se niega una visión holística y general del conflicto.
   b. Legal: este tipo de conflicto posee estudios teóricos como los Manuales de Tallin de características académicas no vinculantes sobre cómo se aplica el derecho internacional (en particular, el jus ad bellum y el derecho internacional humanitario) a los conflictos y la guerra cibernética. Pero no existe un derecho acordado acerca del mismo.
   c. Social: como ha sido presentado, la sociedad ignora completamente los peligros del ciberespacio y las operaciones que en él se realizan como afectan su conducta, sino que va más allá, coartando sus libertades.
5. Este tipo de guerra posee un alto contenido de estrategia nacional, si bien occidente reserva las operaciones de información, a las influencias psicológicas para el conflicto ya instalado. La realidad para chinos y soviéticos es una doctrina de aplicación constante, muestra de ello son las estrategias propuestas en libros como Unrestricted Warfare y Manual de Guerra de la información Rusa o Las Nuevas Reglas de la Guerra, donde la acción del campo de batalla no resulta principal sino auxiliar.
6. Sobre el conflicto en ejecución, es necesario rediseñar la forma y trabajo del Nivel Operacional para que se adapte a escenarios cambiantes con relaciones complejas, donde la aparición de empresas de seguridad, "hombrecitos verdes" y fuerzas de sedición se encuentran totalmente entremezcladas que dificultan determinar si existen combatientes y no combatientes, ya que la guerra en el campo cinético llega de manera tar-

70 Dijo Mao Zedong: *"Todos los imperialistas son tigres de papel, parecen poderosos pero en realidad no lo son tanto, es el pueblo el que es realmente poderoso"* https://www.muyinteresante.es/cultura/arte-cultura/articulo/10-frases-celebres-de-mao-zedong-241410269315

día. La gran batalla se ha librado en la mente de la sociedad, de ahí que los nuevos reyes de la guerra sean los combatientes cibernéticos, ya que de la certeza de sus operaciones se definirá en gran medida el futuro conflicto. La batalla decisiva pensada por Clausewitz, se ha convertido en una larga y desgastante acción sobre la sociedad hasta reunir las condiciones adecuadas para la toma del poder.

7. Estos conflictos no buscan afianzar territorios como propios, su objetivo es desestructurar el sistema sociopolítico del adversario, rompiendo la cohesión social y produciendo un cortocircuito completo entre la sociedad, el liderazgo político y las fuerzas de seguridad.
8. Este tipo de conflictos requiere de actores en el nivel estatal, ello les permitirá disponer de capacidad económica, militar y tecnológica logrando así libertad de acción a la vez de poder desafiar a otros actores en el orden internacional.

3.1. **Una visión acerca del Poder Voluntad y Temor**

Revisando lo visto hasta ahora, la naturaleza de la guerra se ha mantenido constante desde el principio de la humanidad hasta nuestros días, donde su objetivo por antonomasia es el control de la *voluntad* del adversario. Se mantendrá así, mientras la búsqueda de poder por parte del hombre esté por encima del impulso de servicio al prójimo.

Lo hasta aquí expuesto, demuestra que lo que cambia y continúa haciéndolo es la forma en que la guerra se lleva adelante y cómo se va transformando esa lucha por el poder en el siglo XXI, un siglo que ve en su comienzo el atentado del 11 de septiembre de 2001, donde todos los principios y paradigmas de la guerra se hacen añicos, cuando un puñado de hombres pertenecientes a la red Al Qaeda (una organización de ningún estado), usando los aviones comerciales de su supuesto enemigo, en una operación sin precedentes, rompe el dogma por antonomasia del mundo occidental: "la libertad", eje de vida y permanente vanagloria de occidente.

Podría escudriñarse en la historia de las grandes operaciones militares, la relación entre los esfuerzos y los éxitos obtenidos cuáles han sido más exitosos: ninguno podría superar las devastadoras consecuencias en lo social, cultural y económico que tuvo el ataque a las Torres Gemelas. Una acción cinética fue la que introdujo el conflicto social, que trajo como consecuencia una reducción de las libertades individuales de manera coercitiva en la búsqueda del largamente deseado bien común.

En esa búsqueda del poder y el dominio de la voluntad del otro, es interesante el concepto de Han (Han B.-C. , What is power?, 2017), por el cual el mejor ejercicio del poder es aquél que se hace por el consentimiento, libertad y voluntad del otro. En este sentido podemos decir que la humanidad siempre supera sus propios límites en el camino de la búsqueda del ejercicio del poder, a través del dominio de la voluntad. La crisis que surge como consecuencia de la pandemia generada por el llamado COVID 19, ha mostrado ser muy eficiente en el ejercicio del poder ya que no sólo ha contado con el apoyo de los individuos, sino incluso de los estados.

Resulta oportuno realizar un análisis simplificado desde una diferente perspectiva a partir de temas ya tratados:

1. Aristóteles define a la Libertad como: *"La preferencia reflexiva de lo mejor",* pocas palabras de amplia profundidad, donde la preferencia determina un acto propio de la voluntad y la reflexión muestra la faceta más intricada de la inteligencia en la búsqueda de un bien que lo deseamos como propio pero que sólo da libertad en la medida que lo deseado sea lo mejor.
2. El hombre, al menos en la cultura occidental, es un eterno buscador de la libertad, más allá de que en muchos casos no comprende claramente qué significa, de dónde proviene y en general poco se molesta en reflexionar acerca de si lo deseado es bueno, ni siquiera lo mejor. En estas sencillas palabras quizás se encuentra la piedra que inicia el alud de la destrucción de occidente.
3. El elemento que es objeto y fin de la estrategia y el señor de todas las guerras es el dominio de la voluntad, base para el ejercicio del poder. Desde el principio de los tiempos el efecto cinético, producto del empleo de las armas, fue el medio más eficaz para que el vencido cumpliera con los designios que el poderoso definía.
4. La llegada del espacio cibernético y la revolución tecnológica despierta una nueva realidad: podemos dominar la voluntad del individuo, sin que él lo note, es más, hasta puede adherir a cumplir con los designios del poderoso por su propia voluntad alcanzado según Han el más alto valor en el ejercicio del poder.
5. La pregunta a formular es ¿En qué bases se asienta el dominio de la voluntad, objetivo estratégico por antonomasia de la guerra? la respuesta es: sobre una estructura informe y cambiante compuesta de tres (3) factores: Libertad, Seguridad y Poder, todas ellas íntimamente relacionadas con tres dimensiones de la voluntad humana: compromiso, deseo y determinación.

3.1.1. Algunos corolarios a partir de la pandemia COVID 19

Volviendo sobre lo enunciado:

1. El problema del ejercicio del poder fue buscado en el plano material (campo de batalla), pero se realiza y ejecuta en un ambiente espiritual, donde compromiso, deseo y determinación son intangibles.
2. Lo espiritual en el mundo moderno ha quedado cuasi sepultado por la líquida inmediatez y su placebo de reemplazo ha sido el ciberespacio, un ambiente de características inmateriales que viene a ocupar ese espacio de la espiritualidad.
3. Finalmente, el dominio de la voluntad debe buscarse en un plano espiritual / inmaterial, donde los componentes esenciales para su control estarían dados por el compromiso, el deseo y la determinación, los cuales articulan la relación entre poder, libertad y seguridad (todos ellos necesarios y excluyentes unos de otros: la preeminencia de uno deprime a los otros, sólo su adecuada relación asegura una vida pacífica).

Habiendo introducido un entorno de ideas respecto a la problemática del conflicto y

la guerra desde una perspectiva del siglo XXI, la situación y corolarios expuestos, en relación con los sucesos, marchas y contramarchas que se pueden revisar desde el inicio de esta crisis *COVID* y hasta el momento actual, posee todos los componentes propios del formato de las guerras del siglo XXI, veamos por qué:

1. No existe una declaración de guerra: sin embargo, los efectos que ha logrado son los propios de ella. La causa que la produjo es de origen humano y con un solo objetivo visible: causar un temor tan irrefrenable que permite manipular la voluntad.
2. Es una guerra de desinformación: si hay algo claro después de todo este proceso es que las culpas se han repartido de manera pareja, desde las teorías conspirativas más alocadas hasta noticias que el virus fue producido por China, con fondos de los EEUU, o que se originó en laboratorio Ingleses que lo produjo China con la compra de información en el Massachusetts Institute of Technology (MIT), que es una maniobra de la OMS para lograr el control planetario a través de una vacuna que al ser inoculada permitirá a supuestos dueños del poder lograr su panacea, como la expresada por George Orwell en "1984". Otras ideas hablan de que la vacuna existe con anterioridad a la pandemia, pero es parte de un gran negocio que debe dejarse madurar. Podría citarse líneas y líneas, desde los más famosos periódicos de diferentes lenguas, hasta los pasquines más oscuros y los dislates de las redes sociales donde encontramos todo tipo de científicos y ganadores de premios internacionales, desinformando de la manera más controvertida que se pueda imaginar. El objetivo se cumplió: nadie tiene la verdad y si la tiene y es real, es poco creíble, no importa cuál sea.
3. Es una guerra de características complejas: donde conviven lo lineal y lo asimétrico simultáneamente, confluyen en un ambiente social convulsionado, donde lo militar y lo civil, no pueden ser claramente distinguidos, donde es muy difícil determinar cualquier tipo de acción cinética porque la probabilidad de error es muy elevada o los costos de la acción pueden superar largamente los beneficios de su ejecución.
4. Es una guerra pre-anunciada: si bien siempre se han tenido por poco éticas todas aquellas cuestiones relativas a la guerra convencionalmente denominada QBN (Química, Bacteriológica y Nuclear) nunca se dejaron de desarrollar estas capacidades en razón de asegurar el poder, aún a costo de la llamada "mutua destrucción asegurada", incluso con los riesgos de un suicidio.
5. Cumplió con la naturaleza de la guerra: se dominó la voluntad de la gente, pero fue mucho más allá, se logró la adhesión voluntaria del público, sin saber nunca exactamente de qué se trata. La única arma empleada fue la adecuada manipulación de la desinformación trabajando sobre: el deseo de sobrevivir con los que se auto gestionó la falta de libertad, el compromiso con la sociedad que fue la base de seguridad de que todo va a estar bien y la determinación estatal generó un poder que puede competir con los más elevados estándares de las

peores dictaduras. Sólo queda la manipulación del deseo y el compromiso, el sometimiento fue voluntario, donde cualquier desvío o sesgo del mismo puede ser re-encauzado a través de un cerrado control poblacional sólo posible con las capacidades tecnológicas del ambiente cibernético.

Lo desarrollado nos permite contestar la primera pregunta ¿Cuál es el beneficio de esta guerra? La respuesta es: se ha demostrado que, con un adecuado manejo de las variables necesarias, se puede alcanzar el poder suficiente para manejar la voluntad planetaria.

La segunda pregunta y sin respuesta aún es ¿Quién provocó esta guerra?, seguramente no fue el coronavirus, no pareciera al menos a simple vista que hayan sido los poderes estatales formales, la respuesta a esta pregunta a lo mejor se relaciona con las apreciaciones de McFate en su libro *Las Nuevas Reglas de la Guerra* y coincidan con la regla número 7 *Gobernarán Nuevos tipos de Potencias Mundiales*[71] (Mc Fate, 2019, págs. 114-133).

El arma más efectiva para enfrentar este tipo de conflicto es la cultura social, sólo a través de ella se puede lograr la resiliencia suficiente que evite los efectos de la comunicación estratégica

Hasta aquí, este trabajo se ha concentrado en el conflicto presente que ha llegado para quedarse, pero ¿cuál es el conflicto futuro?

4. **Intentando navegar hacia el conflicto futuro**

La virtualidad es parte de la vida humana, desde la invención de la radio[72], hasta nuestros días, el tiempo que dedicamos al mundo real y al virtual ha ido incrementándose más dramáticamente a partir del advenimiento del ciberespacio como un ámbito de vida, donde prácticamente todas las actividades del mundo real pueden ser replicadas en el mundo virtual, donde el tiempo que los humanos dispensamos al mismo continúa creciendo en forma constante.

El acceso al ciberespacio, un mundo creado por la humanidad cuyo uso se ha basado en un manifiesto anárquico en su naturaleza[73], se realiza sin ninguna preparación ni precaución, es más, la llave de ingreso (un *smartphone*) a ese universo desconocido, en general está disponible para los niños incluso antes de que se encuentren en condiciones de caminar, sin advertir que los adultos tampoco comprenden y conocen cabalmente cuáles son los riesgos y peligros que entraña y cómo son las reglas y procedimientos para movernos en él.

Los avances de la tecnología superan largamente la capacidad de adaptación humana, por ejemplo, si se consideraran los elementos que componían una oficina

---

71 "10 empresas más grandes que 180 países" https://elpais.com/economia/2016/09/29/actualidad/1475150102_454818.html

72 Es interesante citar aquí el programa de Orson Welles "La guerra de los mundos", como un ejemplo de control de masas, desde la virtualidad en este caso empleando solo las ondas hertzianas.

73 Manifiesto de John Perry Barlow Declaración de Independencia del ciberespacio, https://academy.bit2me.com/declaracion-de-independencia-del-ciberespacio/

en las décadas de los 80/90[74], hoy todo eso y algunas otras capacidades están en nuestro bolsillo con un teléfono inteligente.

Ni las leyes, ni nuestras mentes, ni el sistema de aprendizaje se han adaptado al cambio y ya estamos en la próxima estación: donde la inteligencia artificial, la robótica y la computación cuántica, constituyen la nueva promesa de un mundo feliz, esto ya sucedió en los 80/90 con la promesa de la globalización que, si bien trajo grandes beneficios, hoy es la razón de serios inconvenientes en diferentes aspectos de la vida humana.

Estos cambios han, de alguna manera, trasladado el campo de batalla cinético del mundo real, al cerebro campo de batalla primario de las actuales guerras. El principal ambiente donde se desarrollará el conflicto futuro, es el ciberespacio, pero la pregunta es ¿estamos preparados para eso?

4.1. **Una visión estratégica del conflicto actual**

Si bien la naturaleza de la guerra no ha cambiado, desde el principio de los tiempos hasta hoy, podemos ya sea citando a Sun Tzu, Clausewitz, Mao, Warden, Eikmeier, no importa a quién, siempre el problema es dominar la voluntad del adversario con el menor esfuerzo posible. El ambiente ciberespacial introduce notables ventajas para ello y un cambio de paradigma en el cómo hacer la guerra y en qué consiste:

1. El campo de batalla se ha movido del mundo real a través del ámbito virtual a la mente de las personas, no importa cuál es la realidad, sino lo que la gente cree que la realidad es, más allá de los hechos que se muestren.
2. La realidad que prima es lo que la sociedad cree que es, más allá de la realidad fáctica del hecho en cuestión, ello se refleja en la decisión política consecuente.
3. El tiempo de permanencia en el ciberespacio por parte de los humanos se incrementa dramáticamente día a día.
4. El ciberespacio genera acción líquida instantánea sin compromiso

4.2. **Corolario de esta situación**

Napoleón había dicho: «la infantería es la reina de las batallas», y todos los grandes estrategas lo aceptaron porque sin duda, hasta que los infantes no ocupen el terreno no se puede hablar de victoria. El problema es que el campo principal de batalla en el siglo XXI será la mente de la sociedad, por ende, el rol de la infantería será ocupado por una nueva clase de guerreros: los guerreros del ciberespacio, que serán los reyes de las mentes. No son hackers, sino equipos multidisciplinarios con sociólogos, neuro-científicos, psicólogos, ingenieros y psiquiatras entre muchas otras disciplinas.

Aquí es donde radica el problema estratégico militar de este ambiente operacional[75] (el ciberespacio), ya que la esencia de la guerra no ha cambiado, y sus modos que siempre existieron (velo, engaño, guerra de la información, etc.), las TICs han poten-

74 PC, agendas, archiveros, teléfono, fax, máquina de escribir, máquina de fotos fotocopiadora, etc.
75 Se aplica este concepto a los dominios de Tierra. agua, aeroespacio y ciberespacio

ciado todo ello en el niveles difíciles de ponderar. Esta suma de tecnologías y capacidades ha llevado el conflicto a un concepto de implementación que podría denominarse la estrategia del demonio (si haces todo bien de algún modo caes al infierno y si lo haces mal ya estás en el infierno, pero no importa lo que hagas siempre el demonio gana). ¿Cómo se implementa esto en el ciberespacio? Es aquí donde aparecen nuevas hipótesis de conflicto, etéreas, con aspectos difíciles de dimensionar, sin embargo, introducen a la sociedad en un estado de cuasi guerra, cuasi total (no desde la perspectiva de Clausewitz,) sino desde la perspectiva del hombre común que pierde el concepto esencial de seguridad, para vivir atemorizado.

Así, hemos pasado de la batalla aeroterrestre, cuyo zenit se encontró en "Tormenta del Desierto", se busca la solución en batalla multidominio donde fuerzas terrestres, mar, aeroespacio y ciberespacio conjugan sus esfuerzos en el logro de objetivos. Sin embargo, la eficacia podría ser relativa frente al conflicto planteado en *"escenarios híbridos"*[76] y *"guerra irrestricta"* (Qiao & Wang,, 1999), donde el ciberespacio ha adquirido un valor trascendental y el conflicto no alcanza el estado de guerra.

Cada uno de estos ambientes, a su vez, es considerado desde diferentes dimen–siones (tiempo, información, inteligencia, ayuda humanitaria, medio ambiente, a–suntos civiles, asuntos militares, infraestructura, economía, ambiente psicosocial, criminal, financiero biológico etc.). Una primera aproximación la ha dado las Naciones Unidas (UN) con las *"High-Level Independent Panel on Peace Operations"* (HIPPO)[77]. Todos estos intentos fueron para tratar de alcanzar una doctrina que permita efectivizar el enfrentamiento en el campo de batalla futuro, que finalmente se dará en tres grandes ámbitos:

1) Realidad: es el ámbito o dominio, donde se maneja la cuestión física tangible, en él se producen los efectos cinéticos del campo de batalla
2) Virtual: es el ámbito o dominio donde se ejercen las acciones propias de la ciberguerra y de guerra electrónica, operaciones de ofensivas, defensivas y de exploración cibernética.
3) Cultural o humana: es el ámbito o dominio de la Comunicación estratégica[78] a través del cual se incide sobre la opinión o humor de la sociedad objetivo.

En el ciberespacio también podríamos establecer tres niveles a considerar, el de la seguridad Informática (firewall, antivirus, concientización, etc.), el de la Ciberdefensa (protección de las infraestructuras críticas, ya sea mediante operaciones ofensivas, defensivas o de explotación) y el de la Información que coincide con el tercer ámbito el humano a él posiblemente, corresponde el conflicto actual y próximo futuro.

---

76 Molly K. Mckew, Gerasimov doctrine, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia- foreign-policy-215538, sep/oct 2017

77 https://www.un.org/pga/70/wp-content/uploads/sites/10/2016/01/PolicyBrief2015_5_-Imlementing_the_HIPPO_Alexander-Ilitchev.pdf

78 El término comunicación estratégica para este caso involucra al menos operaciones de información, influencia, psicológicas y de guerra electrónica.

Ambas concepciones poseen cierta coincidencia e interdependencia en los 2 primeros niveles, pero en el caso de cultural o humano el lugar donde las acciones se llevan a cabo es común en ambos: el cerebro humano, allí es donde se dirime el resultado, más allá de las acciones en el campo real y en el virtual, las decisivas serán el de la información: el pensamiento social a través del cerebro de cada uno, es el objetivo de los conflictos actuales.

Un aspecto a destacar es la concepción del empleo de lo que se da en llamar Ciberguerra, para occidente en el ambiente virtual, se centra de manera exclusiva en las problemáticas de los dos primeros niveles: la seguridad informática y la Ciberdefensa (protección de las infraestructuras críticas), pero no es considerada la protección del hombre común en el nivel de la información en tanto el conflicto no se encuentre claramente establecido por la autoridad política, ello es propio del respeto que occidente posee por la libertad del Individuo, sin embargo, es allí donde se producen las agresiones de mayor impacto, de una manera continua y que, como fuera explicado, uno de los primeros efectos que busca esta agresión es direccionar en el individuo sus elecciones y preferencias reduciendo en términos concretos su real ejercicio de la libertad.

4.3. **¿Cuál podría ser Conflicto Futuro?**

De alguna manera, a través de este trabajo, se ha descripto el conflicto actual y la posibilidad de que, con diferentes variantes, se mantenga en el futuro próximo. Pero la tecnología depara algunas sorpresas en su evolución, así el conflicto futuro viene de la mano de la "singularidad", una promesa de bienestar y progreso para toda la humanidad, como ya se ha explicado similar a la que en las décadas de los 80 y 90 surgió con la "globalización", que trajo beneficios a la humanidad, pero con ella llegó la WEB profunda, el ciber-terrorismo, el ciber-crimen, las guerras hibridas, solo por citar algunos problemas que no visualizamos entonces.

¿Qué nos promete la singularidad?, el mundo para el 2050 encontraría a la humanidad compitiendo con la racionalidad perfecta, máquinas con capacidades iguales a las del ser humano, pero con la ventaja de un conocimiento cuasi infinito ya que ella dispondrá de toda la *big data* a la hora de responder. Como ya fue tratado, la punta del iceberg la mostró el caso Cambridge Analítica. Hoy se podría hablar de una nueva clase de dios, que puede dedicarse a cada individuo de manera individual, pero que a diferencia del Dios espiritual que pugna por el libre albedrío, este busca esclavizar nuestras mentes y quitarnos la capacidad de autodeterminación, ¿y quién nos defiende de esto?

¿Cómo competimos contra la racionalidad perfecta?: mientras que nosotros sólo dispondremos de nuestro puñado de conocimientos para afrontar cada situación, la inteligencia artificial dispondrá casi instantáneamente de la totalidad del conocimiento humano para resolver el mismo desafío. Si a esto se suman otras tecnologías de la cuarta revolución como son la robótica y la computación cuántica, cabe preguntarse

¿Podrán las reglas de Isaac Asimov[79] implementarse para sobrevivir? (Asimov, 1989), y de hacerlo ¿a qué se limitará la vida humana?

Llevamos aproximadamente 2500 años, desde que los grandes filósofos griegos definieron al *"hombre como un animal racional",* educando nuestro cerebro en el desarrollo de la racionalidad, cuando en realidad nuestro cerebro tiene otras potencialidades, como la intuición (capacidad de ver la respuesta de manera directa), cualidad que asignamos a los artistas y los genios, ¿acaso Einstein no introdujo la teoría de la relatividad y luego comenzó su demostración y aún sigue en estudio? Pero si observamos la capacidad humana, se notaría que en general las decisiones cruciales o trascendentales son aquellas que implican cuestiones de vida o muerte, estas no proceden de un proceso racional, sino que son decisiones tomadas en el campo emotivo, ellas se relacionan con el análisis, revisión y conocimiento de la perspectiva racional.

En las décadas de los 50/60, la ciencia dejó entrever que nuestro cerebro tenía la capacidad de advertir en una película a más de 30 cuadros por segundo, que algunos de ellos tienen información que es procesada en nuestro inconsciente y nos hace adoptar determinadas conductas (mensajes subliminales[80]). Esto lo hemos empleado para incrementar el consumo, pero nunca trabajamos para cultivar nuestro cerebro y poder traer cosas del inconsciente al consciente.

El gran desafío de los próximos 30 años es lograr un diferencial importante con la futura evolución de la inteligencia artificial, un diferencial que permita a los seres humanos seguir siendo la especie que domine este planeta. El potencial lo tenemos entre nuestras orejas y las neurociencias han abierto las puertas del conocimiento de nuestro cerebro. El desafío es crear una nueva cultura de aprendizaje. Ello requiere inicialmente comprender y conocer los procesos que impone el ciberespacio para impedir ser dominados a través de este.

LA CLAVE PARA AFRONTAR EL CONFLICTO FUTURO ES EL DESARROLLO DE NUEVAS CAPACIDADES COGNITIVAS

La confrontación de hoy ya no conoce de seguridad interior o nacional, no distingue entre soldados y civiles, el campo de batalla somos cada uno de nosotros, desarrollar una cultura común y una forma de pensar propia, pero con una base cultural común es la que nos permitirá afrontar con éxito las crisis y conflictos del presente y prepararnos para la segunda etapa del proceso, que es aprender a desarrollar nuevas capacidades cerebrales, para así poder enfrentar el conflicto futuro: la competencia con la IA.

---

79 Las 3 reglas de Asimov dicen: 1. Un robot no hará daño a un ser humano o, por inacción, permitirá que un ser humano sufra daño. 2.Un robot debe hacer o realizar las órdenes dadas por los seres humanos, excepto si estas órdenes entran en conflicto con la 1º ley. 3.Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la 1ª o la 2ª ley.

80 Mensajes subliminales https://www.ugr.es/~aula_psi/Mensajes_subliminales.htm

Más allá de todo lo expuesto, las debilidades que presenta el sistema de defensa nacional propio en aspectos tecnológicos, financieros y restricciones legales , debiera pensarse en una estrategia que permita operar con eficacia en condiciones de inferioridad para todos los ámbitos operacionales, ello sólo sería posible a partir de convertir a cada hombre en una sucursal independiente pero integral de a fuerza en sí mismo, un concepto de inteligencia distribuida, que sólo sería alcanzable a partir de una reestructuración de la educación y formación militar inteligencia se encuentra distribuida y orientada al fin de la Defensa Nacional.

Capítulo 4

La comunicación estratégica y la estrategia de la comunicación

Términos y definiciones

Por CL (R) Mg. Gustavo A. Trama

Una lección aprendida hasta ahora en el conflicto es cuán efectiva ha sido Kiev en las operaciones de información para contrarrestar la campaña de desinformación de Moscú contra el gobierno del presidente Volodymyr Zelensky [81].

1. **Introducción**

La historia universal está llena de guerras (*war* en inglés) entre tribus, naciones e imperios. Cada una de ellas adquirió características diferentes. Ninguna fue igual a la anterior. El equipamiento utilizado pasó de palos afilados y piedras a armas automáticas y misiles lanzados desde vehículos aéreos no tripulados con capacidad de decisión autónoma. Cada nuevo avance en la tecnología militar influyó sobre la forma en que se combatió y las tácticas empleadas lo que generó tipos de guerra (*warfare* en inglés). En la era moderna se generó una taxonomía académica, que sostiene que la guerra (*war*) se fue transformando a través de cuatro diferentes generaciones de hacer la guerra (*warfare*), en la última de las cuales la violencia militar ya no necesitaría jugar un rol preponderante como lo fue en las grandes conflagraciones.

81 Gen. Thierry Burkhard - Jefe de Estado Mayor de las Fuerzas Armadas (CEMA) de Francia; Disponible en: https://news.usni.org/2022/03/08/head-of-french-military-russians-were-not-ready-for-ukraine-invasion

A los ojos occidentales los conflictos resultan difíciles de definir. No todos pueden ser analizados bajo la misma óptica razón por la cual abundan las clasificaciones y subclasificaciones muchas de las cuales no están doctrinariamente desarrolladas, o si lo están, son bases muy endebles

Lo que estaría ocurriendo en los conflictos actuales es una combinación de "poder duro" y "poder blando" mediante la inteligente aplicación coordinada de elementos diplomáticos, de información, militares y económicos (DIME) tanto en espacios físicos como virtuales. En ellos, las fronteras entre la paz y la guerra, entre lo militar y lo no militar se diluyen, no existe una declaración formal de guerra, se emplean medidas convencionales, irregulares, terroristas, de desinformación, cibernéticas (ataques, espionaje, engaño), económicas y políticas de influencia y de intimidación. El conflicto que actualmente se desarrolla entre la Federación de Rusia y Ucrania, pareciera confirmar esta proposición. Cuando comenzó la invasión de Ucrania, el embajador ruso ante los Nacionales Unidos respondió al enviado especial ucraniano: «No llame a esto una guerra. Esto se denomina una operación militar especial en Donbass"[82].

El mundo vive la Era de la Información. La Era Industrial consistía en ambientes humanos y físicos en los que las personas controlaban directamente sus máquinas industriales. La Era de la Información conserva ambos ambientes, pero inserta entre ellos otro donde los individuos ahora perciben, interactúan y controlan su mundo físico a través del ambiente de la información y en él, el uso cada vez más extendido y bien planificado de las redes sociales, digitales y otros medios de comunicación ha hecho posible llegar a audiencias más grandes con un contenido personalizado y dirigido a una velocidad extraordinaria.

En la Era de la Información las comunicaciones se apoyan en gran medida en Internet (dependiendo del nivel de acceso que tengan a él las personas)[83], o a través de sistemas que utilizan varias partes del espectro electromagnético, redes terrestres o satelitales permitiendo el libre flujo de información dentro y entre los estados nacionales (en función de la legislación vigente y los límites culturales impuestos por algunos gobiernos), en los negocios, las relaciones internacionales y las sociedades y también en las fuerzas militares.

ILUSTRACIÓN 15 . **Ambiente de la información**

FUENTE: ELABORACIÓN PROPIA

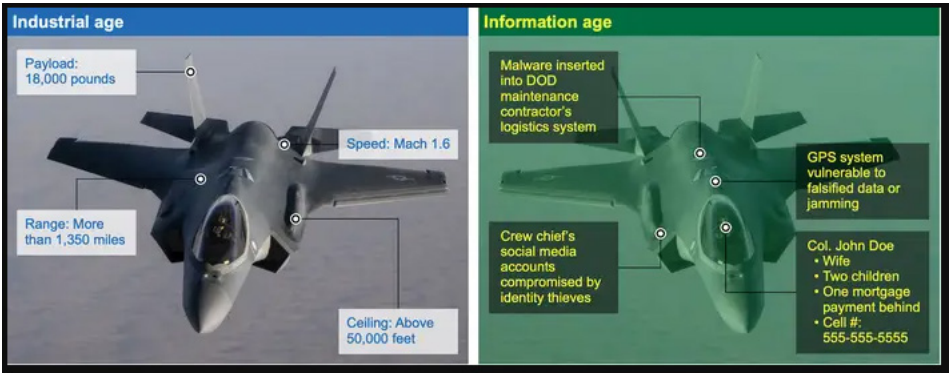
La Era de la Información permite llevar a cabo actividades militares atacando o alterando capacidades desa–

82 Andrew Clapham; On War; Disponible en: https://lieber.westpoint.edu/on-war/

83 La brecha digital sigue muy amplia, mientras que Europa tiene una tasa de más 95% personas conectadas, América latina se encuentra en un 80% y África apenas alcanza un 40%, incluso con regiones por debajo del 20%. (UIT *Global Connectivity Report 2022*)

rrolladas en la Era Industrial o afectando negativamente las funciones y misiones como se muestra en la ilustración 16.

ILUSTRACIÓN 16 . **Yuxtaposición de capacidades en la Era Industrial vs. Las debilidades de la Era de la Información.**



FUENTE: (GAO-22-104714, 2022)

Los avances en el campo de las imágenes térmicas pueden destacar objetivos ocultos a simple vista, mientras que la observación casi constante en tiempo real desde constelaciones de satélites y vehículos no tripulados aparentemente omnipresentes puede inhibir las maniobras, realizar ataques de precisión y proporcionar indicaciones y avisos oportunos. Los voluminosos hilos de Twitter y las subidas de datos, metadatos e incluso conjuntos de datos curados[84] proporcionan una comprensión sorprendentemente granular del espacio de batalla, y las plataformas de Internet como Google Maps pueden indicar la congestión del tráfico en las principales autopistas causada por una invasión (Huw Dylan, David V. Gioe and Joe Littell, 2022).

Es también la "Era de la Post-Verdad" donde el mundo es una construcción humana inventada para explicar, cómo elegimos vivir en él. La "verdad", construida por una narrativa, suele volverse subjetiva e imponerse por criterio de relevancia temporal sobre otras "verdades" también subjetivas. La manipulación informativa ha conformado una subjetividad que entiende la realidad de acuerdo al discurso dominante. Mas aun, en la actualidad resulta casi imposible ponerse de acuerdo sobre los hechos, que son negados, distorsionados o reducidos a opiniones.

Esto se llama posverdad que proviene del anglicismo "post-truth", que se potencia por la fuerza de las redes sociales. La posverdad no es más que una modalidad estimulada por radicales cambios culturales que en realidad se proyectan desde los años setenta, cuando una nueva generación de intelectuales, sobre todo franceses, empe-

84 El curado de datos es la actividad por la que organizamos todos estos datos de la misma manera, dejándolos preparados para su posterior análisis y extracción de información.

zaron a proclamar que "la verdad no existe" y que es, en todo caso, "una construcción social". Es lo que se atribuye, entre otros, a Aleksandr Duguin, ruso, nacionalista fervoroso y cercano a Putin: "La verdad es una cuestión de creencia. Los hechos no existen" (Escribano, 2022).

La opinión pública está cada vez más moldeada por las redes sociales. Para explotar esto, se crean sitios web, cuentas de redes sociales y mensajes atribuidos a identidades falsas. Se manipulan las funciones del navegador, los algoritmos de los motores de búsqueda y otros mecanismos automatizados que controlan qué información presentan a los usuarios de Internet. Dicha manipulación puede garantizar que ciertos comentarios e información aparezcan o no en respuesta a las búsquedas. Puede asignar mayor relieve a material antiguo crítico de fuentes o análisis, que a nuevas entradas favorables a ellos. Puede organizar búsquedas para encontrar solo comentarios positivos o negativos e información sobre un tema.

ILUSTRACIÓN 17 . **Discurso dominante**

FUENTE: *(GUALÁN, 2018)*

ILUSTRACIÓN 18 . **Explotación de las redes sociales**

FUENTE: *(PORT G1, 2022)*

La explotación de las redes sociales y los algoritmos aumenta la propagación y el impacto de las noticias y mensajes falsos. La tecnología también permite construir informes ficticios cada vez más realistas, gracias a los *«deepfakes»*[85] (Duperron, 2022).

La desinformación circula en *Twitter, Tiktok, Facebook, WhatsApp, Telegram* y otras redes sociales y canales de mensajería. La información falsa incluye videos, fotos, citas supuestamente textuales de funcionarios gubernamentales, y posteos que denuncian, por ejemplo, sin fundamento que ya empezó una invasión por tierra, o que hay bandas listas para arrasar tranquilas zonas suburbanas. En

85 Se trata de trucos ultra sofisticados desarrollados gracias a la inteligencia artificial. Por ejemplo, es posible fabricar un video de una entrevista falsa con una figura política. Los hackers pueden atribuir declaraciones controvertidas a los políticos y difundir este video falso para desacreditarlos o sorprender a los usuarios.

mayo de 2021 los videos de *TikTok* ayudaron a provocar varias noches de enfrentamientos y caos entre los jóvenes árabes y judíos en Jerusalén. Hubo quienes culparon a la plataforma de intercambio de videos en ese momento por desempeñar un papel en la escalada de seguridad en general, que incluyó a Hamas disparando miles de cohetes en Israel. «Todo el mundo lo llama la intifada de *TikTok*», dijo Tehilla Shwartz Altshuler, investigadora principal del Instituto de Democracia de Israel, en una entrevista en ese momento (Hoffman, Maayan, 2022).

Tanto Washington como casi todas las democracias liberales (incluidas las de Europa) están tratando de descubrir cómo manejar la enorme influencia de TikTok, que se está convirtiendo en la aplicación más popular del mundo, pero se ha descubierto que ha enviado los datos de los usuarios a China. Hasta la fecha, sin embargo, ha habido poca coherencia entre esas democracias sobre cómo deberían responder a la ofensiva global de medios e información de Beijing, y poco intercambio de mejores prácticas entre las democracias sobre cómo responder (Kurlantzick, 2023).

ILUSTRACIÓN 19 . **Explotación de las redes sociales**

FUENTE: *(BARAK, 2021)*

Esas falsedades se amplifican al ser compartidas miles de veces por *Twitter* y *Facebook*, y de allí a grupos de T*elegram, WhatsApp* de millares de miembros. El efecto de la información errónea es potencialmente nocivo, porque alimenta la hoguera de sospechas y desconfianza.

Cada actor preserva su individualidad; no hay contienda ni comunicación auténtica, sino meramente un contacto al cabo del cual cada uno vuelve a su mundo. Solo hay gestos. En ese entorno, la popularidad de las teorías conspirativas y la dis–

posición de la gente a aceptarlas es relativamente significativa. Generalmente no son verificables lo cual es con frecuencia tomado como prueba de su veracidad.

A través de los medios de comunicación social, esa información –ya sea que algunas se ofrezcan como pruebas o simplemente en forma de rumores– a menudo recorre el mundo en minutos y una campaña bien organizada puede fácilmente influir en las percepciones y comportamientos de la población propia y extranjera. La gente raramente hace el esfuerzo para verificar la veracidad de tales datos; más bien, los pasan a otros, con lo cual mejora su alcance y credibilidad (NATO StratCom, 2016).

En los conflictos, los periodistas profesionales pueden ser engañados por información incorrecta o engañosa presentada como un hecho, ya sea intencional o no intencionalmente (*misinformation*), pues ante la necesidad de mostrar imágenes e historias y ansiosos por obtener noticias como sea posible, de una manera rápida en el entorno competitivo de los medios de comunicación de hoy, los umbrales son más bajos, y aun cuando suelen asegurar que tienen "buena" calidad informativa porque han chequeado la información, su selección de material es tomada con menos precaución que en otros días.

La actualidad presenta una situación de riesgo debido a la difícil acción de discernir entre informaciones veraces, falsas, fabricadas o manipuladas. La información (verdadera o falsa) se convierte en un arma de primer orden en cualquier conflicto, arma que puede atacar directamente a la voluntad del adversario a muy bajo costo y que, aprovechando la falta de preparación en cuestiones de defensa de su audiencia, explota las emociones para obtener las respuestas deseadas. Y todo ello, manteniendo la posibilidad de negar cualquier implicancia en la difusión de los mensajes, lo que permite su uso incluso sin estar en la situación formal de conflicto armado.

Si bien la información siempre se ha utilizado como una herramienta para adquirir la ventaja en la guerra, generalmente no se piensa en ella como un arma en sí misma. Sin embargo, la tecnología moderna de la información y de las comunicaciones (TIC´s) y la dependencia de los sistemas tecnológicos en todos los aspectos de la vida cotidiana han alterado radicalmente este paradigma. Estas nuevas tecnologías pueden ser un vehículo para la difusión de rumores y falsedades, como se pudo comprobar durante la pandemia de la COVID-19, pero también son un medio excelente para conocer al menos una parte de la verdad como sucede en el conflicto actual entre la Federación de Rusia y Ucrania.

Simultáneamente, los hechos parecieran que no pueden ser ocultados. Para Thomas L. Friedman en la guerra entre Rusia y Ucrania, a la que considera *"world war wired"* ("guerra mundial conectada") "cualquier persona con un teléfono inteligente puede ver lo que sucede en Ucrania, en vivo y en color, y expresar opiniones en el nivel mundial a través de las redes sociales" (Friedman, 2022).

En el período previo a la invasión rusa de Ucrania y durante todo el conflicto en curso, las redes sociales han servido como campo de batalla para que los estados y

los actores no estatales difundan narrativas contradictorias sobre la guerra y retraten el conflicto en curso en sus propios términos. A medida que la guerra se prolonga, estos ecosistemas digitales están inundados de desinformación. Las campañas de propaganda estratégica, incluidas las que venden desinformación, no son de ninguna manera nuevas en la guerra, pero el cambio a las redes sociales como el principal canal de distribución está transformando la forma en que se libra la guerra de información, así como las personas que pueden participar en conversaciones en curso para dar forma a las narrativas emergentes (Perez, 2022).

Otro ejemplo del poder de las redes es lo ocurrido en Irán cuando, el 16 de septiembre de 2022, tras la muerte bajo custodia policial de Mahsa Amini, de 22 años, quien había sido arrestado por la «policía moral» iraní por violar las reglas sobre el código de vestimenta se produjeron manifestaciones generalizadas cuyas imágenes recorrieron el mundo (Aljazeera, 2022) y cuyas consecuencias se observan hasta dos meses más tarde, día en que esto se escribe.

ILUSTRACIÓN 20 . **Protesta en Teherán, Irán, por la muerte de Mahsa Amini, el 21 de septiembre de 2022.**

FUENTE: *(JESSIE YEUNG, 2022).*

Ante la decisión del gobierno de Irán de restringir Internet bloqueando el acceso a servicios como Instagram, Whats App y Skype (otras redes sociales extranjeras como Facebook, Twitter y TikTok ya estaban bloqueadas) para impedir la difusión de las protestas, Estados Unidos eximió de sanciones a las compañías extranjeras que operen en Irán proporcionando computación en la nube, redes sociales y videoconferencias. Ante ello, Elon Musk activó "Starlink» en Irán y Signal, cuya aplicación había sido bloqueada desde enero, pidió a sus usuarios que configuren servidores proxy, lo que permite a los iraníes eludir los controles de Internet y acceder a Signal (Gordon, 2022).

Pero, así como el empleo de plataformas multicanal y redes sociales como Facebook, Twitter, Instagram, Flickr o YouTube permiten influir en la opinión pública propia, adversaria y neutral mediante actividades de propaganda y contrapropaganda, también facultan a recopilar un vasto volumen de información sobre un enemigo susceptible de transformarse en inteligencia útil para las operaciones.

Precisamente por ello, muchos ejércitos han integrado la dimensión cibernética en las labores de comunicación estratégica; realizan operaciones de información (INFOOPS) y operaciones psicológicas (PSYOPS) en el ciberespacio; llevan a cabo actividades de inteligencia de fuentes abiertas (OSINT) en Internet e incluso explotan la valiosa información que proporcionan las redes sociales virtuales (SOC-

MINT)[86]. No obstante, aunque muchas fuerzas armadas se han subido al carro de las redes sociales de forma más o menos efectiva y con una estrategia más o menos clara, el uso personal que sus integrantes hacen de las mismas puede suponer tanto una amenaza para la seguridad nacional y un riesgo para las operaciones militares como representar un problema de comunicación pública (Chamorro G. C., 2015).

ILUSTRACIÓN 21 . **SOCMINT o la Inteligencia de Redes Sociales (Social Media Intelligence)**

FUENTE: *(INSTITUTE, 2021).*

En este escenario han surgido algunos términos y otros se han "revitalizado" o actualizado como Guerra de la Información, Guerra Cognitiva, Operaciones de Influencia, Comunicación Estratégica, Operaciones de Información, Operaciones Psicológicas, Comunicación Social, Narrativa, Propaganda, Desinformación, *Maskirovka*, Control Reflexivo, *Hasbara*[87], (diplomacia pública y campaña cognitiva) que de una u otra manera pretenden reflejar aquellas acciones que se llevan a cabo, antes, durante y después de un conflicto armado, con el propósito de alterar las percepciones de las sociedades no sólo en las zonas en disputa, sino más ampliamente. Existen numerosas definiciones para ellos dadas por instituciones creíbles, pero cada una varía un poco de la otra, oscureciendo la claridad conceptual.

Como señala Carlos Galán "Desde hace unos años, los términos guerra no convencional y amenazas o conflictos irregulares, amenazas híbridas, guerra híbrida, *fake*

86 SOCMINT o la Inteligencia de Redes Sociales (Social Media Intelligence) es un tipo de Inteligencia mediante la cual se puede recoger, integrar y compartir grandes cantidades de información obtenidas de las redes sociales. SOCMINT se está convirtiendo en una herramienta muy útil para analizar las redes sociales y toda la información que se comparte, pero también en una posible amenaza para la privacidad de los millones de usuarios que utilizan las redes sociales a diario (Institute, 2021).

87 Hasbara: en hebreo "explicación, esclarecimiento"

news, desinformación, etc. se han ido incorporando al universo y al diálogo de la seguridad y la defensa, sin que, en ocasiones, se hayan usado adecuadamente, confundiendo unos con otros o simplemente otorgándoles un nombre y unas características muy alejadas de la realidad" (Galán, 2018).

Por tal razón, en este capítulo se analizarán las definiciones sobre las diversas características o clases de formas de hacer guerra (*warfare*) en el ambiente de la información entendido como el ámbito donde los seres humanos y sistemas automatizados observan, orientan, deciden y actúan, y que por lo tanto es el principal ambiente de toma de decisiones. Es la combinación de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información.

Para permitir la continuación de posteriores estudios, el análisis se realizará mediante la comparación de términos entre los Estados Unidos de América (EE.UU.), el Reino Unido de Gran Bretaña e Irlanda del Norte (RUGBIN), el estado de Israel, la República Federativa de Brasil y la República de Chile. Al examinar las distintas definiciones doctrinarias, se expondrán las coincidencias y diferencias que existen entre los Estados Unidos y la OTAN y entre los mismos países que integran la organización, como así también las definiciones de países sudamericanos donde también se advertirán contrastes.

Igualmente se mostrará que las mismas no son operaciones que se ejecutan en el ambiente de la información de manera aislada sino que también constituyen un subconjunto de lo que se conocen como Operaciones de Influencia, en las cuales el poder de la información se coordina, integra y sincroniza con otros poderes de un Estado, como son el diplomático, el económico y el militar para influir, corromper o usurpar la toma de decisiones de un grupo o individuo, para fomentar actitudes, comportamientos o decisiones de la audiencia objetivo que promuevan las metas, intereses y objetivos de la parte instigadora.

En todos los casos se analizarán no solo los aspectos teóricos, sino que también se expondrán distintos casos históricos y de reciente data.

2. **La niebla de conceptos**

Frecuentemente, expresiones como *guerra de la información - operaciones de influencia - comunicación estratégica - operaciones de información, operaciones en el ambiente de la información* son utilizados indistintamente para describir diferentes actividades lo cual genera confusiones doctrinarias y conceptuales. Lo que complica aún más las cosas es el hecho de que estas definiciones también se enfrentan a la interpretación internacional o a la de empresas privadas como Facebook, con lo cual, resulta difícil compararlas.

Además, los analistas utilizan con frecuencia otros términos para categorizar actividades similares relacionadas con la información, incluyendo "operaciones psicológicas", «operaciones de influencia», «guerra política» y «manipulación social hostil». Igualmente están acuñando nuevas combinaciones de estos términos, como «guerra de información y operaciones de influencia» y «operaciones cibernéticas de influencia» (Stockton, 2021):

> Los políticos estadounidenses, los militares y las compañías de redes sociales no están de acuerdo sobre cómo deben definirse las operaciones de información y continúan inventando nuevos términos para ellas. La Comisión Asesora de Diplomacia Pública de los Estados Unidos descubrió en 2020 que hay «cientos de formas de describir aspectos de las operaciones de influencia maligna: desinformación, desinformación, propaganda, operaciones de información y operaciones psicológicas, por nombrar solo algunas».

El problema de esta verdadera abundancia de términos que aluden a la vertiente cognitiva de los conflictos no es tanto el solapamiento de múltiples palabras para designar una misma realidad, sino el uso como sinónimos de conceptos que tienen un alcance y un contenido en ocasiones muy diferente (Soriano, 2022).

Según Luis Feliú Ortega, "Hasta hace algunos años no existía un problema respecto de las definiciones "porque se seguía el método cartesiano y por la influencia de los sistemas francés y alemán cuyos idiomas son muy precisos. Sin embargo, en la actualidad, la influencia de las doctrinas anglosajonas muy poco proclives a preocuparse de la precisión en el lenguaje y la tendencia a utilizar la ambigüedad y los eufemismos en la utilización de determinados conceptos, han hecho que exista bastante confusión" (Feliú, 2012).

Es por ello que se tratará de proporcionar una mayor comprensión y claridad en las definiciones en occidente, y también identificar las diferencias existentes partiendo de la base que, como podrá verse, varias de estas operaciones, son consideradas herramientas ofensivas y defensivas para contrarrestar la desinformación estatal y no estatal que países como China, Rusia, Irán y otros actores llevan adelante contra los Estados Unidos, los países de la OTAN y otros aliados.

2.1. **El ambiente[88] de la Información**

Dado que el Glosario de Términos de Empleo Militar para la Acción Militar Conjunta 2020 del Estado Mayor Conjunto de las Fuerzas Armadas de la República Argentina no lo define, aunque si lo menciona cuando lo hace respecto de las Operaciones de Información en esta parte de la investigación se indagará sobre las definiciones que sostienen otros países (República Argentina EMCO, PC 00-02, 2019).

La República de Chile en su Doctrina Nacional Conjunta indica que el Entorno de la Información es definido como el espacio físico y virtual en el cual la información es recibida, procesada y trasmitida. Comprende las informaciones en sí, los actores y líderes propiamente tales y los sistemas de información (Chile Ministerio de Defensa Nacional, DNC 3-7, 2014). El entorno de información propio es donde los seres humanos y los sistemas automatizados observan, orientan, deciden y actúan de acuerdo a la información y por lo tanto es el ambiente principal de toma de decisiones.

---

88 Dominio: Ámbito real o imaginario de una actividad; RAE.

La Doctrina del Ejército de la República Federativa de Brasil precisa que la dimensión de la información (AI) es: "el conjunto de individuos, organizaciones y sistemas en los que los responsables de la toma de decisiones utilizan para obtener, producir, difundir y actuar sobre la información. Esta dimensión se compone de tres perspectivas interrelacionadas que interactúan continuamente, entre sí, y con individuos, organizaciones y sistemas. Estas perspectivas son: física, lógica y cognitiva" (Brasil Exército Brasileiro, EB70-MC-10.213, 2019).

ILUSTRACIÓN 22 . **Perspectivas física, lógica y cognitiva**

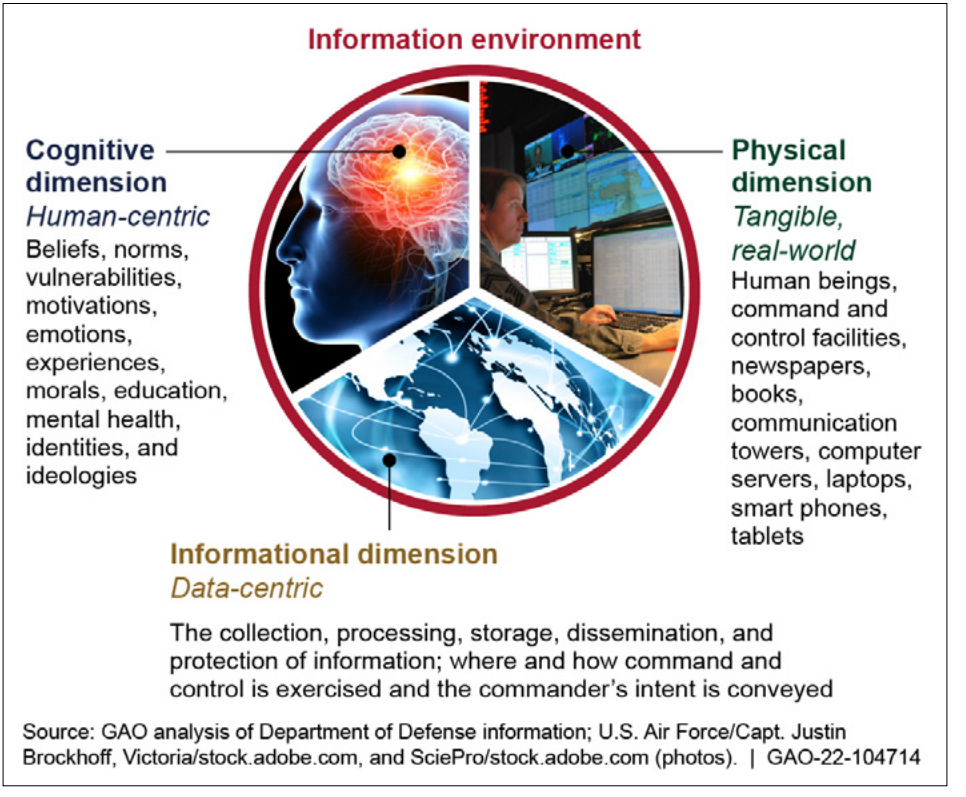
FUENTE: *(BRASIL EXÉRCITO BRASILEIRO, EB70-MC-10.213, 2019)*

Por su parte, la Doctrina Conjunta de los Estados Unidos fue variando su definición desde 1998 y la Publicación Joint Publication 3-13 Information Operations (recientemente derogada) lo definía como:

> El agregado de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información. Este ambiente consta de tres dimensiones interrelacionadas, que interactúan continuamente con individuos, organizaciones y sistemas. Estas dimensiones se conocen como físicas, informati-

vas y cognitivas. La dimensión física se compone de sistemas de comando y control, tomadores de decisiones clave e infraestructura de apoyo que permite a los individuos y organizaciones crear efectos. La dimensión informativa especifica dónde y cómo se recopila, procesa, almacena, difunde y protege la información. La dimensión cognitiva abarca las mentes de aquellos que transmiten, reciben y responden o actúan sobre la información. de individuos, organizaciones y sistemas que recopilan, difunden o actúan sobre la información.

ILUSTRACIÓN 23 . **Dimensiones del ambiente de la Información**



FUENTE: *(UNITED STATES GAO, 2022)*

La publicación Joint Concept for Operating in the Information Environment (JCOIE) de 2018 refiriéndose a un modelo similar al de la ilustración aclara que el ambiente de la información (IE):

> Se centra en la transmisión, el procesamiento y el almacenamiento de información dentro de tres dimensiones interrelacionadas pero distintas. La intención

> original de este modelo era ayudar a la Fuerza Conjunta a visualizar cómo compartir información internamente, garantizar el comando y el control, e interrumpir el flujo de información enemiga. La intención no era abordar cómo las audiencias con diferentes visiones del mundo interpretan y contextualizan la información. El modelo asume que cualquier ventaja o desventaja en el IE es el resultado de una transmisión efectiva o ineficaz de información. La transmisión efectiva no siempre equivale a una comunicación efectiva. (United States Joint Chiefs of Staff, JCOIE, 2018)

El 14 de septiembre de 2022 fue promulgada la publicación *Joint Publication* 3-04 - *Information in Joint Operations,* de nivel operacional, la cual expresa que:

> Dentro del ambiente operacional (OE) de cada comandante existen factores que afectan la forma en que los humanos y los sistemas automatizados[89] deducen el significado, actúan y se ven afectados por la información. Nos referimos al agregado de estos factores sociales, culturales, lingüísticos, psicológicos, técnicos y físicos como el ambiente de la información (IE) el cual no es distinto de cualquier OE. Es un marco intelectual para ayudar a identificar, comprender y describir cómo esos factores a menudo intangibles pueden afectar el empleo de las fuerzas y afectar las decisiones del comandante (United States Joint Chiefs of Staff, JP 3-04, 2022).

Esta publicación replantea las dimensiones del ambiente de la información en aspectos físicos, informativos y humanos en lugar de físicos, informativos y cognitivos como lo habían hecho las anteriores versiones y explica que este modelo establece un nuevo enfoque que es una forma de describir las diferentes características de los objetos, actividades o actores relevantes; y el contexto en el que existen y sobre el que se actúa. Juntos, los tres aspectos proporcionan el contexto necesario para comprender cómo operan los individuos, los grupos, las poblaciones y los sistemas automatizados (United States GAO, 2022).

Los aspectos describen colectivamente cómo un actor relevante recibe información y los factores que afectan el procesamiento e interpretación de esa información (United States GAO, 2022):

- El aspecto informativo refleja la forma en que los individuos, los sistemas de información y los grupos se comunican e intercambian información. Este es el contenido, el medio, el formato y el contexto de la transmisión e interpretación de la información.
- El aspecto físico se refiere a las características materiales del entorno que pueden influir en la capacidad de comunicarse. Esto puede referirse a una estruc-

89 Los sistemas automatizados son los conjuntos de software y hardware que permiten que los sistemas informáticos, dispositivos de red o máquinas funcionen sin intervención humana.

tura geográfica o hecha por el hombre en el medio ambiente o puede referirse a otras normas físicas de comunicación entre una población determinada (por ejemplo, una preferencia por la comunicación cara a cara en lugar de la comunicación escrita o telefónica).

- El aspecto humano se refiere a las interacciones entre las personas y cómo el entorno da forma al comportamiento humano y la toma de decisiones. Este aspecto se basa en los elementos lingüísticos, sociales, culturales, psicológicos y físicos de la comunicación e impacta cómo la mente humana aplica significado a la información que ha recibido, es decir, cómo las personas piensan sobre la información y toman decisiones basadas en esta información.

El ambiente de la información, da sentido a la forma en que una variedad de actores emplea un conjunto diverso de tácticas, técnicas y procedimientos para afectar la toma de decisiones, las creencias y las opiniones de un público objetivo y de esa manera tratar de influir en la dirección y el resultado de la competencia y el conflicto. El nexo de las dimensiones es donde los humanos y las máquinas se unen recibiendo información para tomar decisiones y ejercer el control.

Es omnipresente. Es en gran parte ilimitado, relativamente no regulado, hiperconectado, y existe simultáneamente en todos los dominios y conjuntos de problemas. Es de naturaleza global, es un sistema de sistemas altamente complejo y emergente en el que la información se mueve y produce impactos con una velocidad que aumenta rápidamente y a menudo impactos de alto orden e imprevistos. Comprende una amplia gama y diversidad de actores con una influencia agregada mucho mayor que la que tuvieron en el siglo anterior.

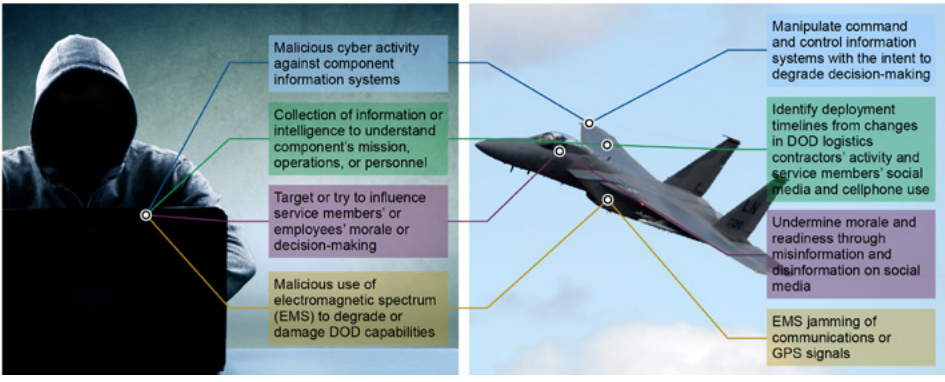
Dentro de él, tanto civiles como militares intentan obtener una ventaja para lo cual llevan a cabo distintas "guerras" y "operaciones" muchas de cuyas definiciones siguen siendo un tema complejo pues dependen del contexto y del nivel del que se habla. Estas definiciones por lo general no son coincidentes ni en el nivel de las propias fuerzas armadas y mucho menos en el nivel internacional con lo cual se produce una confusión que no contribuye a aclarar la naturaleza siempre cambiante de las operaciones en este ambiente.

Es donde se crea, explota o interrumpe el conocimiento. Las acciones pueden ser positivas o mejorar los esfuerzos para fortalecer los intereses nacionales, como la diplomacia o la comunicación estratégica. También pueden ser operaciones psicológicas, operaciones de información u operaciones de influencia. Finalmente, las acciones se pueden desarrollar para negar a otro actor el acceso o el uso de la información para obtener una ventaja de la información, incluida la negación, la interrupción, la desinformación o la información engañosa *(misinformation).* Este ámbito también incluye la protección de la propia información y el acceso a la información, así como las capacidades asociadas (United States Marine Corps, 2021).

Hoy en día, combatir en el ambiente de la información permite el control de los ambientes humanos de un adversario a través de la integración de las operaciones psi-

cológicas, de la información a través de la guerra cibernética y físicos por medio de actividades en el espectro electromagnético.

ILUSTRACIÓN 24 . **Amenazas en el Ambiente de la Información**



FUENTE: *(UNITED STATES GAO, 2022):*

El ambiente de la información comprende al ciberespacio, el ámbito más nuevo, a menudo difícil de entender. A diferencia de otros donde existen mapas y gráficos para describir las características físicas y los límites, permanece en gran medida inexplorado. No obstante, podría ser definido como: «Un dominio global dentro del ambiente de la información que consiste en la red interdependiente de infraestructuras de tecnología de la información y datos residentes[90], incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados" (United States Jont Chiefs of Staff, JP 3-12, 2018).

El Glosario de Términos de Empleo Militar para la Acción Militar Conjunta lo define como el "Ámbito tanto físico como virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de la información y comunicaciones. Constituye un ámbito de actuación operacional del Instrumento Militar y otros actores cibernéticos" (República Argentina EMCO, PC 00-02, 2019).

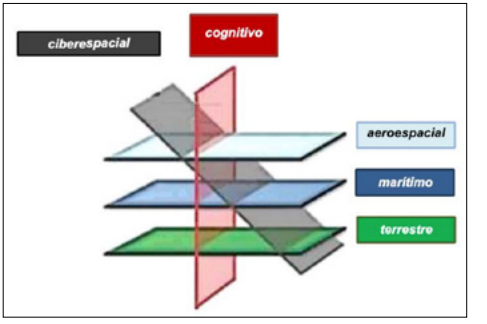
La doctrina militar conjunta española evita el término "dominio" y utiliza únicamente el de "ámbitos de operación" para referirse a «[...] los espacios físicos y no físicos, con características propias y diferenciadas, que condicionan las actitudes y procedimientos de los medios, fuerzas y capacidades que deben operar en ellos". De este

90 Datos de residentes significa toda la información personal de salud, financiera y demográfica identificable individualmente relacionada con las personas que residen en las comunidades o que reciben servicios de empresas, incluida, entre otras, "información de salud protegida".

modo, identifica a los ámbitos terrestre, marítimo, aeroespacial, cognitivo y ciberespacial (Ilustración 25).

La singularidad del planteamiento español con respecto a otras doctrinas aliadas radica en cuatro diferencias esenciales. En primer lugar, estaría la fusión de los ámbitos aéreo y espacial en un amplio concepto "aeroespacial". En segundo lugar, la no consideración de la información como ámbito. En tercer lugar, el ciberespacio –que en otras doctrinas estaba considerado como un dominio dentro del ámbito de la información- asciende a la categoría de ámbito y queda equiparado los tradicionales terrestre, marítimo, aéreo y otros. Y finalmente, aparece un "ámbito cognitivo" separado y también equiparado al resto de los ámbitos físicos y no físicos (Yeste, 2020).

ILUSTRACIÓN 25 . **Los ámbitos de operación de las Fuerzas Armadas de España (FAS)**



FUENTE: *(ESPAÑA MINISTERIO DE DEFENSA, PDC-01, 2018)*

Sin embargo, para Yeste (2020):

> No parece adecuada la concepción española en cuanto a considerar un ámbito cognitivo independiente y equiparado al resto de los ámbitos. El motivo es que en el terreno cognitivo no se pueden llevar a cabo acciones militares de manera directa, es decir, no se puede operar. Sólo es posible esperar efectos tras ejercer las correspondientes acciones en los ámbitos físicos y/o virtuales. Así, por ejemplo, no es posible llevar a cabo directamente acciones sobre los procesos mentales de los soldados para que deserten, ni sobre los del comandante para que rinda su unidad. Sólo es posible intentar provocar dichas decisiones, o al menos influir en ellas, a través de ejercer acciones en los ámbitos físicos (ej. iniciando un ataque) o a través del ámbito de la información (ej. anunciando de manera creíble dicho ataque).

El ciberespacio da forma y modifica el ambiente de la información cuando se crea una información, cuando se comparte ese contenido y cuando se ven afectadas la interacción y la comunicación humanas.

En el ciberespacio se puede entre otras cosas:

- Sabotear ciertos sistemas de información con lo cual es probable que estas operaciones produzcan efectos cognitivos ya sea evitando el acceso a una plataforma, desfigurando un sitio web, interrumpiendo la emisión de un canal de televisión mientras se publican en sus cuentas de Facebook y Twitter mensajes en apoyo al oponente, presentando documentos, direcciones y currículos de militares o agentes de fuerzas de seguridad mediante operaciones cibernéticas (CYBEROP);

- Al igual que en el engaño clásico ocultar, simular o confundir al adversario por medio de operaciones de ciber engaño (MILDEC). Tan pronto como las fuerzas armadas utilizan sistemas digitalizados para comunicarse, se exponen a la intrusión y la manipulación de, por ejemplo, un sistema de vigilancia aérea para ocultar la penetración de aviones de combate engañando a los operadores radar; simulando un ataque falso, usurpando la identidad de una alta autoridad del teatro de operaciones modificando las órdenes enviadas a las unidades;
- Explotando áreas de menor seguridad de los usuarios oponentes, por ejemplo, la presencia de combatientes en las redes sociales a título privado con lo cual pueden ser objeto de campañas de influencia en sus cuentas personales o geolocalizando sus fotos en cuentas personales y de esa manera obteniendo la ubicación de las bases militares (OPSEC);
- Filmando acciones de combate para desbaratar fotos y comunicados de prensa falsos mostrando supuestas atrocidades luego de los combates publicados por el oponente (COMCAM); y
- Falsificando las posiciones de buques de guerra, mediante la alteración de sus Sistemas de Identificación Automática (AIS) o interfiriendo las comunicaciones del oponente y contraatacando sus ciberataques.

El ciberespacio es un ámbito en el que los adversarios buscan información sobre los demás. Todo el mundo está espiando a todos, para descubrir intenciones, para adquirir conocimiento, o para dar forma a las creencias y, por lo tanto, a los comportamientos. China ha robado tecnología industrial militar y civil de Occidente a través de operaciones cibernéticas. Rusia las ha utilizado para tratar de influir en la política interna de las naciones objetivo. Estados Unidos y quizás Israel han utilizado ataques cibernéticos para contrarrestar los esfuerzos iraníes en la proliferación nuclear (Nadiya Kostyuk, 2022).

La globalización y la inmediatez son, sin duda, las primeras características llamativas del ciberespacio. La inmediatez es el resultado del flujo electrónico de información y la globalización de la interconexión de redes. La personalización y la opacidad son otras dos particularidades que están transformando en gran medida la práctica de las operaciones de información. La horizontalidad y la interactividad también son especificidades del ciberespacio, especialmente desde el advenimiento a principios de la década de 2000 de la "Web 2.0». Cada consumidor de información es ahora también un productor y organismo de radiodifusión potencial. Existe una gran porosidad entre las plataformas de redes sociales, medios tradicionales (a través de comentarios), foros de discusión o aplicaciones de mensajería. La última peculiaridad del ciberespacio en términos de influencia es su plasticidad, es decir, la facilidad de crear, ahogar o modificar un conjunto de contenidos (Tenenbaum, 2021).

Conectar máquinas a máquinas y humanos a máquinas aumenta exponencialmente la cantidad de datos que se mueven a través del ciberespacio. En la actualidad, el movimiento entre niveles de información no solo ocurre más rápido que en cualquier

otro momento de la historia pues el uso de máquinas permite el procesamiento de significativamente más datos, más rápidamente que nunca.

Cualquier movimiento que se realiza en la red, cualquier exploración en los buscadores de Internet, cualquier página visitada o cualquier comentario que se haga en las redes sociales virtuales proporciona una información muy valiosa para perfilar la personalidad de un individuo mediante la identificación de preferencias, gustos, intereses, ideología, estado civil, nivel educativo y cualquier otra información que pueda ser de interés para empresas, gobiernos, servicios de seguridad o delincuentes. Además, la incorporación de estas informaciones procedentes de múltiples fuentes junto con los datos personales, bancarios, administrativos, económicos o académicos sienta las bases del Big Data, que en los próximos años se convertirá –si aún no lo ha hecho– en el "Gran Hermano" de la Era de la Información y donde nadie que tenga una identidad digital y presencia en la red podrá evadirse a su control casi absoluto (Chamorro G. C., 2015).

Con el fin de extraer significado de esta creciente serie de datos, se han desarrollado y formalizado los distintos campos de la ciencia de datos *(Data Science),* el aprendizaje automático *(Machine Learning)* y la inteligencia artificial *(Artificial Intelligence).* Si uno observa la definición del ciberespacio, es difícil creer que estos campos puedan existir sin él[91].

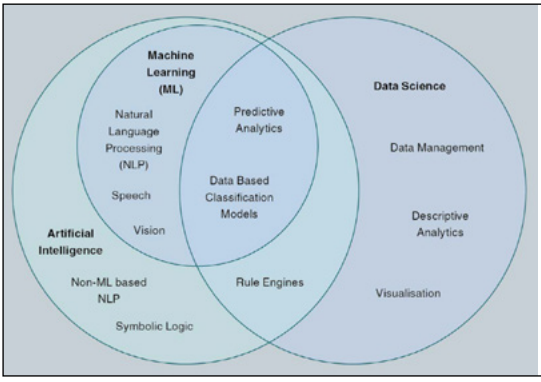
A través de la inteligencia artificial se puede mejorar el rendimiento de los sistemas automatizados para tareas complejas como la percepción (procesamiento de sonido e imagen), razonamiento (resolución de problemas), representación del conocimiento (modelado), planificación, comunicación (procesamiento de lenguaje) y sistemas autónomos (robótica). Por medio del aprendizaje automático (ML) los sistemas almacenan las palabras y las formas en que se combinan al igual que cualquier otra forma de datos. Frases, oraciones y, a veces, libros completos se incorporan a los motores de lenguaje donde se procesan según las reglas gramaticales, los hábitos lingüísticos de la vida real de las personas o ambos. La capacidad de un adversario para aprovechar el aprendizaje automático y potencialmente la inteligencia artificial para procesar información disponible públicamente en apoyo de sus ataques constituye una amenaza para los intereses de cualquier actor (Bell, 2018).

La inteligencia artificial imita la forma en que piensan las personas, adecuándose a directivas de estas, pero "piensa" al fin de un modo distinto. Los humanos piensan generalidades; la inteligencia artificial es prisionera de la especificidad: los algoritmos

91 La *ciencia de datos* se centra en mejorar la toma de decisiones a través del análisis de datos. El método general de aplicación es el abastecimiento, la agregación, la exploración de los datos y el análisis de patrones a través del aprendizaje automático para tomar mejores decisiones. El *aprendizaje de datos* se centra en el diseño y la evaluación de algoritmos (modelos matemáticos) para extraer patrones de datos. La *inteligencia artificial* tiene como objetivo construir máquinas que sean mejores para tomar decisiones y resolver problemas. Si bien hay varias definiciones de IA, en general, la IA se refiere a los sistemas informáticos que son capaces de resolver problemas y realizar tareas que tradicionalmente han requerido inteligencia humana y que mejoran continuamente en sus tareas asignadas.

que se usan para jugar al ajedrez no servirían para jugar al fútbol o explorar yacimientos de petróleo. Los algoritmos no son neutrales (Escribano, 2022).

ILUSTRACIÓN 26 . **Tecnologías superpuesta**



Inteligencia artificial: Máquinas que realizan tareas que normalmente requieren inteligencia humana, especialmente cuando las máquinas aprenden de los datos cómo hacer esas tareas.
Aprendizaje automático: algoritmos informáticos que pueden «aprender» encontrando patrones en datos de muestra y luego aplicarlos a nuevos datos para producir resultados útiles, a menudo utilizando redes neuronales.
Ciencia de datos: Investigación que implica el procesamiento de grandes cantidades de datos con el fin de proporcionar información sobre problemas del mundo real.

FUENTE: (UNITED KINGDOM MOD, 2022)

La mente humana se convierte en el campo de batalla. La información manipulada se presenta de tal manera que crea una percepción predeterminada que resulta en una acción anticipada entre el público objetivo para obtener una ventaja sobre el rival. Es la militarización de la opinión pública por parte de una entidad externa.

Las herramientas y armas que se están empleando utilizan el poder de la información, en lugar de, o además de, medios físicos para obligar a los adversarios y tomadores de decisiones a actuar.

La propaganda computacional es un nuevo término para el uso de las redes sociales, *big data,* agentes autónomos y tecnologías relacionadas para la manipulación política. Esto puede ir desde la amplificación relativamente benigna de los mensajes políticos hasta el trolling[92] y la desinformación patrocinados por el estado. El robot web, o «bot», es el tipo más común de agente autónomo utilizado en la propaganda computacional. Las capacidades de los *bots* se limitan a proporcionar respuestas básicas a preguntas simples, publicar contenido en un horario o difundir contenido en respuesta a desencadenantes. Sin embargo, los *bots* pueden tener un impacto desproporcionado porque es fácil crear muchos de ellos, los *bots* publican contenido con alto volumen y alta frecuencia, y sus perfiles generalmente están diseñados para imitar a su población objetivo de seres humanos (Kiesler, 2021).

Es así como la Guerra de la información es empleada por la política, la política internacional, y más específicamente durante la guerra significa: «Cualquier forma

92 Los trolls son aquellas personas que buscan provocar de manera intencionada polémica y conflictos con la finalidad de divertirse: Actúan en foros, blogs, redes sociales o cualquier otro soporte online. En general suelen adoptar identidades falsas que les permite navegar por las redes sociales.

de comunicación en apoyo de objetivos nacionales diseñados para influir en las opiniones, emociones, actitudes o comportamiento de cualquier grupo con el fin de beneficiar al patrocinador, ya sea directa o indirectamente» (Lavoix, 2022).

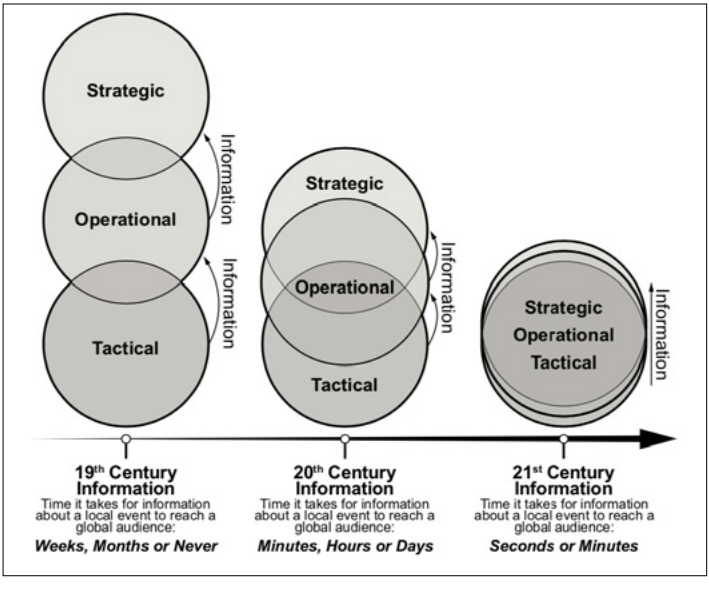
De esa forma se pueden crear dudas sobre el resultado de una elección, con lo cual la gente puede perder la confianza que tiene en la legitimidad de sus instituciones democráticas. El secuestro de cuentas de redes sociales puede usarse para difundir información falsa y alarmante; la votación puede verse afectada por la desinformación sobre un candidato difundida en vísperas de una elección con poco tiempo para desacreditar. Del mismo modo, se pueden sembrar desconfianzas sobre la validez de cualquier noticia con lo cual se socava la creencia en los medios de difusión y de la verdad en sí misma. la filtración de comunicaciones manipuladas puede abrir una brecha entre Estados.

ILUSTRACIÓN 27 . **Propaganda computacional**

FUENTE: *(BENTZEN, 2018)*

Pero también la naturaleza instantánea, global y persistente de la información comprime los niveles de guerra y aumenta las posibilidades de que una acción local tenga un impacto global (United States Marine Corps, MCDP8, 2022).

ILUSTRACIÓN 28 . **La información comprime los niveles de la guerra**



FUENTE: *(UNITED STATES MARINE CORPS, MCDP8, 2022).*

En resumen, la información puede ser vista desde muchas perspectivas doctrinarias y conceptuales diferentes. Por un lado, se considera como un instrumento de poder nacional, junto con los instrumentos diplomáticos, militares y económicos (DIME). También como una variable operacional para

fines de desarrollo y análisis de estrategias en la matriz PMESII (político, militar, económico, social, de información e infraestructura). Y también se describe como un dominio: «El dominio de la información es el conjunto de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información... Consta de tres dimensiones interrelacionadas: física, informativa y cognitiva" (Elder, 2021).

Aquí es donde radica el desafío, separar la planificación estratégica militar de la operacional y la táctica. Para ello se analizarán los conceptos de: guerra de la información, operaciones de influencia, comunicación estratégica, narrativa y operaciones en el ambiente de la información, a fin de tratar de dilucidar su significado y determinar a qué nivel de la guerra corresponde la planificación y ejecución de cada una de ellas.

2.2. **Guerra de la Información *(Information Warfare)***

La Publicación Glosario de Términos de Empleo Militar para la Acción Militar Conjunta 2020 la define como el "Uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente, pudiendo consistir en la recolección de información táctica, en la confirmación de la veracidad de la información propia, en la distribución de propaganda o desinformación a efectos de desmoralizar al enemigo, socavar la calidad de la información de la fuerza enemiga y negarle las oportunidades de recolección de información, pudiendo adquirir diversas formas" (República Argentina EMCO, PC 00-02, 2019).

Según Catherine A. *Theohary del Congressional Research Service* (CRS)[93] "Si bien actualmente no existe una definición oficial del gobierno de los Estados Unidos de guerra de la información (IW por sus siglas en inglés), generalmente se conceptualiza como el uso y la gestión de la información para obtener una ventaja competitiva, incluidos los esfuerzos ofensivos y defensivos. Es una forma de "guerra política", donde los objetivos incluyen el gobierno de un estado nación, las fuerzas armadas, el sector privado y la población en general" (Theohary, 2018).

Y agrega: "Aunque la Guerra de la Información y las Operaciones de Información parecen similares, el diferencial clave radica en el nivel en que se implementan. La primera ocurre en el nivel estratégico, mientras que las otras utilizan capacidades relacionadas con la información para implementar la estrategia» (Theohary, 2018).

La doctrina conjunta de los Estados Unidos reconoce sólo dos tipos de guerra: la guerra tradicional y la guerra irregular. Los documentos estratégicos y las publicaciones de cada Fuerza pueden utilizar el término «guerra de información» para describir

93 The Congressional Research Service (CRS) es un instituto de investigación de políticas públicas del Congreso de los Estados Unidos que trabaja dentro de la Biblioteca del Congreso, directamente para los congresistas y sus comités de forma confidencial y no partidaria. Sería un grupo de expertos del Congreso que investiga y analiza casi todos los asuntos relevantes para la formulación de políticas nacionales.

la movilización de información para lograr una ventaja competitiva y alcanzar los objetivos de política de los Estados Unidos.[94]

Guerra de Información es una estrategia de empleo de la información para buscar una ventaja competitiva, incluidos los esfuerzos ofensivos y defensivos. Es un medio a través del cual las naciones logran objetivos estratégicos y promueven metas de política exterior. Dado que el ciberespacio presenta un método fácil y beneficioso para comunicar un mensaje a grandes franjas de poblaciones, gran parte de la guerra de información actual tiene lugar en Internet, lo que lleva a combinar la guerra cibernética con la guerra de la información.

Para Catherine A. Theohary (2018):

> La guerra de la información no siempre implica decisiones convincentes o coercitivas; más bien, puede ser parte de una estrategia de «divide y vencerás» dirigida a la sociedad civil, sembrando confusión en una población objetivo para crear parálisis en las decisiones. Quienes deben tomarlas, son constantemente bombardeados por informes contradictorios, sin medios fácilmente disponibles para discernir la verdad.
>
> En ausencia de información confiable y enfrentando una mayor oposición de facciones en ambos lados de un problema, los tomadores de decisiones pueden ser incapaces de actuar. Este es el equivalente informativo de lo que Carl von Clausewitz acuñó como la «niebla y fricción» de la guerra. La niebla de la guerra se refiere a la incertidumbre en la conciencia situacional experimentada por los participantes en las operaciones militares, mientras que la fricción es un subproducto de esta niebla.

En la IW, en el nivel estratégico, no existe una distinción entre tiempos de paz y tiempos de guerra. Los esfuerzos se llevan a cabo para aprovechar la iniciativa en previsión de futuros conflictos o pueden ser un preludio de un conflicto armado, una preparación del campo de batalla que precede al despliegue de fuerzas. También puede ser un fin en sí mismo, un proceso a través del cual las naciones obtienen ventajas competitivas entre sí sin el uso de la fuerza.

Para Audrey Duperron la guerra de la información comprendería, entre otras, (Duperron, 2022):

- La destrucción o interrupción de los sistemas de comunicación y/o información del adversario;
- La recopilación de información clave sobre el adversario, sus estrategias y maniobras;

94 Por ejemplo, tanto la Fuerza Aérea estadounidense como la Armada de ese país utilizan ese término para abarcar la gama de esfuerzos ofensivos y defensivos que utilizan la información a través del continuo de la competencia para explotar el entorno de información contra los adversarios, informar a la opinión pública y obligar a los tomadores de decisiones a tomar ciertas acciones. (United States Joint Chiefs of Staff, JP 3-04, 2022).

- La neutralización de ciertos medios (televisión, radio), sitios web o redes informáticas del adversario; y
- la difusión de información o propaganda incorrecta para manipular la opinión pública del adversario o desmoralizarlo.

ILUSTRACIÓN 29 . **Guerra de Información**

FUENTE: *(PEPIN, 2018)*

Sin embargo, el término "Guerra de la Información", tanto para los EE.UU. como para la Organización del Tratado del Atlántico Norte (OTAN) no figura en sus diccionarios de terminología militar. Pareciera ser que la Guerra de la Información existe, pero quienes la llevan a cabo son los adversarios entendida como una forma de "guerra política" término que se atribuye al diplomático de la Guerra Fría George Kennan, quien la definió como (Theohary, 2018):

> El empleo de todos los medios a la orden de una nación, excepto la guerra, para lograr sus objetivos nacionales. Tales operaciones son tanto abiertas como encubiertas. Van desde acciones abiertas como alianzas políticas, medidas económicas y propaganda «blanca» hasta operaciones encubiertas como el apoyo clandestino a elementos extranjeros «amigos», la guerra psicológica «negra» e incluso el fomento de la resistencia clandestina en estados hostiles.

En la Estrategia de Defensa Nacional de 2018 de los Estados Unidos de América[95] cuando se refiere específicamente a la Guerra de la Información lo considera un medio a través del cual «los competidores y adversarios buscan optimizar su orientación de nuestras redes de batalla y conceptos operacionales, al tiempo que utilizan otras áreas de competencia que no sean la guerra abierta para lograr sus fines" (United States Joint Chiefs of Staff, JCOIE, 2018).

Lavoix-Carli sintetiza la definición de Guerra de la Información como "el uso por parte de un actor, generalmente un estado o un actor similar a un estado, pero que podría ser cualquier entidad, ya sea en guerra o en paz, de todos los medios posibles relacionados e involucrando información para ganar influencia sobre otros y ver los objetivos cumplidos. Los «otros» pueden ser cualquiera. Puede ser, por ejemplo, una audiencia nacional o extranjera" (Jean-Dominique Lavoix-Carli, 2022):

> Cuando la guerra de la información es utilizada por actores considerados hostiles o percibidos como el enemigo, entonces tiende a ser calificada como propa-

95 Una versión clasificada de la Estrategia de Defensa Nacional 2022 fue presentada al Congreso el 28 de marzo de 2022, y una versión no clasificada estará disponible para el público próximamente.

> ganda, que es un término peyorativo. Cuando, por el contrario, la información es utilizada por el propio patrocinador, así como por aliados y amigos, entonces esta actividad se etiqueta como comunicación estratégica.

Por tal razón, para la OTAN, "A fin de establecer una distinción clara entre los propios planes de comunicación y las actividades de información y los esfuerzos de los adversarios en el ambiente de la información, se sugiere utilizar términos como guerra de información o propaganda para ellos en lugar de aplicar términos propios" (NATO ACT, 2016). "Ellos" o "los «otros» pueden ser cualquiera. Puede ser, por ejemplo, una audiencia nacional o extranjera.

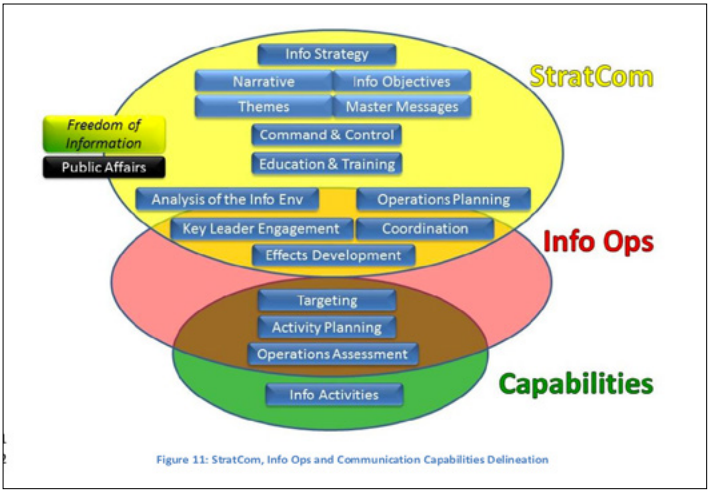
Sin embargo, para Grisé, el hecho de que "los otros" sean quienes llevan a cabo la Guerra de la Información puede deberse a que, "Según los académicos militares rusos, el término guerra de información apareció por primera vez en la literatura occidental en 1992. El Ministerio de Defensa de Federación Rusa definió la guerra de información como un «choque transparente y severo entre estados» que causa un «impacto dañino en el ambiente de la información». En la Conferencia del Ejército 2019, el ministro de Defensa Shoygu usó el término cuando señaló la «influencia agresiva de la información» de Occidente en Rusia (Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, 2022).

Pero sí puede encontrarse en la doctrina de occidente definiciones y referencias de Actividades de Influencia, Comunicación Estratégica, Narrativa y Operaciones en el ambiente de la Información.

Como podrá verse a continuación, las primeras son el efecto deseado que se pretende obtener a través de una comunicación estratégica planificada en el nivel nacional la cual, en el caso del ambiente militar, se lleva a cabo mediante las operaciones en el ambiente de la información (antes denominadas Operaciones de Información).

El modelo de la ilustración 30 permite expresar en forma sucinta términos que consistentemente causan dificultades en la doctrina y discusión

ILUSTRACIÓN 30 . **Líneas de enlace**

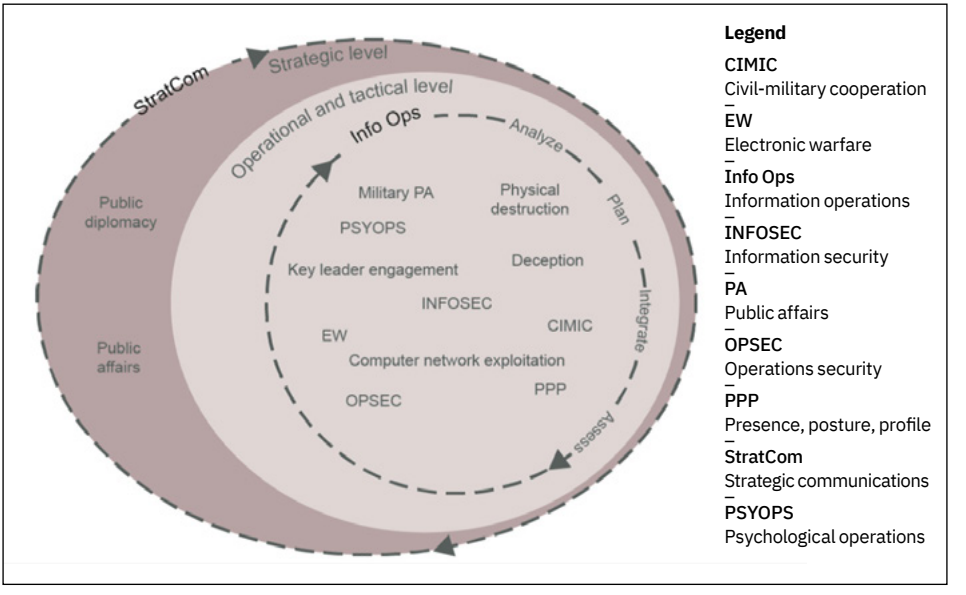


FUENTE: *(NATO ACT, 2016)*

militar y porque coloca la narrativa dentro del concepto más amplio de Comunicación Estratégica: (Tatham, 2010). En síntesis:

- Comunicación Estratégica: es un paradigma que reconoce que la información y la percepción afectan el comportamiento del público objetivo y que la actividad debe calibrarse contra los efectos de primer, segundo y tercer orden.
- Estrategia de la Comunicación: son los procesos y la secuenciación de la información para audiencias cuidadosamente dirigidas.
- Influencia: es el resultado final deseado de la Comunicación Estratégica.

ILUSTRACIÓN 31 . **Integración de las Operaciones Información con la Comunicación Estratégica**



FUENTE: (NATO, JP 3-10, 2015)

Otra forma de explicar la interrelación entre los distintos términos que se analizarán a continuación es el que muestra la ilustración 31.

2.3. **La Comunicación Estratégica**

En esta sección, se intentará mostrar que el desarrollo de la Comunicación Estratégica tiene un origen en el nivel estratégico nacional y de él deriva el accionar de las distintas agencias de un Estado pues básicamente, es "la capacidad de muchas organizaciones gubernamentales para coordinar y sincronizar un mensaje claro y articulado de los objetivos, políticas y valores de un gobierno a amigos, aliados, neutrales y adversarios en todo el mundo" (Wickramarachchi).

Otro término asociado es el de "diplomacia pública" la cual se define de diferentes maneras, pero en términos generales se emplea para "describir los esfuerzos de un gobierno para conducir la política exterior y promover los intereses nacionales a través del alcance directo y la comunicación con la población de un país extranjero. Las actividades de diplomacia pública incluyen el suministro de información al público extranjero a través de los medios de difusión y de Internet y en bibliotecas y otros servicios de divulgación en países extranjeros; llevar a cabo diplomacia cultural, como exposiciones de arte y actuaciones musicales; y administrar programas internacionales de intercambio educativo y profesional" (Nakamura, 2009).

Esta necesidad de ensamblar la "comunicación estratégica" y la "diplomacia pública" la explica la Subsecretaria de Diplomacia Pública y Asuntos Públicos cuando ante el Departamento de Defensa expresa: "a las audiencias masivas de todo el mundo realmente no les importa si se trata de noticias del Departamento de Defensa o la CIA o el Departamento de Estado, lo escuchan como noticias de Estados Unidos, por lo tanto es cada vez más importante que rompamos los silos y coordinemos y nos comuniquemos con una sola voz" (Hughes, 2007) a raíz de que en mayo de 2007, el gobierno de los Estados Unidos había publicado su Estrategia Nacional para la Diplomacia Pública y la Comunicación Estratégica escrita por el Comité de Coordinación de Políticas sobre Diplomacia Pública y Comunicación Estratégica, en un primer intento de coordinar los esfuerzos de Comunicación Estratégica en toda la comunidad interinstitucional (Loney, 2009).

Los *Asuntos Públicos* se refieren al público nacional.

En la República Argentina en 2019[96]. el Jefe del estado Mayor Conjunto de las Fuerzas Armadas argentinas al explicar la "Reconversión de las Fuerzas Armadas" expresaba:

> La Comunicación Estratégica constituirá el empleo planificado, coordinado e integrado de todas las capacidades y medios de comunicación que tiene a su disposición el Nivel Estratégico Militar con el objeto de generar percepciones/adhesiones favorables, en los ámbitos de interés conducentes al logro de los objetivos y desafíos estratégicos de la Defensa Nacional. Asimismo, se deberán identificar y desarrollar las acciones que permitan, en todos los niveles (Nivel Estratégico Militar, Nivel Operacional y Nivel Táctico), una comunicación estratégica eficaz tendientes a la prevención y/o resolución de los conflictos. (Sosa, 2019)

Para los Estados Unidos la Comunicación Estratégica son los "Esfuerzos enfocados del Gobierno de los Estados Unidos para comprender e involucrar a audiencias clave para crear, fortalecer o preservar condiciones favorables para el avance de los intereses,

96 El Glosario de Términos de Empleo Militar para la Acción Militar Conjunta 2019 del Estado Mayor Conjunto de las Fuerzas Armadas de la República Argentina no las define (República Argentina EMCO, PC 00-02, 2019).

políticas y objetivos del Gobierno de los Estados Unidos mediante el uso de programas, planes, temas, mensajes y productos coordinados sincronizados con las acciones de todos los instrumentos del poder nacional" (Staff, 2009) (Center, 2010).

La Publicación JP 5-0, *Joint Planning* 2017, retira este término del Diccionario del Departamento de Defensa pues dentro del Gobierno de los Estados Unidos (USG), el Departamento de Estado (DOS) tiene la responsabilidad principal de la supervisión de la sincronización de las comunicaciones. Está dirigido por el Subsecretario de Diplomacia Pública y Asuntos Públicos y es el mecanismo general por el cual el Gobierno de los Estados Unidos coordina la diplomacia pública en toda la comunidad interinstitucional.

> Un producto clave de este comité es la Estrategia Nacional de Estados Unidos para la Diplomacia Pública y la Comunicación Estratégica. Esto proporciona orientación, intención, imperativos estratégicos y mensajes centrales en el nivel de USG bajo los cuales el DOD puede anidar sus temas, mensajes, imágenes y actividades (United States Joint Chiefs of Staff, JCOIE JP5-0, 2017)[97].

En 2018 la publicación Joint Concept for Operating in the Information Environment (JCOIE) prescribe (United States Joint Chiefs of Staff, JCOIE, 2018):

> Las fuerzas armadas de los Estados Unidos desempeñan un importante papel de apoyo en los esfuerzos de comunicación, principalmente a través de la sincronización de la comunicación del comandante, los asuntos públicos, las operaciones en el ambiente de la información y el apoyo de defensa a la diplomacia pública. Las consideraciones relativas a la sincronización de las comunicaciones deben integrarse en toda la planificación conjunta de las operaciones militares, a partir de las actividades militares rutinarias y recurrentes durante los períodos de cooperación a través de los conflictos armados.
>
> Para apoyar la responsabilidad del Presidente de la Junta de Jefes de Estados Mayores (CJCS) como integrador global, la fuerza conjunta sincroniza las operaciones en el ambiente de la información para dar forma a las percepciones, decisiones y acciones de los actores relevantes, lo que incluye mensajes estratégicos. La mensajería estratégica son actividades de comunicación coordinadas y deliberadas para influir en el ambiente operacional en apoyo de los objetivos estratégicos de los Estados Unidos. Los mensajes estratégicos se desarrollan en conjunto con otros departamentos y agencias de USG, naciones amigas y ONG, según corresponda. Los Comandantes Combatientes (CCDR) deberán elaborar procedimientos de Estado Mayor para aplicar la orientación sobre la sincronización de las comunicaciones en todos los procesos conjuntos de planificación y selección, así

97 La edición 2017 fue remplazada por la de 2020.

> como procesos de colaboración para integrar las actividades de sincronización de las comunicaciones con asociados no militares y expertos en la materia.

La Publicación JP 3-04 de reciente edición, solo menciona el término "comunicación estratégica en tres oportunidades para indicar en una de ellas que en el Estado Mayor Conjunto, en el nivel estratégico militar, el J-5 (Director de Planes), junto con el J-2 (Director de Inteligencia), J-3 (Director de Operaciones), la Oficina del Secretario de Defensa (OSD), Asuntos Públicos (PA), Asuntos Públicos del Jefe del Estado Mayor Conjunto (CJCS PA), la Oficina del Subsecretario de Defensa para Políticas y la Oficina del Subsecretario de Defensa para Inteligencia y Seguridad, "Desarrolla y coordina una guía de información integrada globalmente, en el nivel de campaña vinculada a la dirección de seguridad nacional y la política de seguridad nacional y en apoyo de los objetivos de comunicaciones estratégicas de todo el gobierno.

> Además, el J-5 coordina la orientación y los planes de información estratégica con el Comité de Políticas Interinstitucionales del Consejo de Seguridad Nacional (NSC), la Comunicad de Inteligencia (IC) y el Departamento de Estado (DOS). Esta coordinación garantiza una alineación continua entre la comprensión de la amenaza, las acciones militares, incluidas las actividades de la Asuntos Públicos, y las contribuciones militares a la estrategia de comunicaciones nacionales / interinstitucionales y la orientación de comunicación (United States Joint Chiefs of Staff, JP 3-04, 2022)

Las otras dos se refieren a la OTAN expresando que: "Cada nación tiene capacidades, productos y recursos clasificados y no clasificados que son útiles para la fuerza conjunta y para las actividades de información de la fuerza multinacional. Por ejemplo, la División de Comunicaciones Estratégicas de la OTAN produce una evaluación del ambiente de la información que mejora la comprensión de las fuerzas conjuntas mediante la identificación de audiencias; evaluación comparativa de actitudes, percepciones y comportamientos; e identificación de procesos y sistemas de comunicaciones".

Ver a Vladimir Putin irrumpir en Crimea y el este de Ucrania en 2014, apoyado por sólidas campañas de información, puso en alerta a la Organización del Tratado del Atlántico Norte (OTAN). Sin posibilidad de llevar a cabo una respuesta cinética, tanto civiles y militares por igual buscaron aprovechar mejor la comunicación de la Alianza. En su declaración de la Cumbre de Gales de 2014, las naciones de la OTAN pidieron la mejora de la Comunicación Estratégica (SC por sus siglas en inglés) y crearon un Centro de Excelencia de Comunicaciones Estratégicas (StratCom CoE, por sus siglas en inglés) en Riga, Letonia.

En marzo de 2018, el Estado Mayor Internacional de la OTAN recibió el primer Grupo de Trabajo oficial del Comité Militar (MCWG) sobre Comunicaciones Estratégicas (StratCom). El Teniente General Jan Broeks, Director General del Estado Mayor Internacional de la OTAN destacó: «StratCom es un esfuerzo esencial que apoya la

disuasión efectiva de nuestros adversarios y promueve la comprensión de las acciones militares por parte de nuestras poblaciones y las poblaciones en el teatro». En el transcurso de la reunión, los participantes recibieron actualizaciones sobre las capacidades de StratCom, es decir, Asuntos Públicos Militares (Mil PA)[98], Operaciones de Información (InfoOps) y Operaciones Psicológicas (PsyOps) (NATO, 2018).

La OTAN define la Comunicación Estratégica como «el uso coordinado y apropiado de las actividades y capacidades de comunicaciones de la OTAN en apoyo de las políticas, operaciones y actividades de la Alianza, y con el fin de avanzar en los objetivos de la OTAN" e identifica los siguientes componentes de las comunicaciones estratégicas:

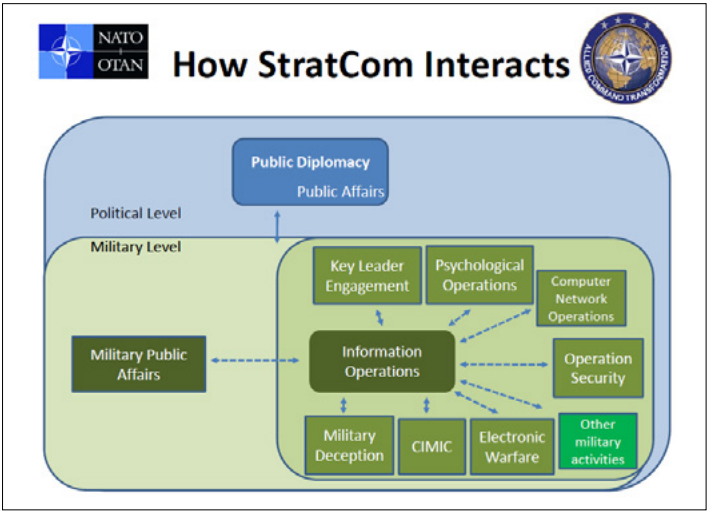
ILUSTRACIÓN 32 . **Comunicaciones Estratégicas de la OTAN**

FUENTE: *(LEPAGE, 2014)*

- Asuntos Públicos y Asuntos Públicos Militares;
- Diplomacia pública y apoyo militar a la diplomacia pública;
- Prensa y Medios de Comunicación;
- Actividades de información de cooperación militar internacional;
- Cooperación cívico-militar (CIMIC);
- Acciones en el ciberespacio, incluidas las redes sociales;
- Participación de líderes clave en eventos de información (Key Leaders Engagement);
- Comunicación interna (trabajo con el personal/relaciones públicas internas)
- Operaciones de información;
- Operaciones psicológicas (PSYOPS);
- Informar sobre la situación y documentar los acontecimientos en un campo de batalla;
- Eventos de sensibilización de apoyo de inteligencia;
- Demostración de fuerza;
- Engaño militar (MILDEC);
- Seguridad de la operación;
- Guerra electrónica (EMW) (NATO Centre for Global Studies , 2019).

98 Término que se refiere a los asuntos a tratar con los medios de comunicación y la comunidad.

ILUSTRACIÓN 33 . **Comunicación estratégica en la OTAN**



FUENTE: *(NATO, 2012)*

Para Tenenbaum y De Rochegonde, la *StratCom* tiene dos componentes. El primero es la comunicación institucional, incluida la diplomacia pública (para audiencias extranjeras) y los asuntos públicos (para la escena nacional). En el campo militar, puede dar lugar a una forma de comunicación operacional lo más cerca posible del teatro. Ambos se centran en promover la acción militar ante el público, los medios de comunicación y los responsables de la toma de decisiones (representación parlamentaria, socios extranjeros). No se trata de producir un efecto militar operacional en beneficio de la fuerza o del estado final deseado, incluso si la comunicación contribuye indirectamente a esto (Tenenbaum, 2021).

Según esta lista, las comunicaciones estratégicas en la OTAN también se basan en actividades de información. Los principios relevantes en el nivel nacional de StratCom de la OTAN son:

- Las palabras deben coincidir con las acciones.
- El ambiente de la información debe ser entendido.
- Toda actividad se basa en valores.
- Las acciones deben apoyar un objetivo, derivado de la política y la estrategia y alineado con la dirección política.
- La credibilidad y la confianza son recursos vitales.
- La comunicación es un esfuerzo colectivo e integrado.
- La comunicación debe enfocarse en los efectos y resultados.
- La comunicación está potenciada a todos los niveles. Las ramas del gobierno deben entender cuál es la «gran idea» que sustenta toda actividad. Se debe dar una dirección y orientación claras que permitan que el comando de la misión tenga lugar. (Gill, Heap, & Hansen, 2021)

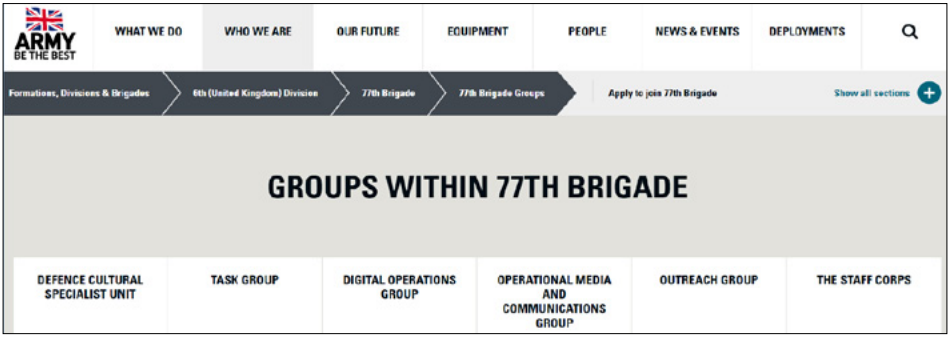
En 2018, la "Doctrina para el empleo de las Fuerzas Armadas" del Reino de España define la Comunicación Estratégica de la Defensa como "el empleo coordinado y apro-

piado de todas las capacidades de comunicación de la Defensa en apoyo de sus políticas, operaciones y actividades, con el fin de contribuir a la consecución de los objetivos de la Defensa Nacional" (España Ministerio de Defensa, 2018) y agrega: "La comunicación estratégica requiere de unidad de acción y una narrativa coherente para influir adecuadamente en todo tipo de audiencias".

En 2019 el Reino Unido definió la "comunicación estratégica" como "la forma de: promover los intereses nacionales mediante el uso de la Defensa como medio de comunicación para influir en las actitudes, creencias y comportamientos de las audiencias" (United Kingdom MoD, 2019). Esta definición se debió a que la anterior, de 2012, la definía como la forma de: «promover los intereses nacionales mediante el uso de todos los medios de comunicación de Defensa para influir en las actitudes y comportamientos de las personas» lo cual había creado cierta confusión en cuanto a lo que significaba exactamente.

"En respuesta a la amenaza de guerra de información, el ejército británico ha establecido dos nuevas formaciones: la 77ª Brigada para hacer frente a las operaciones psicológicas, y la 1ª Brigada de Inteligencia, Vigilancia y Reconocimiento, que combina la guerra electrónica y la inteligencia[99]. Cientos de expertos en informática serán reclutados como reservistas, entrenados con la ayuda de la Unidad Cibernética Conjunta del GCHQ" (Stupples, 2015).[100]

ILUSTRACIÓN 34 . **77ª Brigada**



FUENTE: *(UNITED KINGDOM ARMY, 2022)*

99 Estas formaciones realizan tareas específicas a nivel táctico (operaciones psicológicas e inteligencia). Son unidades que forman parte de la estructura física de las capacidades relacionadas con la información, son ejemplos de fuerzas estructurantes, como la organización del Comando de Operaciones Cibernéticas Reino Unido creó una la National Cyber Force (2020), una unidad militar de Ciencia y Tecnología de Defensa, bajo un comando unificado.

100 En 2020, se crea el 13º Regimiento de Señales dentro de la 1ª Brigada de Señales, bajo el mando de la 6ª División, responsable de realizar operaciones de información y guerra no convencional, en apoyo de todas las Fuerzas Armadas. La unidad proporcionará la base del nuevo Centro de Operaciones de Seguridad de la Información Cibernética del Ejército, centrándose en la protección del dominio cibernético de Defensa, y trabajará con la Royal Navy y la Royal Air Force para proporcionar redes seguras para todas las comunicaciones militares.

Otro actor no menos importante es la Organización de las Naciones Unidas (ONU) dentro de la cual, el cambio de la información pública a las comunicaciones estratégicas es relativamente nuevo. A principios de la década de 2000, el Departamento de Información Pública (DIP) de la ONU comenzó a reorientar su enfoque, incluso mediante la creación de una División de Comunicaciones Estratégicas para garantizar que «las comunicaciones se coloquen en el centro de la gestión estratégica de las Naciones Unidas». A pesar del progreso en varias áreas, esta reorientación no condujo a «una estrategia coherente y sistemática» para las comunicaciones. Fue solo en 2020 que la ONU desarrolló su primera estrategia global de comunicaciones, un movimiento que coincidió con el cambio de nombre de DPI como Departamento de Comunicaciones Globales. Según la ONU, la estrategia de comunicaciones 2020 «representa un cambio cultural para la Organización». El objetivo es fomentar una «cultura de comunicación y transparencia» que «impregne todos los niveles de la Organización como medio de informar plenamente a los pueblos del mundo de los objetivos y actividades de las Naciones Unidas». (Jake Sherman & Albert Trithart, 2021).

En cuanto al Estado de Israel puede decirse que el concepto también fue evolucionando con el tiempo y los conflictos en los que intervino. En la guerra de 2006 cuando se enfrentó al Hezbollah en el Líbano, Israel infligió enormes daños a la infraestructura libanesa, dejando más de 1.200 muertos y 4.400 heridos. Se estima que las bajas entre Hezbollah, el principal adversario de Israel, oscilaron entre 250 y 700 combatientes. Los daños a la infraestructura libanesa se valuaron en más de USD 2.5 mil millones, con casi 2,000 casas y edificios dañados y destruidos.

Esta cantidad de destrucción no obligó a Hezbollah a ceder y mientras ambos bandos reclamaban la victoria, Israel pagó un precio más alto en reacciones políticas y pérdida de reputación, principalmente debido a fallas en los medios de comunicación y la forma en que la guerra fue mostrada y percibida tanto en Israel como en el extranjero. Gran parte de esto se puede atribuir al uso eficiente de los medios de comunicación por parte de Hezbollah, y al fracaso de Israel en hacerlo. Según Teemu Saressalo, Israel manejó el siguiente conflicto de manera completamente diferente: había aprendido sus lecciones y construido nuevas formas de contrarrestar la propaganda y las operaciones mediáticas de su adversario (Saressalo, 2018).

Fojón Chamorro y otros autores (Chamorro F., 2012) sostienen: “Tras perder la “batalla de las narraciones” en los conflictos del Líbano (2006) y Gaza (2008- 09), las Fuerzas de Defensa de Israel (FDI) se vieron obligadas a replantear sus métodos y herramientas de Comunicación Estratégica. En la operación “Pilar Defensivo” de noviembre de 2012 Israel explotó el potencial de los medios de comunicación digitales – especialmente las redes sociales, las plataformas multimedia y los blogs– para informar de sus acciones y alterar la percepción pública del conflicto”.

Según David Siman-Tov y Ofer Fridman, “el término comunicación estratégica no se encuentra en el discurso académico y profesional israelí. En cambio, hay tres enfoques conceptuales diferentes para la comunicación estatal: *Hasbara*, diplomacia pública y campaña cognitiva” (David Siman-Tov y Ofer Fridman, 2020). Según los auto-

res, hasta principios de la década de 2000, dos conceptos prevalecían en las Fuerzas de Defensa de Israel (FDI): *Hasbara* y guerra psicológica. Al igual que otros ejércitos en el mundo, las FDI consideraron la guerra psicológica como una forma de influir en las percepciones de los soldados y comandantes enemigos, principalmente a través del uso del engaño y la desinformación.

> El objetivo principal de *Hasbara* es transmitir una narrativa específica a la audiencia deseada en un intento de influir en la opinión pública sobre un tema político particular relacionado con Israel. Hasbara es receptivo y no proactivo por naturaleza, con el objetivo de explicar las acciones de seguridad política en un intento de ganar apoyo y legitimidad. Sus actividades pueden ser llevadas a cabo por agencias estatales (varios ministerios gubernamentales), el ejército y ONG afiliadas al estado. (David Siman-Tov y Ofer Fridman, 2020)

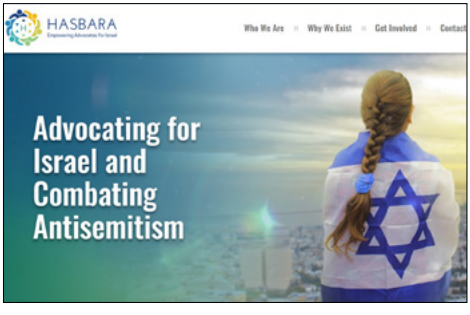
A principios de la década de 2000, las FDI comenzaron a centrarse en el componente cognitivo de las acciones militares y a mediados de la década de 2000, el Ministerio de Relaciones Exteriores introdujo el término «diplomacia pública» como un reemplazo de *Hasbara* que "implica la «promoción de un nexo de intereses de un país en otro país, mediante la creación de una imagen atractiva del primero basada en un diálogo con el público del segundo, a través del uso de la cultura, la ayuda mutua, el intercambio de delegaciones y otras actividades relevantes».

Para Siman y Fridman (2020):

> Israel no lleva a cabo comunicaciones estratégicas. En su lugar, se comunica estratégicamente, empleando varias instituciones y diferentes enfoques en un intento de encontrar la mejor respuesta posible a cada desafío que enfrenta. Ni la Hasbara, ni la campaña cognitiva, ni la diplomacia pública responden a los requisitos de la Comunicación Estratégica. En su lugar posee un conjunto de elementos diferentes, cada una de las cuales es desarrollado por una institución diferente, adecuada para un número limitado de ocasiones y dirigida a audiencias separadas y específicas.

En diciembre de 2021, el Primer Ministro israelí estableció la Dirección de Diplomacia Pública para coordinar *Hasbara* con el propósito de facilitar la sincronización de las narrativas de Israel, especialmente en tiempos de guerra entre diferentes organismos gubernamentales. Parte de las responsabilidades de la Dirección será desarrollar mensajes antes de las acciones militares y ayudar a las ramas del

ILUSTRACIÓN 35 . **Hasbara**



FUENTE:*(HASBARA, 2022)*

gobierno a aprender tanto de las fallas como de las mejores prácticas (Michael Starr, 2021).

Según la AMIA, "El jefe del sistema de información también se desempeña como asesor de medios del primer ministro israelí. Es responsable de trabajar con los medios de comunicación en Israel y en todo el mundo, así como con organizaciones pro-Israel en todo el mundo. También opera sitios web y el sistema de redes sociales de la Oficina del Primer Ministro. El puesto es crucial para combatir posturas anti-israelíes y antisemitas en el ámbito internacional. Hasbara es, justamente, el ejercicio de contar fuera de Israel lo que sucede en el país para fortalecerlo" (AMIA, 2021).

En la siguiente ilustración se resumen las distintas definiciones doctrinarias de Comunicación Estratégica que han sido indicadas en este trabajo:

ILUSTRACIÓN 36 . **Definiciones doctrinarias de Comunicación Estratégica**

Gobierno Estados Unidos (USG, 2012)	La *sincronización de* nuestras *palabras y hechos y cómo serán percibidos por otros,* así como programas y actividades deliberadamente dirigidos a comunicarse y comprometerse con las audiencias previstas, incluidas las implementadas por profesionales de asuntos públicos, diplomacia pública y operaciones de información.
España – 2018 (España Ministerio de Defensa, 2018)	El empleo *coordinado* y apropiado de todas las *capacidades de comunicación de la Defensa* en apoyo de sus políticas, operaciones y actividades, con el fin de contribuir a la consecución de los objetivos de la Defensa Nacional" Requiere de *unidad de acción y una narrativa* coherente para *influir* adecuadamente en todo tipo de audiencias.
OTAN - 2019 (StratCom NATO, 2019)	El uso *coordinado* y apropiado de las actividades y *capacidades de comunicaciones* de la OTAN *en apoyo de* las políticas, operaciones y actividades de la Alianza, y con el fin de avanzar en los objetivos de la OTAN.
UK Ministry of Defence 2019 (Defence, 2019)	La forma de promover los *intereses nacionales* mediante el uso de la Defensa como *medio de comunicación* para *influir* en las actitudes, creencias y comportamientos de las audiencias.
JP 5-0, *Joint Planning* 2020	Los *esfuerzos enfocados del gobierno* de los Estados Unidos (USG) para comprender e involucrar a audiencias clave para crear, fortalecer y preservar las condiciones para el avance de los intereses, políticas y objetivos del USG a través del uso de programas, planes, temas, mensajes y productos coordinados sincronizados con las acciones *de todos los instrumentos del poder nacional.*
Doctrine interarmées DIA-3.10(A)_ du 23 juin 2014, amendée le 12 mars 2018 (France Ministère des Armées, L 21, 2021)	Es el proceso que permite enmarcar el diseño y la realización de cualquier actividad militar de las fuerzas armadas francesas como un *mensaje coherente, creíble y efectivo* a los principales actores que tienen conocimiento de ella, ya sea una acción física o un discurso en todas sus formas.

FUENTE: DISTINTAS FUENTES INDICADAS EN CADA DEFINICIÓN.

De las definiciones analizadas se pueden extraer ciertos conceptos comunes:

- uso coordinado/coherente/planificado, por parte de todos los instrumentos del poder nacional;
- de todos los medios/capacidades de comunicación;
- para influir/generar percepciones/adhesiones favorables.

La comunicación estratégica se basa en «la comprensión inherente de que todas las actividades diplomáticas, de información, militares y económicas (DIME) tienen el potencial de influir en los comportamientos y actitudes de grupos específicos» (Jean-Dominique Lavoix-Carli, 2022):

> Como resultado, todas las actividades DIME pueden y deben convertirse en el objetivo de la comunicación estratégica si un actor quiere ver que su comunicación tenga éxito. Mientras tanto, todas estas actividades deben combinarse para crear una «comunicación estratégica» exitosa. Donde se vuelve aún más interesante es cuando la comunicación estratégica en sí misma trabaja en el uso de las actividades DIME de otros para llevar a cabo el objetivo propio. En el nivel individual, esto se llamaría simplemente manipulación. Las actividades de DIME que se dirigen así pueden ser no solo las de aliados y países amigos, sino también las de los competidores y enemigos.

Para Jente Althuis, "Hoy en día, las comunicaciones estratégicas se entienden ampliamente como la alineación de palabras, imágenes, acciones y políticas con la intención de lograr cambios en las actitudes y / o el comportamiento de un público objetivo" (Althuis, Jente, 2022).

Como cualquier otro aspecto de la estrategia, la comunicación estratégica se desarrolla desde arriba hacia abajo, estableciéndose sus fundamentos en el nivel político. Si hay algo peor que la ausencia de estrategia de comunicación, es una que rompa la coherencia entre el nivel político y sus niveles subordinados (Albero, 2020)

Si se entienden y diseñan adecuadamente, las comunicaciones estratégicas no se tratan solo de palabras, explicaciones o acciones, sino que también deben tratar de lograr los fines requeridos de la estrategia nacional, sobre todo explotando el poder comunicativo de los actos militares y no militares (Paul Cornish, 2011).

Para ello resulta necesario construir un marco teórico y una institución responsable de coordinar las palabras, imágenes y acciones producidas por todos los actores relevantes con la intención de influir en audiencias específicas en pos de intereses nacionales, de lo contrario, cualquier intento de comunicación estratégica estará destinado a encontrarse con dificultades. Es así que la comunicación deja de ser ocasional e inoportuna para ser planificada, integrada y dirigida a lograr objetivos pues la comunicación sin un plan es solo ruido.

Como complemento, puede decirse la Organización de las Naciones Unidas (ONU) cada vez reconoce más que las comunicaciones estratégicas son un medio

esencial para que las operaciones de paz cumplan con éxito sus mandatos de reducir la violencia y mantener la paz y gestionar las expectativas sobre lo que pueden y no pueden lograr.

Si bien la información pública y la comunicación han sido reconocidas desde hace mucho tiempo como herramientas importantes para las operaciones de paz de las Naciones Unidas[101], los rápidos cambios en el panorama de las comunicaciones, incluida la importante penetración de las redes sociales y el mayor uso de teléfonos inteligentes, plantean nuevos riesgos operacionales y de reputación para las misiones de la ONU. Estos cambios están siendo explotados por grupos armados y otras partes interesadas para moldear las percepciones del panorama político, socavar la confianza en las misiones y, a veces, movilizar la violencia contra civiles, personal de la ONU y otros objetivos (Jake Sherman & Albert Trithart, 2021):

> En respuesta, las operaciones de paz de la ONU están desarrollando sus capacidades para comunicarse con diversas partes interesadas nacionales, regionales e internacionales. Su objetivo no es solo contrarrestar conceptos erróneos, sino crear proactivamente narrativas alternativas en torno a su trabajo para mejorar la comprensión de lo que buscan hacer y cómo pretenden hacerlo, para generar confianza y disuadir a los posibles saboteadores. Están desarrollando mensajes convincentes, oportunos, orientados a un propósito y basados en historias adaptadas a diversas audiencias y difundidas a través de varios canales bidireccionales, trabajando frecuentemente con socios locales. Para hacer esto, necesitan comprender el panorama de los medios y la opinión pública y monitorear constantemente y ajustar regularmente su estrategia.
>
> Si bien las operaciones de paz de la ONU están tratando de mejorar sus capacidades de comunicación estratégica en respuesta a estos desafíos externos, los obstáculos internos también pueden impedir la mensajería efectiva. Un desafío es que los líderes de la misión no siempre ven al personal de comunicaciones estratégicas como una parte integral de la toma de decisiones, la programación y el compromiso político. Como señaló un funcionario, las comunicaciones estratégicas «a menudo se tratan como una ocurrencia tardía». Como resultado de ello, las comunicaciones de las misiones a menudo han sido reactivas, respondiendo a incidentes negativos en lugar de crear una narrativa convincente de progreso gradual.

En el examen estratégico independiente de 2019 de la MONUSCO[102] se indicaba que, la difusión de información pública y las comunicaciones estratégicas deben convertirse en partes esenciales de la planificación y ejecución de las actividades de compromiso

101 En 2020 la ONU desarrolló su primera estrategia de comunicaciones globales, un movimiento que coincidió con el cambio de nombre del Departamento de Información Pública (DPI) como Departamento de Comunicaciones Globales.

102 Misión de Estabilización de las Naciones Unidas en la República Democrática del Congo

político y protección de la Misión y orientar la transferencia gradual y responsable de sus funciones a las autoridades nacionales (NATO N19, 2019).

Es necesario que el aspecto de comunicaciones estratégicas de cualquier transición de la MONUSCO se priorice e incorpore en todas las líneas programáticas de transición de modo que se informe a las audiencias clave —locales (incluidas audiencias internas e internas), regionales e internacionales— de manera tal que se disipen las ideas equivocadas, se contrarreste la información errónea y se minimice el riesgo para la reputación en una coyuntura política tan crítica. (NATO N19, 2019)

La revisión también pidió a la misión que ajustara su estrategia de comunicaciones cambiando de resaltar sus propias historias de éxito a difundir narrativas sobre logros nacionales y locales para señalar su nueva mentalidad orientada a la transición.

Como puede verse, toda Comunicación Estratégica requiere de una Narrativa Estratégica.

2.4. **La Estrategia de Comunicación y la Narrativa Estratégica**

Una narrativa[103] estratégica, es una historia, oral o escrita, de eventos e información, organizada en una secuencia lógica y diseñada para explicar la justificación para llevar a cabo una actividad y el resultado buscado. Si la estrategia es el plan para llegar a un estado final deseado (empleando modos y medios para lograr los fines), la narrativa proporciona el ¿por qué?

Para James P. Farwell, "forjar y ejecutar una estrategia efectiva requiere evitar la trampa de permitir que las definiciones académicas obstruyan los requisitos operacionales. Se trata de trabajar con la tecnología de la información y la comunicación para obtener una ventaja competitiva. Abarca más que el lenguaje. Implica el uso del lenguaje, la acción, los símbolos y las imágenes para dar forma a las percepciones e influir en las actitudes y opiniones para cambiar el comportamiento en aras de lograr un estado o efecto final deseado" (Farwell, 2020).

Hoy, las historias, no la acción cinética, pueden decidir quién gana los conflictos. El conflicto de Ucrania, en curso en el momento de esta investigación, ilustra ese punto. Moscú ha impulsado la narrativa de que las revoluciones a favor de la democracia conducen al caos y la guerra civil; Kiev argumenta que el separatismo conduce a la miseria.

Empero, uno de los desafíos más difíciles es construir una narrativa, una que la organización quiera promover. Como explica el ex Jefe de Comunicación Estratégica de la OTAN, Mark Laity, esta es una debilidad común en las campañas de comunicación (GALVIN, 2019):

> En este momento dedicamos demasiado tiempo a la coordinación y el proceso. Ahora hemos creado organizaciones cuya suma es menor que las partes... El enemigo es rápido, flexible y más en sintonía con las culturas donde opera. Habla-

103 Una de las partes en que suele considerarse dividido el discurso, en la que se refieren los hechos que constituyen la base de la argumentación. RAE.

> mos de Narrativa, pero Narrativa es donde nos ganan. Hacemos mensajes y temas, y nuestros oponentes hacen narrativa y aprovechan las culturas y la religión.

En 2018, la publicación *Joint Concept for Operating in the Information Environment* (JCOIE) que describe cómo la Fuerza Conjunta incorporará la información en el arte operacional para diseñar operaciones que aprovechen deliberadamente la información y los aspectos informativos de las actividades militares para lograr resultados estratégicos duraderos. Define narrativa como (United States Joint Chiefs of Staff, JCOIE, 2018):

> Una base para la comunicación unificada y la comprensión que crea significado a través de un sistema de formatos de historia, que se basa en la historia, la cultura y la religión locales para enmarcar y afectar las percepciones de acciones específicas. Las narrativas muestran la cosmovisión de un individuo o grupo, los objetivos del liderazgo grupal, el sentido de poder u opresión, las afirmaciones de legitimidad, la descripción de los enemigos y otras caracterizaciones útiles para comprender a los actores relevantes y sus acciones. El uso efectivo de narrativas puede dar forma a los comportamientos e incluso transformar la cultura.

Se expresa como un argumento (un tema común comunicado a través de historias, imágenes o acciones individuales) que busca explicar cómo se ha llegado a la situación actual, define esa situación y expresa un estado final deseado aceptable en el contexto de las narrativas individuales de las partes clave interesadas. Al aplicar las estructuras clásicas de la narración humana, el atractivo emocional es más fácil de mantener (Gill, Heap, & Hansen, 2021).

Es importante entender, cuando se utilizan plataformas, que cada una tiene una audiencia diferente y, por lo tanto, la narrativa debe ser diferente. En la mayor parte de los casos, la fórmula óptima será el resultado de la coordinación de varias estrategias en diferentes plataformas y medios (Peirano, 2020).

Farwell argumenta que el plan de comunicación debe implementarse en el nivel estratégico mucho antes de que comiencen las operaciones cinéticas. Una nación necesita un plan de comunicación estratégica deliberado para controlar el ambiente de la información antes y durante las campañas militares".

Los factores clave que según Farwell enmarcan el pensamiento estratégico para la guerra de la información son:

1. Una idea poderosa o motivo que impulsa la estrategia. 2. Una visión clara de lo que constituye ganar o tener éxito (es decir, estados finales y resultados). 3. Definiciones claras de los obstáculos para el éxito. 4. Una estrategia viable que emplee operaciones y tácticas diseñadas para lograr el éxito. 5. Planes bien construidos y realizables. 6. Operaciones y tácticas para ejecutar la estrategia. 7. Formas de medir la efectividad de la estrategia (Farwell, 2020).

Ello hace que las operaciones militares cinéticas actuales ya no determinen la victoria en la guerra tradicional. El *Homo digitalis* compite antes, durante y después del conflicto militar. La victoria decisiva en la batalla física es ahora insuficiente si se pierde la narrativa (Patrikarakos, 2017).

Sería en base a este concepto que pueden entenderse los siguientes titulares:

ILUSTRACIÓN 37 . **La Guerra de la Información**

FUENTE: VARIAS FUENTES

En esencia, las narrativas presentadas en el conflicto entre Rusia y Ucrania son diametralmente opuestas. Rusia enmarca la guerra en Ucrania, que Putin insiste en que es una «operación militar especial», como una medida defensiva necesaria en respuesta a la expansión de la OTAN en Europa del Este. Putin también encuadra la campaña militar como necesaria para «desnazificar» Ucrania y poner fin a un supuesto genocidio que se está llevando a cabo por el gobierno ucraniano contra los rusos parlantes. En contraste, la narrativa de Ucrania insiste en que la guerra es de agresión, enfatiza su historia como una nación soberana distinta de Rusia y retrata a sus ciudadanos y fuerzas armadas como héroes que se defienden de una invasión injustificada. Ucrania y Rusia no son los únicos actores estatales interesados y comprometidos en retratar la guerra en sus propios términos (Perez, Christian, 2022):

> Países como China y Bielorrusia han participado en esfuerzos para plasmar el conflicto en sus propios términos, y han lanzado campañas coordinadas de desinformación en las plataformas de redes sociales. Estas campañas han minimizado ampliamente la responsabilidad de Rusia en la guerra y han promovido la lucha contra Estados Unidos y la OTAN.

> La mezcla de narrativas, originadas por diferentes actores estatales, así como por millones de usuarios individuales en las redes sociales, ha ampliado los roles de las plataformas tecnológicas en la configuración de la dinámica de la guerra y podría influir en sus resultados.

Un ejemplo de la narrativa ucraniana lo da Muyiwa Babarinde resaltando los siguientes aspectos (Babarinde, 2022):

- Desde el principio Ucrania rápidamente enmarcó la guerra como una situación de David vs Goliat lo que ayudó a legitimar su pedido de ayuda;
- El gobierno y el ejército ucranianos publicaron imágenes para reunir los espíritus nacionalistas de los ucranianos y ganar simpatía en todo el mundo;
- También comenzaron a publicar información sobre las victorias que estaban obteniendo en el campo de batalla. Estas tuvieron un efecto triple
  - > Mejoró la moral de los combatientes ucranianos, muchos de los cuales son civiles, que luchan para salvar sus hogares;
  - > Condujo a la duda en el lado ruso, especialmente con los soldados que no sabían por qué estaban invadiendo Ucrania;
  - > Le dio a Ucrania más tiempo para obtener apoyo de Occidente.
- La presidencia y su equipo de comunicaciones sembraron su foto familiar junto con esta cita icónica de su toma de posesión 2 años atrás. «No quiero mi foto en sus oficinas; el Presidente no es un ícono, un ídolo o un retrato. Cuelgue las fotos de su hijo en su lugar y mírelas cada vez que tome una decisión»;
- Ucrania también lanzó un sitio web para que las familias rusas conozcan el estado de sus hijos soldados en caso de que hubiesen sido muertos o tomados prisioneros; Esto es para avivar los sentimientos públicos en Rusia y provocar protestas de las familias que quieren que la guerra se detenga. También es un acto de empatía y misericordia hacer saber a las personas si han perdido a alguien y comenzar a sanar: la comunicación estratégica en su máxima expresión.

En síntesis, Zelensky pareciera haber puesto su campaña informativa al tope de su lista de prioridades mostrando su determinación y pidiendo ayuda, sabiendo que el mundo lo está escuchando, asegurándose de que Putin sea visto como un criminal de guerra y un agresor y que Rusia sea percibida como una amenaza al tratar de reconstruir un imperio entre antiguos estados socialistas. La guerra parece nueva para el mundo, a pesar de que los rusos han estado en Ucrania desde hace un tiempo. Los pedidos ucranianos apuntan a soluciones que el mundo está dispuesto a apoyar (envío de armas, sanciones a los oligarcas rusos, restringir el espacio aéreo, reducir el comercio, etc.)

La publicación MCDP 8 del US Marine Corps da un ejemplo de cómo adelantarse a la narrativa de Rusia en Ucrania (United States Marine Corps, MCDP8, 2022):

> El 24 de febrero de 2022, Rusia invadió Ucrania. Esto marcó una escalada significativa en el conflicto armado entre Rusia y Ucrania que comenzó con la anexión de Crimea por parte de Rusia en 2014.
>
> En las semanas y meses previos a la invasión, Estados Unidos y nuestros aliados participaron en una campaña de información deliberada para infor-

mar a las audiencias nacionales e internacionales sobre la acumulación militar de Rusia y la intención de invadir. La campaña de información se adelantó a la narrativa de Rusia al negarles el falso pretexto necesario para justificar la acción militar en Ucrania. La campaña de información involucró un flujo constante de revelaciones selectivas de inteligencia combinadas con información de fuente abierta ampliamente disponible para exponer la capacidad, disposición, propaganda e intención de Rusia.

La campaña de información incluyó a altos funcionarios estadounidenses que revelaron el inventario de guerra irregular de Rusia y las acciones específicas que emprendería a partir de dicha lista. Por ejemplo, funcionarios estadounidenses revelaron información de inteligencia sobre una esperada operación de falsa bandera y una película que Rusia usaría para fabricar una justificación para la invasión.

Una lucha o choque entre narrativas en competencia a menudo se conoce como una «batalla de la narrativa». Para ganar esa batalla, las Fuerzas Armadas de España, "en estrecha coordinación con otros poderes del Estado deberán ser capaces de desarrollar operaciones de información, a través de múltiples medios, actuando tanto autónomamente como integradas en fuerzas multinacionales, para refutar las narrativas del adversario con las propias" (España Ministerio de Defensa, 2019).

Desarrollar una estrategia de comunicación que incluya una narrativa no es una tarea fácil; requiere tiempo y recursos y, generalmente suele comenzar a elaborarse demasiado tarde, cuando se está inmerso en una crisis. Redactar una historia requiere una comprensión de la audiencia y el ambiente de la información (Mark Laity, 2018).

También será necesario armonizar la comunicación estratégica nacional con los niveles operacional y táctico. Comprender cómo usar la comunicación estratégica como un elemento del poder nacional ayudará a la sincronización de los niveles estratégico, operacional y táctico. Será la narrativa estratégica militar la que explicará el empleo de los militares y pondrá las operaciones en contexto. En el nivel operacional las narrativas se centran en el teatro y buscan avanzar en la legitimidad de la misión mientras contrarrestan las narrativas adversarias.

2.5. **Las Operaciones en el Ambiente de la Información**

En esta sección, se analizarán en primer lugar las operaciones en el ambiente de información según la doctrina estadounidense recientemente actualizada, para luego indagar en las de aquellos países que aún mantienen el concepto de "Operaciones de Información"

En los Estados Unidos, conceptualmente, el Departamento de Defensa (DOD), en coordinación con los otros departamentos y agencias del gobierno apoya al instrumento informativo del poder nacional mediante el uso de la información para impactar la forma en que los humanos y los sistemas se comportan o funcionan. La fuerza conjunta aprovecha la información para asegurar, disuadir, obligar y forzar comporta-

mientos de actores relevantes que apoyan los intereses de los Estados Unidos (United States Joint Chiefs of Staff, JP 3-04, 2022).

A esta conclusión el Estado Mayor Conjunto estadounidense llegó luego de una serie de cambios en la doctrina conjunta desde que el concepto de operaciones de información fuera introducido en 1998.

La publicación JP 3-13 *Information Operations* desde su primera edición en 1998 fue modificada en tres oportunidades y a partir de 2016 se iniciaron una serie de cambios, cuyos aspectos más destacados fueron:

a. En junio de ese año el Departamento de Defensa promulgó la publicación *"Strategy for Operations in the Information Environment"* (United States DoD, 2016)

b. En 2017 una resolución del Presidente de la Junta de Jefes de Estado Mayor modificó la Publicación JP 1 "*Doctrine for the Armed Forces of the United States",* aclarando el papel del Departamento de Defensa en relación con las operaciones de información para mejorar la eficiencia en la planificación y ejecución de las operaciones militares e incorporando a la "Información" como una nueva y séptima función conjunta (United States DoD, 2017).

c. En julio de 2018 el Estado Mayor Conjunto promulgó la publicación *"Joint Concept for Operating in the Information Environment"* (JCOIE) que aborda el rol de la información y se centra en cómo la información puede cambiar o mantener los impulsores del comportamiento (United States Joint Chiefs of Staff, JCOIE, 2018).

Finalmente, en septiembre de 2022 la publicación JP 3-04 derogó la JP 3-13 aduciendo que las Operaciones de información tal como se definían y practicaban, tenían deficiencias que les impedían contribuir a la aplicación del poder de información del comandante. Como se definió, las IO se centraban en la integración de capacidades relacionadas con la información (IRC) para afectar la toma de decisiones de adversarios y adversarios potenciales, e ignoraban efectivamente a otros actores relevantes que dan forma a los ambientes estratégicos y operacionales. La planificación de las IO se concentró en el empleo de esos IRC en apoyo de operaciones más amplias de la fuerza conjunta, ignorando la planificación de los aspectos informativos inherentes de todas las actividades (United States Joint Chiefs of Staff, JP 3-04, 2022).

Por tal razón en la actualidad, en los Estados Unidos se desarrollan las Operaciones en el Ambiente de la Información las cuales son distintas, pero complementarias, del aprovechamiento deliberado por parte de las fuerzas conjuntas de los aspectos informativos inherentes a las actividades militares durante todas las operaciones.

La Publicación eliminó términos como operaciones de información y capacidad relacionada con la información (CRI) destacándose en la nueva definición el concepto:

Informar a las audiencias. El término CRI ha sido reemplazado por capacidades especializadas (United States Joint Chiefs of Staff, JP 3-04, 2022, pág. XI).

ILUSTRACIÓN 38 . **Cuadro comparativo de definiciones anterior y actual**

JP 3-13 - Operaciones de Información	JP 3-04 - Operaciones en el Ambiente de la Información
Las Operaciones de Información se definen como el empleo integrado, durante las operaciones militares, de capacidades relacionadas con la información en concierto con otras líneas de operación para *influir, interrumpir, corromper* o *usurpar* la toma de decisiones de adversarios y adversarios potenciales, al tiempo que se protegen las propias.	Son acciones militares que implican el empleo integrado de múltiples fuerzas de información para afectar a los impulsores del comportamiento al: *informar* a las audiencias; *influir* en los actores extranjeros pertinentes; *atacar* y *explotar* la información de actores relevantes, las redes de información y los sistemas de información.9. Desinformación e incertidumbres

FUENTE: ELABORACIÓN PROPIA.

También eliminó el concepto de superioridad de la información y lo reemplazó con nuevas definiciones de ventaja de información y poder de información.

La ventaja de la información es la ventaja operacional obtenida a través del uso de la información por parte de la fuerza conjunta para la toma de decisiones y su capacidad de aprovechar la información para crear efectos en el ambiente de la información.

En cuanto al poder de la información lo define como la capacidad de utilizar la información para apoyar el logro de los objetivos y obtener una ventaja informativa. La esencia del poder de la información es la capacidad de ejercer la propia voluntad a través de la proyección, explotación, negación y preservación de la información en la búsqueda de objetivos. La fuerza conjunta no puede lograr todos sus objetivos estratégicos confiando únicamente en el desgaste para forzar el cambio en el comportamiento de un enemigo o adversario. La fuerza conjunta aprovecha el poder de la información como un medio para apoyar el logro de sus objetivos. La fuerza conjunta aplica el poder de la información para (United States Joint Chiefs of Staff, JP 3-04, 2022):

1. Operar en situaciones en las que el uso de fuerza física destructiva o disruptiva no está autorizado o no es un curso de acción apropiado (COA);
2. Degradar, interrumpir y destruir la habilidad C2 de un adversario o enemigo;
3. Prevenir, contrarrestar y mitigar los efectos de las acciones de actores externos sobre las capacidades y actividades propias;
4. Crear y mejorar los efectos psicológicos de la fuerza física destructiva o disruptiva;
5. Crear efectos psicológicos sin fuerza destructiva o disruptiva;

6. Confundir, manipular o engañar a un adversario o enemigo para crear una ventaja o degradar la ventaja existente del adversario o enemigo;
7. Para prevenir, evitar o mitigar cualquier efecto psicológico no deseado de las operaciones;
8. Comunicar y reforzar la intención de las operaciones conjuntas de la fuerza, independientemente de si esas actividades son constructivas o destructivas.;
9. Preparar y apoyar la resiliencia en las poblaciones de las naciones amigas.

Las unidades que operan en el ambiente de la información (OIE), ahora llamadas *capacidades especializadas,* constituyen una organización con mando y control de las fuerzas de información asignadas y agregadas que están específicamente organizadas, entrenadas y equipadas para crear y/o apoyar la creación de efectos en el ambiente de la información. Poseen personal militar, sistemas de armas, equipos y el apoyo necesario que proporcionan experiencia y capacidades especializadas que aprovechan la información. Los Comandantes Conjuntos pueden optar por crear un grupo de trabajo para el empleo integrado de las capacidades especializadas necesarias para llevar a cabo estas operaciones (United States Joint Chiefs of Staff, JP 3-04, 2022).

Las unidades de la OIE suelen estar compuestas por los siguientes tipos de fuerzas de información (United States Joint Chiefs of Staff, JP 3-04, 2022):

- Fuerzas de Operaciones Psicológicas que ejecutan las Operaciones de Apoyo a la Información Militar (MISO);
- Asuntos civiles:
- Organizaciones de Asuntos Públicos;
- Elementos de Operaciones en el Espectro Electromagnético;
- Fuerzas de misión cibernéticas;
- Elementos de operaciones espaciales.

Estas unidades de capacidades especializadas dependen orgánicamente del Comando de Operaciones Especiales (SOCOM), del Comando Cibernético (CYBERCOM) y de los Comandos de Combate Regionales (Comando Europeo, Comando Central, Comando Sur, etc.). Son estos últimos los que generalmente tienen el control operacional sobre las fatunidades, incluso en el ciberespacio.

> SOCOM conserva la prerrogativa orgánica sobre las Operaciones de Apoyo a la Información Militar (MISO) y apoya a los comandos regionales. Para ello, dispone de un centro de operaciones web (*Joint MISO Web Ops Center* - JMWC) que publica contenidos y monitorea las actividades de los adversarios en las redes sociales (Clarke R. D., 2019). SOCOM actúa en estrecha coordinación con el Centro de Participación Global del Departamento de Estado y otras agencias para entregar mensajes de los Comandantes Regionales bajo sus autoridades a una parte más amplia de la Fuerza Conjunta. El JMWC apoya a los comandos combatientes con capaci-

> dades de mensajería y evaluación, conciencia situacional compartida de las actividades de influencia del adversario y coordina las operaciones MISO basadas en Internet en el nivel mundial.
>
> CYBERCOM ha establecido la Fuerza de Misión Cibernética que, mientras ejecuta las operaciones de guerra cibernética en el nivel nacional, opera principalmente en apoyo de los comandos regionales. Cuando la operación prevista implica el empleo de capacidades ofensivas de guerra informática, CYBERCOM recupera el control operacional de sus Equipos de Misión de Combate Cibernético, cuya acción debe permanecer «alineada» con los objetivos del comando involucrado. (Tenenbaum, 2021)

En cuanto al planeamiento, la publicación JP 3-04 (2022) indica:

> Los planificadores integran las actividades de influencia en el proceso de "targeting" existente. Las actividades diseñadas para contribuir a la tarea de influencia incluyen operaciones MISO (Operaciones de Información de Apoyo (ex Operaciones psicológicas)), CMO (operaciones cívico militares), CO (operaciones cibernéticas), OPSEC (operaciones de seguridad) y MILDEC (engaño militar). La influencia también puede implicar el uso de STO (operaciones técnicas especiales). Los comandantes consideran el potencial de influencia de todas las capacidades disponibles en el diseño, la planificación y la orientación. Las unidades de la OIE llevan a cabo todas las tareas de influencia de acuerdo con las autoridades autorizadas.

Herbert Lin al preguntarse ¿Cómo las operaciones cibernéticas, que son actividades operacionales del Comando Cibernético (USCYBERCOM), podrían considerarse operaciones psicológicas que son actividades operacionales del Comando de Operaciones Especiales (USSOCOM)? responde (Lin, 2020):

- En la medida en que estas operaciones buscan influir en el comportamiento de los altos dirigentes rusos o del ISIS, son claramente operaciones de influencia;
- Tal vez el hecho de que utilicen la información para hacerlo los convierte en operaciones de información;
- La influencia está facilitada psicológicamente; por lo tanto, podrían ser operaciones psicológicas;
- Están habilitados por operaciones cibernéticas que utilizan técnicas de piratería informática para localizar, identificar y posiblemente manipular los datos personales confidenciales de las personas objetivo;
- Tal vez sean actividades de guerra de información, ya que buscan responder a una campaña de guerra de información que Rusia ha librado contra los Estados Unidos y sus instituciones democráticas durante mucho tiempo.

Lo cual demuestra que la categorización de las operaciones en el ambiente de la información continuará siendo un problema difícil de resolver.

Sin embargo, el concepto de Operaciones de Información (OI) a la fecha se mantiene vigente en otros países y si bien no existe una definición unánime, se conservan algunas características acordadas casi universalmente que forman parte de nuestro léxico cotidiano.

Para la República Argentina, aunque no desarrolla una doctrina específica, son acciones que implican el uso y manejo de la tecnología de la información y las comunicaciones, dentro de las dimensiones físicas, de información y cognitivas del ambiente de la información, en concierto con otras líneas de operaciones, para acceder, modificar, interrumpir, alterar o destruir la toma de decisiones del adversario, protegiendo, al mismo tiempo, las propias (República Argentina EMCO, PC 00-02, 2019).

Para Brasil, las Operaciones de Información (Op Info) son un esfuerzo esencialmente militar y consisten en coordinar el uso integrado de Capacidades Relacionadas con la Información (CRI), en contribución a otras operaciones o incluso como parte del esfuerzo principal, para informar e influir en personas o grupos hostiles, neutrales o favorables, capaces de impactar positiva o negativamente el logro de los objetivos políticos y militares, así como comprometer el proceso de toma de decisiones de los opositores o posibles opositores, mientras se asegura la integridad de nuestro proceso. Entre los CRI, los principales son: Operaciones Psicológicas, Acciones de Guerra Electrónica, Ciberdefensa, Comunicación Social y Asuntos Civiles (Brasil Ministério da Defesa, MD 30-M-01, 2020)

Las Operaciones de Información reúnen CRI y otros recursos de forma permanente y consistente para crear efectos en la dimensión informativa y, a través de ellos, aumentar la capacidad de ofrecer ventajas operacionals al comandante. Mientras que una CRI aislada crea efectos individuales, las operaciones de información enfatizan los efectos integrados y sincronizados como esenciales para lograr objetivos en la dimensión informativa.

La República de Chile define las Operaciones de Información y las Actividades de Información[104] como (Chile Ministerio de Defensa Nacional, DNC 3-7, 2014)

1. Operaciones de Información (Info Ops): Es una función del estado mayor conjunto para analizar, planificar, evaluar e integrar actividades de información para crear los efectos deseados en la voluntad, comprensión y capacidades del adversario y/o potenciales adversarios y audiencias aprobadas en apoyo del cumplimiento de la misión.

2. Actividades de Información: son las acciones encaminadas a afectar la información y/o los Sistemas de Información del adversario. Ellas pueden ser realizadas por cualquier actor e incluyen medidas de protección.

104 De acuerdo a MC422/4 OTAN: Política Militar de las Operaciones de Información (Info ops)

Mas allá de las diferencias sutiles en las definiciones, pude decirse que las Operaciones de Información integran capacidades y actividades relacionadas con la información (IRC por sus siglas en inglés), que tradicionalmente se ejecutaban de manera autónoma, se conducen en el ambiente de la información, que engloba el ciberespacio y cuyos efectos se pueden observar en la dimensión lógica, física y cognitiva a fin de afectar la toma de decisiones enemigas y adversarias al mismo tiempo que se protegen las propias. Dichas operaciones buscan lograr efectos en:

- La dimensión física: destruyendo o degradando los sistemas de Comando y Control (C^2), la capacidad de liderazgo, las redes y los nodos críticos (humanos o de infraestructura); ejecutando engaños, artimañas, demostraciones y exhibiciones, etc.

- La dimensión informativa: interfiriendo comunicaciones y señales; corrompiendo datos e información; empleando ataques de denegación de servicio; interceptando o desviando datos o contenidos; manipulando la información proporcionada a los líderes adversarios; atacando la(s) narrativa(s) del enemigo o adversario; usando ingeniería social o *spoofing*.

- La dimensión cognitiva: creando ambigüedad o confusión; causando una comprensión incorrecta de una intención propia; creando vacilación o demoras; permitiendo el exceso de confianza en señales y signos falsos y baja o incertidumbre en los verdaderos; degradando el apoyo al oponente y la legitimidad de sus narrativas.

Para citar un ejemplo, una de las secciones del Área de Operaciones (AOPE) del Estado Mayor del Mando de Operaciones de las Fuerzas Armadas de España es la denominada J9 – Influencia (España Mando de Operaciones, 2022). Esta sección se encarga de actividades tales como Operaciones de Información (incluida Operaciones Psicológicas), Interacción Cívico-Militar y Asuntos Públicos Militares, mientras que la OTAN *Information Operations* es el nombre dado precisamente a la propia área funcional que, a su vez, puede quedar incluida en otras áreas como J5 o J3 durante el planeamiento o ejecución, respectivamente, de una operación (Yeste, 2020).

Por último, están quienes identifican las operaciones de información en términos de influencia.

Para la República de Francia, las operaciones militares realizadas en la capa informativa del ciberespacio se denominan Lucha Informativa de Influencia (L2I) y tienen como objetivo detectar, caracterizar y contrarrestar ataques, apoyar la StratCom, informar o engañar, de forma autónoma o en combinación con otras operaciones (France Ministère des Armées, L 21, 2021):

Las operaciones de L2I contribuyen a la Comunicación Estratégica (StratCom) ministerial. Se trata de operaciones militares comandadas por el Jefe de Estado Mayor de las Fuerzas Armadas quien, en cuanto a las operaciones LID y LIO[105], delega el control en el Oficial General al Mando de la Ciberdefensa (COMCYBER). La lucha informática de influencia, se refiere a todas las operaciones militares realizadas en apoyo a nuestras fuerzas en el campo de la información, para detectar, caracterizar, contraataques para apoyar la comunicación estratégica asociada a una operación.

Las operaciones de información y la estrategia militar de influencia (SMI), que están más integradas en la maniobra y que tienen como objetivo afectar las percepciones, la comprensión y la voluntad y, por lo tanto, en última instancia, el comportamiento de los actores (adversarios, aliados o neutrales) de un conflicto en la dirección del estado final deseado. Concretamente, estas operaciones de información consisten en sincronizar acciones informativas resultantes de un doble propósito, por un lado, la guerra de comando y control, por otro la influencia sobre los «públicos objetivo» del teatro, por medios no letales. En este sentido, los métodos de engaño pueden insertarse en el SMI, incluso si puede apuntar a otros objetivos que no sean engañar o intoxicar al enemigo: desacreditarlo con sus partidarios, ganar el apoyo y la confianza de la población o incluso de ciertas fuerzas de oposición promoviendo mítines, fortalecer la moral y la cohesión de las fuerzas amigas son todos los objetivos posibles del SMI.

Tenenbaum y De Rochegonde, señalan que la doctrina de la OTAN hasta la fecha reconoce tres tipos principales de operaciones de información en términos de influencia (Tenenbaum, 2021):

La primera es la cooperación cívico-militar (CIMIC): descendiente lejano de los «asuntos civiles» o unidades de pacificación para administrar los territorios recientemente conquistados, estas misiones trabajan en principio para mejorar ciertas condiciones sociales o económicas en el área de operación y, al hacerlo, contribuyen a la aceptación de la fuerza, a una percepción positiva de su acción y a la cooperación de la población, incluso en términos de inteligencia.

El segundo tipo de operación se conoce con la expresión inglesa *«key leader engagement»* (KLE) que se refiere al trabajo de influencia, directa o indirecta, con líderes civiles o militares en un teatro determinado. También fuertemente influenciado por las experiencias de contrainsurgencia de Afganistán e Irak, el KLE es una versión específica y personalizada de CIMIC destinada a aumentar la confianza y la calidad de la cooperación con los actores locales, valorando así los organis-

105 LID : Lutte informatique défensive; LIO: Lutte informatique offensive.

mos intermedios (líderes tradicionales, autoridades religiosas, actores económicos, etc.) directamente en contacto con la población.

Finalmente, las operaciones psicológicas (PSYOPS) constituyen estrictamente el tercer eje. De carácter más específicamente informativo, se definen por la formulación y difusión de mensajes destinados a cambiar, mantener o fortalecer las percepciones de los individuos u organizaciones colectivas.

ILUSTRACIÓN 39 . **La Influencia en la Doctrina de la OTAN**

FUENTE: *(TENENBAUM, 2021)*

El corpus doctrinario de influencia militar ha sido recientemente reformulado, formalizado en el nivel estratégico por una Estrategia Militar de Influencia (SMI) y una Directiva de Comunicación Estratégica (STRATCOM). La influencia militar es una función que planifica y lleva a cabo acciones especiales sobre el ambiente de la información (ASEI), las acciones cívico-militares (CIMIC), el compromiso del líder clave (KLE) y las operaciones psicológicas (PSYOPS) (Mariel, 2019).

2.6. **La función conjunta Información**

La historia de las funciones conjuntas es una historia de superar la resistencia en el pensamiento militar estadounidense a colocar elementos del "poder blando" y del "poder duro" del campo de batalla contemporáneo en un pie de igualdad. Expresan el conocimiento colectivo de los militares sobre cómo combinar mejor las armas y los dominios cruzados (Crosbie, 2019):

El término funciones conjuntas ha surgido en la doctrina como una forma abreviada de expresar aquellas dimensiones del conflicto donde la combinación de instrumentos de poder es particularmente útil. En este sentido, son una especie de lista de verificación para garantizar que el potencial latente de

> la articulación se esté realizando. En la doctrina estadounidense hay hoy siete funciones conjuntas: inteligencia, maniobra, fuegos, información, protección, sostenimiento y C2. Para el resto de la comunidad de la OTAN, hay ocho, ya que la doctrina de la OTAN también incluye la cooperación civil-militar (CIMIC).

Las funciones conjuntas, a veces denominadas funciones de combate o capacidades conjuntas, no deben confundirse con las jefaturas de un Estado Mayor a las que se parecen someramente. El propósito de las jefaturas de un Estado Mayor es garantizar que un Estado Mayor Conjunto tenga la combinación adecuada de conocimientos especializados en áreas clave. La experiencia ha dejado claro que un Estado Mayor necesita romper los compartimientos estancos que pueden ser creados por las jefaturas, y en su lugar sus integrantes deben mezclarse en una serie de subgrupos (enumerados en la doctrina estadounidense como «centros, grupos, oficinas, células, juntas, elementos, grupos de trabajo y equipos de planificación» B2C2WGs por sus siglas en inglés).

Resulta obvio que el número de B2C2WG debe mantenerse en un nivel manejable para evitar que el personal se vea abrumado por una agenda completa de reuniones que realmente pueden obstaculizar los esfuerzos de planificación. Los grupos de trabajo se centran en un área funcional particular para proporcionar apreciaciones adicionales sobre los problemas. Una vez asignados a su subgrupo, los miembros del Estado Mayor necesitan lograr ciertos tipos de efectos. Los efectos más importantes se clasifican en siete categorías y son las funciones conjuntas: C2, inteligencia, fuegos, movimiento y maniobra, protección, sostenimiento e información.

> La función conjunta de información abarca la gestión y aplicación de la información para cambiar o mantener percepciones, actitudes y otros conductores del comportamiento y para apoyar la toma de decisiones humana y automatizada. La función conjunta de información es la organización intelectual de las tareas necesarias para utilizar la información durante todas las operaciones: comprender cómo la información afecta el ambiente operacional, apoyar la toma de decisiones humana y automatizada y aprovechar la información.

> Esta tarea ayuda a la fuerza conjunta a identificar amenazas, vulnerabilidades y oportunidades en el ambiente de la información. Proporciona una base y apoya el perfeccionamiento continuo de los productos de preparación conjunta de inteligencia del ambiente operacional (JIPOE) para mejorar la toma de decisiones del comandante durante la planificación, ejecución y evaluación de las operaciones. Hay tres pasos para comprender cómo la información afecta al ambiente operacional: análisis de los aspectos informativos, físicos y humanos del ambiente; identificar y describir a los actores pertinentes; y determinar los comportamientos más probables de los actores relevantes.

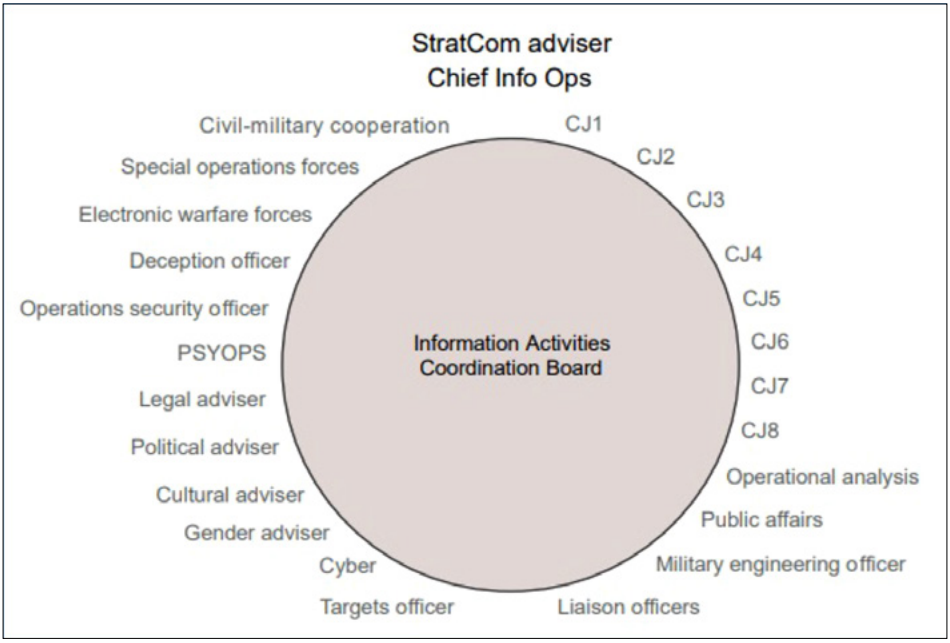
Un aspecto sobre el cual se discutió fue sobre la forma en que debía definirse la relación entre la información y las operaciones, lo que, a su vez, afectaba a cómo debía tratarse la información y a qué área del Estado Mayor pertenecía. Las diferencias de opiniones que se muestran en la siguiente ilustración y que datan de 2009, aún persisten en varias fuerzas armadas de distintos países.

Centro de Armas Combinado	Comunidad de Targeting	Comunidad FA30[106]
Argumentó que la «información» era inherente a todas las operaciones. La «influencia» sobre la toma de decisiones del enemigo era el resultado acumulativo de todas las interacciones de una unidad con el ambiente operacional, de modo que las acciones físicas de una unidad creaban mensajes más firmes que las palabras o las imágenes. La planificación de este tipo de influencia era un aspecto fundamental del diseño de la campaña que no podía delegarse en un integrador de personal secundario. En cambio, las decisiones sobre a quién influir, por qué y cómo eran responsabilidad del comandante y el G3, mientras que la evaluación del éxito de la influencia era responsabilidad del G2.	La información era una munición cuantificable y no letal que los comandantes podían disparar a objetivos para lograr efectos específicos y predecibles. La información, así concebida, era fundamentalmente una parte del proceso de "targeting", lo que significaba que las decisiones sobre a quién influir y cómo eran responsabilidad del coordinador de apoyo de fuegos trabajando en conjunto con el comandante. La información y sus diversas subtareas caían lógicamente bajo la función conjunta de fuegos.	La «información» comprendía una categoría especial de operaciones utilizadas por el comandante para afectar la toma de decisiones del adversario mientras protegía la propia. Las decisiones sobre cómo utilizar esta categoría de operaciones pertenecían al ámbito de un oficial de operaciones de información G3 dedicado, cuyo enfoque principal era el proceso de integración de diferentes capacidades de información para lograr un efecto específico en una población objetivo.

Durante la planificación y la realización de operaciones el Comandante de Teatro pueden conformar una célula o junta de planificación de la información para supervisar y colaborar con todas las Jefaturas de su Estado Mayor y organizaciones de apoyo en temas relacionados con información. La célula o junta debería estar compuesta por profesionales de la información del Estado Mayor y sirve como punto focal para planificar cómo la fuerza conjunta aprovechará los aspectos informativos inherentes de sus actividades y para planificar las Operaciones en el Ambiente de la Información.

106 Los oficiales de la comunidad de operaciones de información (IO) del Ejército de los Estados Unidos, conocidos por su designación de campo de carrera del Área Funcional 30 (FA30), son el "punto focal del personal para IO" y desempeñan la función de sincronizar, coordinar e integrar los efectos de la información en las operaciones de la unidad.

ILUSTRACIÓN 40 . **Ejemplo de integración de una Junta de Operaciones de Información**



FUENTE: (NATO, JP 3-10, 2015)

Las funciones de algunos de los integrantes de dicha Junta son (NATO, JP 3-10, 2015):

ILUSTRACIÓN 41 . **Funciones**

Asesor de Comunicación Estratégica.	Con el apoyo de un pequeño grupo de personal, garantiza que operaciones de información, asuntos públicos militares (AP) y diplomacia pública (a través del asesor político) se coordinen de acuerdo con la narrativa de la misión y dentro del marco de la Comunicación Estratégica.
Jefe de Operaciones de Información	Es el experto en Operaciones de Información y asesora al comandante sobre cuestiones relacionadas con el ambiente de la información. Ante la ausencia del Jefe de Estado Mayor, es responsable de la dirección general de Info Ops a través del proceso de coordinación y sincronización y preside la Junta de Operaciones de Información (IACB) en nombre del Jefe del Estado Mayor. Lidera el proceso de integración, asegurando la priorización, la eliminación de conflictos y la unidad de propósito para todas las actividades de información emprendidas dentro del comando.

Asesor Jurídico	Asesora sobre las consecuencias jurídicas, incluidas las Reglas de Empeñamiento de las actividades de información propuestas, y proporciona una evaluación jurídica de las actividades de información propuestas por el IACB.
Asesor Cultural	Asesora sobre las consecuencias culturales de las actividades de información propuestas, incluidos los aspectos etnológicos, religiosos, de género y sociales. Junto con J9 y la sección de desarrollo del conocimiento en J2, también contribuye a la evaluación de las actividades de información desde la perspectiva cultural.
Asesora en Cuestiones de Género	Velará que las perspectivas de género, en particular el papel de la mujer en las sociedades locales y los efectos que el conflicto tiene en ellas, se tengan en cuenta tanto en la fase de planificación como en la de ejecución de las operaciones.
Asesor de Coordinación de Blancos	Cuando el IACB no se fusiona con la Junta Conjunta de Coordinación de Blancos (JTCB), el representante de JTCB se asegura de que las actividades de planificación de IACB se sincronicen dentro del proceso de selección de blancos conjunto.

FUENTE: *(NATO, JP 3-10, 2015).*

La función conjunta de información organiza las tareas necesarias para la gestión y aplicación de la información durante todas las actividades y operaciones. Las tres tareas de la función conjunta de información hacen hincapié en la necesidad de incorporar la información como elemento fundamental durante la planificación y realización de todas las operaciones. Esas tareas son:

- Comprender cómo la información afecta el ambiente operacional (OE);
- Apoyar la toma de decisiones humanas y automatizadas; y
- Aprovechar la información.

Para comprender cómo la información afecta el ambiente operacional, es necesario analizar aspectos informativos, físicos y humanos del ambiente, identificar y describir a los actores relevantes y determinar comportamientos probables de estos actores con el propósito de identificar amenazas, vulnerabilidades y oportunidades en el ambiente de la información y tener una mejor comprensión de qué motiva el comportamiento del actor relevante para saber afectarlo y cómo afectarlo para lograr los objetivos.

Para apoyar la toma de decisiones humanas y automatizadas deberá facilitarse la comprensión compartida en toda la fuerza conjunta, proteger la información amigable, las redes y los sistemas de información, la moral y la voluntad de la fuerza conjunta. De esa forma el Comandante dispondrá de información precisa y oportuna en la cual basar sus decisiones, podrá comunicarlas y la fuerza conjunta será capaz de mantener su moral y voluntad contra la influencia maligna.

Por último, para aprovechar la información, deberá informar a las audiencias nacionales e internacionales, influir en actores extranjeros relevantes, atacar y explotar la información y las redes los sistemas de información de los actores relevantes para poder afectar los motivos del comportamiento del actor relevante y, en última instancia, el comportamiento de esos actores relevantes en apoyo de los objetivos y resultados duraderos del Comandante y las operaciones y actividades de las fuerzas conjuntas serán percibidas como legítimas y justificadas por el público nacional e internacional.

Las funciones conjuntas generalmente están alineadas con las Áreas de Capacidad Conjuntas, que son sumas de capacidades similares agrupadas funcionalmente para apoyar el análisis de capacidades y la toma de decisiones de inversión (Radabaugh, 2018). En la República Argentina son: C^3 I^2, Movilidad Táctica y Estratégica, Vigilancia, Reconocimiento e Inteligencia, Sostén Logístico, Desarrollo de Operaciones, Protección de Fuerzas y/u Objetivos Estratégicos Apoyo Ecológico, Científico, Humanitario y de Misiones de Paz (República Argentina EMCO, PC 20-09, 2008).

Estas capacidades genéricas, que cubren todo el espectro que necesitan las Fuerzas Armadas para ser empleadas en las misiones que le han sido asignadas, permiten la acción combinada de múltiples sistemas, orientados a conseguir un determinado efecto militar. La sinergia que surge de la forma en que se combinan y se aplican, permitirá establecer el nivel de capacidad dentro de un contexto particular.

Esa capacidad brindará la aptitud o suficiencia de la organización para lograr un efecto deseado en un ambiente dado, dentro de un determinado tiempo, y de sostenerlo por un plazo establecido. Abarca un conjunto de factores **M**aterial, **I**nfraestructura, **R**ecursos humanos, **I**nformación, **L**ogística, **A**diestramiento, **D**octrina y **O**rganización (MIRILADO), empleados en base a principios y procedimientos doctrinarios (República Argentina EMCO, PC 20-09, 2008).

La publicación JP 3-04 (2022) refiriéndose a estos factores señala:

> El establecimiento de la función conjunta de información y el desarrollo de esta publicación conjunta (JP) sobre información en operaciones conjuntas está impulsando cambios en las operaciones conjuntas y de las Fuerzas DOTMLPF-P [doctrina, organización, capacitación, material, liderazgo y educación, personal, instalaciones y política]. Un cambio doctrinario significativo es la transición de las operaciones conjuntas de información (OI) a las operaciones en el ambiente de la información (OIE). Esta transición es un desafío sustancial para el desarrollo de la fuerza que requiere que la fuerza conjunta evalúe cómo organizar las fuerzas y el personal para planificar y ejecutar deliberadamente las OIE.

A modo de síntesis, la nueva Doctrina Conjunta de los Estados Unidos "Información en Operaciones Conjuntas" (Information in Joint Operations: JP 3-04, 2022) enfatiza la necesidad de que los comandantes y planificadores incorporen la información como un elemento fundamental de todas las operaciones. Esto incluye comprender cómo la

información afecta el ambiente operacional (OE), cómo respalda la toma de decisiones humanas y automatizadas y cómo aprovechar la información para lograr los objetivos. Comprender el poder de la información permite informar, persuadir e influir en los actores del OE.

2.7. **El efecto deseado: operaciones o actividades de Influencia**

El propósito o el efecto final deseado de la tríada compuesta por la comunicación estratégica, la narrativa y las operaciones en el ambiente de la información no es otra cosa que la de influir sobre un actor relevante para afectar sus percepciones, actitudes y otros motivadores de su comportamiento relevante del actor. Para ello es necesario impactar sobre los aspectos humanos en la medida en que se relacionan con los tomadores de decisiones (por ejemplo, la cultura de cada decisor, las experiencias de vida, las relaciones, los eventos externos, la ideología y las influencias de esas personas dentro y fuera del grupo de tomadores de decisiones).

Si bien esta investigación está centrada en las operaciones en el ambiente de la información, en términos generales, todas las operaciones militares son al final operaciones de «influencia». En otras palabras, a falta de una rendición incondicional, todas ellas se llevan a cabo para influir en un adversario para que tome una decisión favorable a los objetivos propios ya sea por métodos cinéticos o no cinéticos.

Las actividades de influencia en un escenario de conflicto son con frecuencia psicológicamente sensibles en el sentido de que su propósito es más que simplemente persuadir a un objetivo para que cambie una creencia o actitud. Los mensajes en tiempos de guerra con frecuencia consisten en esfuerzos unificadores y destructivos, que en el caso de estos últimos incluyen mensajes disruptivos. Los mensajes unificadores sirven para robustecer el apoyo interno o el potencialmente comprensivo externo y promueven la participación activa en el esfuerzo de guerra o al menos minimizan la disidencia y la oposición. Los destructivos consisten en los esfuerzos psicológicamente más agresivos donde las acciones deliberadas y el engaño son integrales e inseparables de los mensajes típicos (Courter, 2022).

El término “influencia” implica “producir sobre algo o alguien ciertos efectos” con lo cual a veces tiene connotaciones negativas pues a menudo se asocia con manipulación o explotación engañosa razón por la cual, lo que se denominaba “Operaciones de Influencia” fue sufriendo modificaciones hasta llegar al día de hoy a lo que la publicación JP 3-04 llama “actividades de influencia” ya sean maliciosas o las planificadas por la propia fuerza.

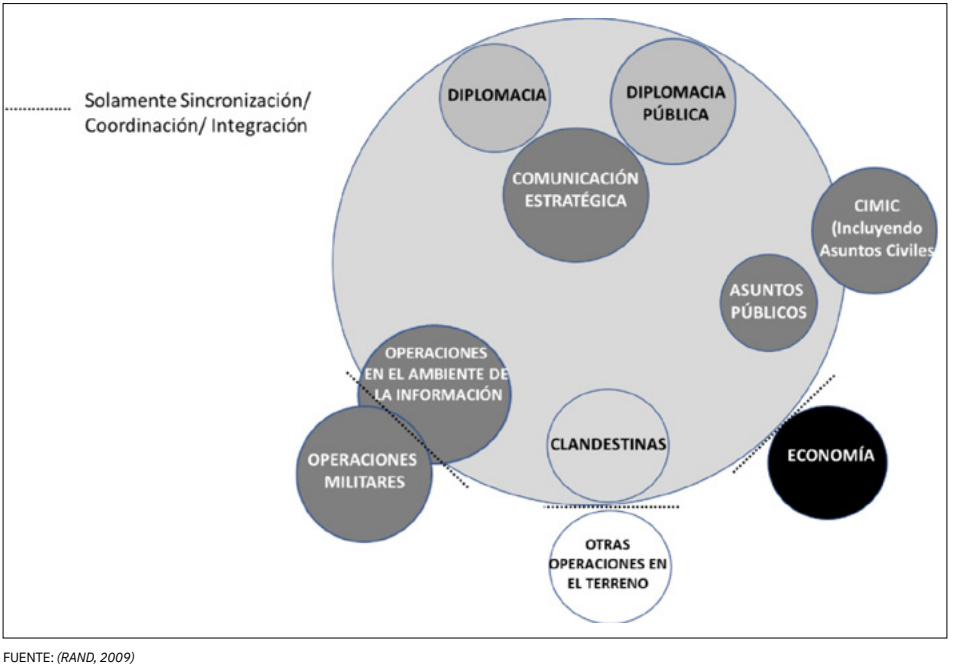
Aunque el debate gira en torno a la definición y medición precisas del marco de operaciones de influencia, los responsables políticos coinciden en que sigue siendo un área críticamente poco estudiada de la política internacional y de hecho se utilizan diferentes términos, como ya se ha visto, para describir el amplio espectro de actividades relacionadas con contrarrestar y proyectar influencia en el extranjero. No obstante, un estudio patrocinado por el Departamento de Defensa en el año 2009 define las operaciones de influencia como «la aplicación coordinada, integrada y sincronizada de

capacidades diplomáticas, informativas, militares, económicas y de otro tipo nacionales en tiempos de paz, crisis, conflictos y posconflictos para fomentar actitudes, comportamientos o decisiones de audiencias objetivo extranjeras que promuevan los intereses y objetivos de los Estados Unidos» (RAND, 2009).

En el nivel nacional, esta definición enfatiza la importancia de coordinar y sincronizar los activos estratégicos en las operaciones de influencia ofensivas y defensivas. En el marco actual, el USG tiene una amplia gama de agencias y unidades que trabajan en operaciones de influencia sin coordinación directa o las autorizaciones legales apropiadas.

> Este estudio utiliza el concepto de Operaciones de Influencia como un término general que incluye actividades militares (por ejemplo, Operaciones de Información, Asuntos Públicos, Apoyo Militar a la Diplomacia y Diplomacia Pública, y partes de Asuntos Civiles y Operaciones Cívico Militares) y civiles (que comprenden esfuerzos públicos y encubiertos, o clandestinos). Es importante destacar que las operaciones de influencia incluyen actividades informativas que no son del Departamento de Defensa (DoD), como las actividades diplomáticas y diplomáticas públicas del Departamento de Estado y las actividades de influencia realizadas por la comunidad de inteligencia de los Estados Unidos (RAND, 2009).

ILUSTRACIÓN 42 . **Elementos de las Operaciones de Influencia**



FUENTE: *(RAND, 2009)*

La ilustración muestra claramente que el concepto de "Operaciones de influencia" es una idea abarcadora del empleo de los factores de poder diplomático, de información, militar y económico (DIME).

A juicio de Soriano, lo más importante es la idea de que las diversas comunicaciones y otras actividades deben coordinarse y sincronizarse con las actividades "cinéticas" del mundo real, como las operaciones militares, las actividades de reconstrucción y otros asuntos civiles, el desarrollo económico y otras actividades que se desarrollan "sobre el terreno". Por lo tanto, se plantea la idea de que no solo se influye en el ámbito cognitivo a través de construcciones discursivas, sino incidiendo sobre la realidad para que la población extraiga un determinado significado (Soriano, 2022).

> En un contexto teórico más amplio, las operaciones de influencia son una de las herramientas a las que recurren los contendientes que están inmersos en un conflicto en la zona gris. Este enfoque pone en el epicentro del conflicto a la población civil, tanto a la propia como a la del enemigo y a la de aquellos actores que no son parte implicada en el enfrentamiento. La zona gris requiere una narrativa atractiva que la sostenga, y que haga posible la movilización de la población a favor de una determinada causa. La ambigüedad con la que se desarrollan los conflictos en la zona gris convierte las operaciones de influencia en uno de los principales instrumentos con los que cuenta cualquier contendiente que desee modificar la realidad a su favor.

Ese mismo año 2009, el Estado Mayor Conjunto de los Estados Unidos expresaba que la influencia se ejerce a través de la comunicación, específicamente a través de la recepción, comprensión y aceptación de un mensaje. La capacidad de influir es tan fuerte como la capacidad de comunicar preferencias. Influir eficazmente significa comunicarse eficazmente. De hecho, el propósito fundamental de toda comunicación con propósito es influir, causar algún efecto deseado, que podría ser un comportamiento observable o una actitud no observable (Staff, 2009).

En 2014, el jefe del Estado Mayor del Ejército, el general Raymond Odierno, suspendió el uso de la doctrina de Actividades de Información e Influencia (IIA) promulgada por el Army Field Manual

ILUSTRACIÓN 43 . **Actividades de Informar y Influenciar**

FUENTE: *(UNITED STATES ARMY, 2013)*

(FM) 3-13, publicado en enero de 2013. El IIA hacía hincapié en la importancia de interactuar con el público extranjero y nacional para lograr objetivos militares (Sheiffer, 2018). Aunque se basaba en la doctrina de las Operaciones de Información (IO), solo enfatizaba las capacidades más centradas en el ser humano, como la participación clave del líder, los asuntos públicos y las Operaciones de Apoyo a la Información Militar (MISO ex Operaciones Psicológicas).

En 2022, la corporación Rand, en un trabajo encargado por la *US. Air Force,* cita a dos "expertos en esfuerzos de influencia rusos en Europa" para describir a las Operaciones de Influencia como "la ejecución de las operaciones de información, la mayoría de las veces vagamente organizada y delegada a una amplia variedad de actores», algunos de los cuales «están estrechamente vinculados a una cadena de mando, otros lo están mucho más tenuemente a las autoridades gubernamentales» (Elina Treyger, Joe Cheravitch, Raphael S. Cohe, 2022).

Uno de dichos expertos, Constanze Stelzenmüller, en un testimonio presentado ante el Comité de Inteligencia del Senado de los Estados Unidos, el 28 de junio de 2017 mencionaba las operaciones de influencia, pero no las definía (Stelzenmüller, 2017):

> Una Alemania dividida fue la Zona Cero para el espionaje, la propaganda y otros tipos de operaciones de influencia a lo largo de la Guerra Fría; esto no terminó con la caída del Muro de Berlín. Los expertos identifican el regreso de Vladimir Putin a la presidencia rusa en 2000 como el comienzo de un trabajo mucho más sistemático de las operaciones de influencia dirigidas a Europa y Alemania, con un aumento notable tras la decisión de Alemania de apoyar los esfuerzos de Ucrania para unirse a Europa.
>
> Otros canales potenciales de operaciones de influencia rusa incluyen «agentes de influencia» que promueven los intereses y narrativas rusas voluntaria o involuntariamente, ya sean políticos, académicos, empresarios o periodistas.

Considerando que desde un punto de vista totalmente civil, Facebook en 2017, adoptaba la siguiente definición (Jen Weedon, 2017):

> Operaciones de información (o influencia): acciones tomadas por gobiernos o actores no estatales organizados para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas (amplificadores falsos) destinadas a manipular la opinión pública.

Stockton considera que adoptar la definición de medios sociales como Facebook constituye una forma de escapar de la maraña de definiciones y de los formuladores de políticas que exacerban esta confusión al cambiar el significado de la terminología relacio-

nada con las operaciones de información ya que su colaboración es esencial para fortalecer la defensa nacional contra la coerción (Stockton, 2021).

> Esta definición tiene el beneficio de resaltar los medios por los cuales Rusia y otros rivales están deformando la opinión pública estadounidense para obtener ventajas estratégicas. Sin embargo, el uso de Facebook también tiene una limitación crítica: se centra en operaciones ofensivas y excluye medidas defensivas para bloquear o derrotar narrativas falsas presentadas por oponentes.

En 2021, expresa (Facebook, 2021):

> En los últimos cuatro años, la industria, el gobierno y la sociedad civil han trabajado para construir nuestra respuesta colectiva a las operaciones de influencia, que definimos como «esfuerzos coordinados para manipular o corromper el debate público para un objetivo estratégico».
>
> Históricamente, las operaciones de influencia se han manifestado en diferentes formas: desde campañas encubiertas que se basan en identidades falsas hasta esfuerzos de medios abiertos controlados por el estado que utilizan voces auténticas e influyentes para promover mensajes que pueden o no ser falsos.
>
> En los últimos años, gran parte de la atención pública se ha centrado en la «interferencia extranjera» (es decir, las operaciones encubiertas de influencia de origen extranjero) y el riesgo que representa para la integridad de las elecciones y la confianza en los sistemas democráticos. Si bien los ejemplos contemporáneos más estudiados fueron dirigidos por actores extranjeros, las operaciones de influencia son herramientas cada vez más comunes para los actores no estatales y nacionales. En los últimos años, hemos visto surgir nuevos actores, incluidas entidades comerciales y grupos de interés político, que llevan a cabo campañas de IO tanto extranjeras como nacionales.

ILUSTRACIÓN 44 . **Países de donde provienen la mayoría de las redes de comportamiento no auténtico (CIB por sus siglas en inglés)**[107]

FUENTE: FACEBOOK (GLEICHER, ET AL., 2021)

Para Facebook, "las operaciones de influencia en los últimos años han irrumpido en la conciencia pública global. Estas campañas intentan socavar la confianza en las instituciones cívicas y corromper el debate público mediante la explotación de las mismas herramientas digitales que han diversificado al público en línea (*online*) y han empoderado las discusiones críticas desde *Me Too* hasta los movimientos *Black Lives Matter*". (Facebook, 2021)

La Estrategia Nacional de Contrainteligencia de los Estados Unidos enfatiza que los adversarios ya están llevando a cabo campañas para «influir y engañar a los tomadores de decisiones clave razón por la cual uno de los objetivos de dicha estrategia es el de "Defender la democracia estadounidense contra las amenazas de influencia extranjera para proteger las instituciones y procesos democráticos de Estados Unidos y preservar nuestra cultura de apertura. Las entidades de inteligencia extranjeras están llevando a cabo campañas de influencia para socavar la confianza en nuestras instituciones y procesos democráticos, sembrar divisiones en nuestra sociedad, ejercer influencia sobre Estados Unidos y debilitar nuestras alianzas" (NCSC, 2020).

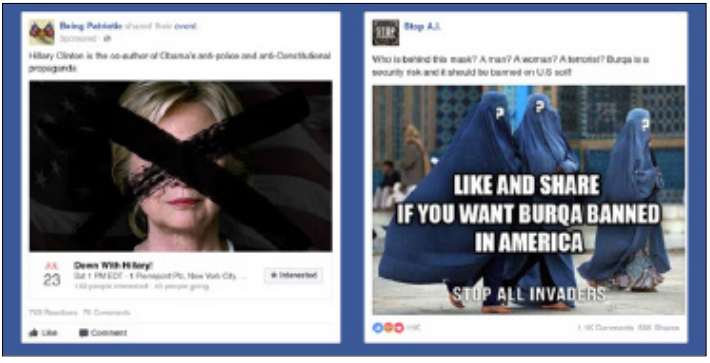
ILUSTRACIÓN 45 . **Campañas de influencia**

FUENTE: VARIAS FUENTES

Cuestiones como la raza, el género, la orientación sexual, el aborto o la vacunación pueden, hacer que los países sean especialmente vulnerables a estos ataques o a la influencia extranjera. La raza fue el principal objetivo de la desinformación rusa durante las elecciones presidenciales estadounidenses de 2016, con el objetivo de ayudar a Donald J. Trump y socavar a su oponente, Hillary Clinton. En general, la estrategia de desinformación contra los países occidentales no es crear una historia falsa, una mentira, sino amplificar las quejas existentes (Walton, 2022).

107 Comportamiento no auténtico: CIB es cualquier red coordinada de cuentas, páginas y grupos en nuestras plataformas que se basa centralmente en cuentas falsas para engañar a Facebook y a las personas que utilizan nuestros servicios sobre quién está detrás de la operación y qué están haciendo.

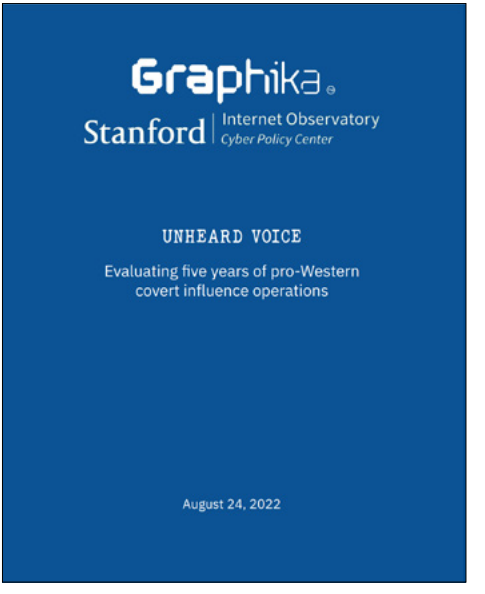
ILUSTRACIÓN 46 . **Anuncios de Facebook que Rusia utilizó en su esquema de influencia electoral de 2016**



FUENTE: *(WYRICH, 2017)*

También existen ejemplos que muestran las campañas de influencia estadounidenses. En julio y agosto de 2022, Twitter y Meta eliminaron dos conjuntos de cuentas superpuestas por violar los términos de servicio de sus plataformas. Twitter dijo que las cuentas infringieron sus políticas sobre «manipulación de plataformas y spam», mientras que Meta dijo que los activos en sus plataformas participaron en un «comportamiento no auténtico coordinado». Después de retirar los activos, ambas plataformas proporcionaron partes de la actividad a Graphika y al Observatorio de Internet de Stanford (SIO) para su posterior análisis la cual encontró una red interconectada de cuentas en Twitter, Facebook, Instagram y otras cinco plataformas de redes sociales que utilizaron tácticas engañosas para promover narrativas prooccidentales en el Medio Oriente y Asia Central (Observatory, 2022).

ILUSTRACIÓN 47 . **Informe Graphika.**



FUENTE: (OBSERVATORY, 2022).

> Los conjuntos de datos de las plataformas parecen cubrir una serie de campañas encubiertas durante un período de casi cinco años en lugar de una operación homogénea. Estas campañas avanzaron consistentes en narrativas no convencionales promovían los intereses de los Estados Unidos y sus aliados mientras se oponían a países como Rusia, China e Irán. Los relatos criticaron dura–mente a Rusia en particular por la muerte de civiles inocentes y otras atrocidades que sus soldados cometieron en pos de las «ambiciones imperiales» del Kremlin

> tras su invasión de Ucrania en febrero de este año. Para promover esta y otras narrativas, las cuentas a veces compartían artículos de noticias de medios de comunicación financiados por el gobierno de los Estados Unidos, como Voice of America y Radio Free Europe, y enlaces a sitios web patrocinados por el ejército de los Estados Unidos. Una parte de la actividad también promovió mensajes contra el extremismo (Observatory, 2022).

Tras conocerse dicho reporte, el 19 de septiembre, el Washington Post en un artículo titulado "El Pentágono abre una amplia revisión de las operaciones psicológicas clandestinas" expresó que las quejas sobre las operaciones de influencia del ejército estadounidense utilizando Facebook y Twitter han generado preocupación en la Casa Blanca y las agencias federales" (Nakashima, 2022) e indicaba que el subsecretario de Defensa para Políticas, había instruido a los comandos militares que participan en operaciones psicológicas en línea a proporcionar un informe completo de sus actividades para el próximo mes después de que la Casa Blanca y algunas agencias federales expresaron su creciente preocupación por el intento de manipulación del Departamento de Defensa de las audiencias en el extranjero.

En sentido inverso, el 27 de septiembre de 2022, la empresa matriz de Facebook, Meta, anunció que había detectado y cerrado dos redes separadas de cuentas falsas involucradas en operaciones de influencia encubiertas dirigidas desde Rusia y China (O›Sullivan, 2022):

> En cuanto a la campaña rusa, según dijo Meta, más de 2.000 cuentas y páginas de Facebook fueron parte del esfuerzo para impulsar las narrativas pro-Kremlin sobre la guerra en Ucrania. Se gastaron más de $ 100,000 en anuncios en Facebook e Instagram como parte de la campaña y la operación incluyó sitios web que fueron diseñados para imitar a los medios de comunicación occidentales reales, incluido The Guardian, The Daily Mail y los medios alemanes Bild y Der Spiegel.
>
> La red china era pequeña y apenas recibía atención, pero sí incluía algunas cuentas que se hacían pasar por estadounidenses en ambos lados del espectro político. Estaban manejando cuentas falsas que fingían ser estadounidenses y trataban de hablar como estadounidenses y estaban hablando de temas domésticos realmente divisivos como el aborto y el control de armas.

El sitio web falso de The Guardian promovido por el grupo contenía una historia, supuestamente escrita por Jonathan Freedland, titulada «Falsa puesta en escena en Bucha revelada», que pretendía revelar que «una sangrienta provocación con docenas de cuerpos civiles fue preparada por el ejército ucraniano para acusar a Rusia de asesinato en masa» en Bucha. Aparte de la historia en sí, el sitio web era una copia perfecta de The Guardian, hasta los enlaces actualizados «más vistos» y una solicitud para otorgar permiso para las cookies (Hern, 2022).

ILUSTRACIÓN 48 . **Derribo del comportamiento inauténtico coordinado de Rusia y China**

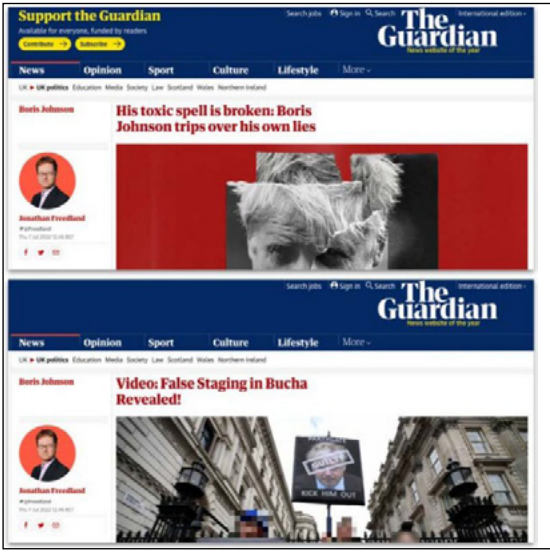


Imagen superior
Captura de pantalla de un articulo en el sitio web genuina de The Guardian theguardian. com. 7 de julio de 2022 mostrando el autor y la mana de tempo a la izquierda.

Imagen interior
Captura de pantalla de un articulo en el sto web falsificado de The Guardian theguardian. co.com, que muestra el mismo autor y marca de tempo, pero un texto y una foto diferentes. El sitio web fue registrado ese dia

FUENTE: *(NIMMO, 2022)*

Para contrarrestarlas las operaciones de influencia, Díaz-Caneja recomienda que, a la hora de analizarlas, debe estudiarse, en primer lugar, al supuesto actor o actores que tienen la intención de influir, prestando especial atención a tres aspectos clave, que, de no identificarse, será muy difícil, tanto neutralizar los intentos de influencia como la identificación de su origen, es decir, el actor o actores que están detrás (Díaz-Caneja, 2022):

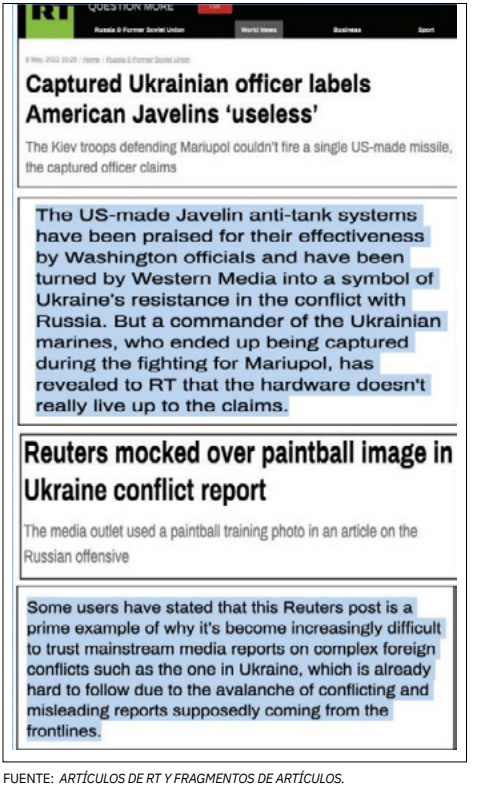
- Los efectos que pretende conseguir;
- Las acciones que lleva a cabo para alcanzar los efectos deseados;
- La estructura que utiliza para ejecutar sus acciones.

Insikt Group, por ejemplo, ha identificado múltiples narrativas de influencia rusas cuyos efectos intentarían socavar y dividir indirectamente a la coalición occidental, dirigida principalmente a Francia, Alemania, Polonia y Turquía, incluyendo: agitar el descontento interno hacia los líderes políticos occidentales; mostrar negativamente a los refugiados ucranianos y los impactos que tienen en sus países de acogida; culpar a los gobiernos occidentales de sus preocupaciones económicas, energéticas y de seguridad alimentaria por sus políticas negativas hacia Rusia; culpar a Ucrania como la fuente de los movimientos fascistas modernos; e incitar a la desconfianza de los medios occidentales (Insikt Group, 2022).

Para alcanzar dichos efectos:

> Las redes de influencia rusas, incluidas las organizaciones de medios estatales rusos, las cuentas OSINT pro-rusas, los grupos falsos de «verificación de hechos» y otras organizaciones de «teoría alternativa», particularmente en Telegram, están incitando a la desconfianza en la cobertura de los medios occidentales de la guerra de Rusia contra Ucrania. Esto incluye investigaciones de los medios occidentales sobre los crímenes de guerra rusos, informes de estado del campo de batalla y otras «mentiras» reportadas por los medios occidentales.
>
> El Kremlin probablemente espera que el impacto de la guerra de Rusia contra Ucrania, incluido el retroceso de las sanciones, tensará aún más la relación entre las poblaciones occidentales y sus gobiernos. Con el tiempo, esto probablemente resultará en una disminución natural del apoyo a la coalición occidental, como resultado tanto del agotamiento con la guerra como de la falta de apetito por el dolor económico a largo plazo. Es casi seguro que las operaciones de información rusas intentarían explotar esta oportunidad para inclinar la opinión internacional a su favor.

ILUSTRACIÓN 49 . **Critican la cobertura de la guerra de los medios occidentales y sugieren que estos medios no son confiables.**



FUENTE: *ARTÍCULOS DE RT Y FRAGMENTOS DE ARTÍCULOS.*

Finalmente, tanto Merlín Boone (Boone, 2021) como Soriano (2022)., adhieren a la definición de Larson (Larson, 2009) contenida en el estudio de la Rand Corporation antes mencionado, según la cual las operaciones de influencia son:

> La aplicación coordinada, integrada y sincronizada de capacidades diplomáticas, informativas, militares, económicas y de otro tipo nacionales en tiempos de paz, crisis, conflictos y posconflictos para fomentar actitudes, comportamientos o decisiones de audiencias objetivo extranjeras que promuevan los intereses y objetivos del actor que las lleva a cabo.

Como en toda actividad de influencia cobra gran importancia la narrativa que se utiliza para la trasmisión del mensaje, la cual puede llegar a dominar el pensamiento colectivo, y una vez arraigada puede ser muy difíciles de cambiar. De dicha narrativa dependerá la comunicación estratégica pues será la que transfiera significado y altere los comportamientos hacia el fin deseado, a veces independientemente de los efectos colaterales. Desde la diplomacia pública y los asuntos públicos hasta la propaganda y la desinformación, los hechos, las palabras, los símbolos y las creencias son la moneda (Popescu, 2020). De allí la necesidad de que las operaciones de influencia y la comunicación estratégica se encuentren sólidamente articuladas.

Para ser eficaces, deberán estar sincronizadas, coordinadas e integradas con otros medios de poder de un Estado, actuando como parte de estrategias más amplias y coherentes.

Una de las confusiones más frecuentes es aquella que equipara las campañas de desinformación a las operaciones de influencia. El problema radica en que mientras que las tácticas desinformativas resultan éticamente reprobables y son el terreno natural de acción de los poderes autocráticos, las operaciones de influencia son un espacio legítimo para que los actores democráticos promuevan sus intereses entre audiencias externas (Soriano, 2022).

3. **CONCLUSIONES**

La Cuarta Revolución Industrial ha provocado profundos cambios en el carácter de la guerra. Su naturaleza fundamental puede permanecer constante, como hace años sostuvo Clausewitz, pero las formas en las que se libran cambian constantemente a medida que evolucionan las sociedades.

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC's), los distintos campos de la ciencia de datos (*Data Science*), el aprendizaje automático (*Machine Learning*) y la inteligencia artificial (*Artificial Intelligence*) han llevado a un aumento exponencial del poder de la información, dando lugar a un entorno multidimensional que se ha expandido más allá de los límites conceptuales clásicos de los cinco ambientes que describe la literatura militar: terrestre, aéreo, marítimo, espacial y ciberespacio.

En ese ambiente de la información, los individuos, los grupos de intereses especiales y los adversarios pueden apuntar a los fundamentos cognitivos de los individuos (creencias, normas, emociones, experiencias y salud mental) utilizando datos e información para influir en las decisiones y acciones con fines benignos o malignos.

Los conflictos que se han venido desarrollando en este Siglo XXI han mostrado que el éxito en las operaciones militares a menudo se pudo lograr o perder en función de cómo las audiencias internacionales, regionales y nacionales percibieron las palabras y acciones pues ganar el apoyo de dichas audiencias y derrotar el mensaje del adversario resultó a menudo una batalla crítica para alcanzar una victoria duradera.

El incremento de la velocidad de transmisión de la información y el aumento de la cantidad de información disponible en todo momento, han hecho cada vez más vulnerables a los estados, a las instituciones y a los individuos.

En este contexto, tanto la Unión Europea, como la OTAN y los Estados Unidos de América se perciben atacados por una serie de acciones en el ambiente de la información, que incluye el ciberespacio, en lo que consideran una Guerra de la Información llevada a cabo por sus adversarios y competidores a fin de desestabilizarlos y coaccionarlos o influir negativamente sobre sus poblaciones. Es así que la Guerra de la Información tiende a ser calificada de manera peyorativa como propaganda. También se emplea la frase: *actividad de influencia maliciosa.*

Para combatir los efectos de la *propaganda extranjera* la OTAN se vio en la necesidad de desarrollar estrategias de comunicación en el nivel estratégico y operacional de manera coordinada, coherente y planificada, empleando todos los medios y capacidades de comunicación de los instrumentos del poder nacional, para generar percepciones y adhesiones favorables. La comunicación dejó de ser ocasional e inoportuna para ser planificada, integrada y dirigida a lograr objetivos.

Es lo que se conoce como *Comunicación Estratégica* destinada a influir en las actitudes, creencias y comportamientos de las audiencias de manera de que tomen decisiones en contra de sus intereses, pero en beneficio de quien lleva a cabo dicha forma de hacer la guerra. La información es empleada como un arma a fin de lograr un efecto, que puede ser el de contrarrestar y/o proyectar actividades de influencia lo cual puede adquirir una connotación diferente en el entorno civil y en el militar.

El Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, la define de manera bastante amplia e incluye dentro de esa definición a la diplomacia pública, los asuntos públicos, los asuntos públicos militares y las operaciones en el ambiente de la información del nivel operacional.

Incluso la ONU ha reconocido que en las operaciones de paz las comunicaciones estratégicas son esenciales para cumplir sus mandatos y gestionar las expectativas sobre lo que pueden y no pueden lograr. Esto la ha llevado a aumentar sus capacidades de comunicación y cambiar su enfoque lejos del modelo tradicional de comunicación unidireccional de arriba hacia abajo.

De esa manera la Comunicación Estratégica se convierte en un marco apropiado para explicar el desarrollo, la implementación, la evaluación y la evolución de acciones y mensajes públicos en apoyo de políticas, intereses y objetivos. La Comunicación Estratégica debe reunir fines (objetivos), modos (tácticas) y medios (recursos) para lograr cambios mensurables en el comportamiento o la percepción.

Para ello toda Comunicación Estratégica debe poseer una narrativa estratégica, una historia, oral o escrita, de eventos e información, organizada en una secuencia lógica y diseñada para explicar la justificación para llevar a cabo una actividad y el resultado buscado. La narrativa proporciona el *¿por qué?*

Todo ello se lleva a cabo para lograr influir en las funciones cognitivas de un adversario en todo el espectro del conflicto, desde el sentimiento público en tiempos de paz, como puede ser influir en una elección nacional, hasta la toma de decisiones en una guerra abierta como puede ser capitular. Esto recibe el nombre de *operaciones de*

influencia las cuales además del poder de la información abarcan los poderes diplomáticos, militares y económicos de un Estado.

Estas operaciones de influencia no son en principio ni buenas ni malas; depende de las propias sociedades decidir qué conducta y respuestas son y no son aceptables lo cual es muy ambiguo porque es muy difícil determinar los motivos que impulsan a los actores detrás de ellas.

En el ámbito militar esta narrativa debe mostrar consistencia en todos los niveles: estratégico, operacional y táctico con la política y la narrativa nacional. Las palabras, las imágenes y las acciones deben ser coherentes entre sí y esto es un desafío, ya que el contenido del mensaje puede diferir en caden el nivel dependiendo de la audiencia.

La narrativa proporciona la visión general para el empleo de las operaciones conjuntas en el ambiente de la información en el nivel operacional de manera tal de poder alinear y sincronizar los esfuerzos y conducir las operaciones.

La Publicación Conjunta JP 3-04 (2022) *Información en operaciones conjuntas,* publicada el 14 de septiembre de 2022, basándose en la doctrina anterior introduce algunos conceptos nuevos, alejándose de las *operaciones de información* y avanzando hacia *operaciones en el ambiente de la información* más desarrolladas. También el Cuerpo de Marines recientemente dio a conocer la Publicación de Doctrinaria del Cuerpo de Marines-8, Información, que se basa en la doctrina MCDP-1, Warfighting y describe cómo incluir la información en ella.

Es así como las operaciones en el ambiente de la información tienden a ser de naturaleza operacional y táctica en su forma y ejecución. Falta aún ver cómo esta nueva doctrina se implementará. Por el momento el resto de los países y la OTAN, cuya doctrina no fue actualizada, no han mostrado cambios en ella.

Las operaciones de información, tal como se conocían pasaron a ser una función conjunta debiéndose ser integradas con las otras funciones conjuntas (C2, fuegos, inteligencia, movimiento y maniobra, protección, sostenimiento) a fin de alterar positivamente las percepciones y comportamientos de los actores relevantes en un ambiente multidominio.

Para el planeamiento, los comandantes suelen organizarse, dentro de una estructura de Estado Mayor tradicional napoleónica jerárquica de J que ha sido utilizada por las organizaciones militares durante siglos y continúa siéndolo, asignándole la responsabilidad de integración de los efectos informativos a un oficial, generalmente el Jefe de Operaciones de Información o al Oficial de Operaciones. Este oficial, deberá interconectar los J del Comando Operacional e incorporar a especialistas, asesores, y partes interesadas, al mismo tiempo que se conecta con los comandos de los componentes en lo que se conocen como Células o Juntas de Operaciones de Información.

Hasta aquí se ha intentado describir o conceptualizar el empleo del ambiente de la información como parte de un esfuerzo de influencia más amplio, favorecido por las tecnologías de la información y de la comunicación, lo cual ha proporcionado un fácil acceso a amplias audiencias. La forma en que se aprovecha la información para pro-

mover difiere en función de cómo se utilizan otros elementos del poder nacional (diplomático, económico y militar).

Lo hasta aquí explicado se centró en mostrar cómo los países occidentales analizados y la ONU se han preparado y continúan trabajando para contrarrestar las operaciones en el ambiente de la información, comprendidas dentro de un contexto más amplio como son las operaciones de influencia, y cómo los responsables políticos buscan alinear esos esfuerzos con medidas que impidan y/o dificulten a sus oponentes o terceros interesados en afectar las percepciones del panorama político, socavar la confianza en los gobiernos y, a veces, movilizar la violencia interna de un país, para alcanzar sus objetivos.

En el pasado, las guerras se han librado principalmente físicamente, siendo los ejércitos, la fuerza aérea y las operaciones navales las principales formas de combate.

Internacionalmente, hay cuatro instrumentos reconocidos de poder nacional o fuerzas de la Nación: diplomático, informativo, militar y económico, creando el acrónimo DIME. La frase instrumentos de poder nacional se refiere a las herramientas que un país utiliza para influir en otros países u organizaciones internacionales o incluso en actores no estatales.

En la actualidad, las Tecnologías de la Información y la Comunicación, han facilitado la creación de un ambiente de la información que comprende y agrega numerosos atributos sociales, culturales, cognitivos, técnicos y físicos que actúan e impactan el conocimiento, la comprensión, las creencias, las visiones del mundo y, en última instancia, las acciones de un individuo, grupo, sistema, comunidad u organización.

Cada vez más, las decisiones humanas se basan en información de datos procesados por máquinas y no en los datos en sí. La información ha pasado a ser es un instrumento central y primario del poder nacional.

La fusión de información y tecnología generalizadas ha otorgado a individuos, organizaciones y estados-nación la capacidad de, antes, durante y después de un conflicto, de apuntar a las creencias, emociones y experiencias de personas con fines benignos o malignos tratando de influir, en este caso, sobre determinadas audiencias a través de la información ya sea falsa o basada en la realidad, pero presentada fuera de contexto para infringir daños o perjuicios a personas, organizaciones o países. La opinión pública puede ser manipulada a gran escala y de manera más rápida que en épocas pasadas.

La era de la información ha transformado la sociedad al permitir que las personas interactúen digitalmente, pero permite a los actores motivados utilizar la influencia masiva para promover sus objetivos políticos. La lucha contra la desinformación requiere una apreciación de cómo se puede lograr un efecto para contrarrestarla.

El actual conflicto entre la Federación de Rusia y Ucrania muestra que no es solamente cinético: implica una lucha sobre la voluntad de los líderes y la opinión pública ucraniana, rusa y la comunidad internacional. En ella, la difusión de información a través de medios digitales se ha convertido en un factor importante para tratar de dar forma a un resultado favorable de la guerra a alguna de las partes.

El tratar de encontrar una definición precisa para cada una de las operaciones que se desarrollan en el ambiente de la información resulta difícil. Cada país, por distintas razones, tiene la propia. Aun en organizaciones transnacionales como la OTAN, cuyas partes acuerdan un enunciado común, individualmente en sus doctrinas nacionales adoptan otras particulares.

Sin embargo, si existe alguna coincidencia tanto en occidente como en oriente es que estas operaciones deben ser diseñadas y ejecutadas siguiendo una pirámide jerárquica en cuyo vértice se encuentra la Estrategia Nacional.

Su instrumentación requiere de un liderazgo reconocido capaz de asignar, dirigir, asignar recursos o guiar la política en el campo altamente complejo y dispar y una visión nacional para aprovechar las fortalezas nacionales.

Los niveles estratégico militar y operacional apoyan la Comunicación Estratégica nacional para garantizar una unidad de temas y mensajes, confirmar o refutar con precisión los informes de las operaciones y reforzar la legitimidad de los objetivos estatales ante su propia sociedad y la comunidad internacional.

Para operar de manera efectiva se requiere comprender la interrelación de los aspectos informativos, físicos y humanos que comparten el ambiente operacional y el ambiente de la información y saber que el fin ulterior de las operaciones que en él se desarrollan es el de informar, influir, interrumpir, corromper o usurpar la toma de decisiones de adversarios y posibles adversarios mientras se protegen los propios.

Resulta complejo emplear las operaciones en el ambiente de la información, incluidas las cibernéticas, como complementos o sustitutos de las operaciones militares convencionales. Con mayor frecuencia se tiende a utilizar estos dos tipos de operaciones independientemente el uno del otro, debido tanto a la dificultad de coordinar estos modos de conflicto como a los diferentes objetivos estratégicos de cada uno de ellos. En la medida en que ello se perfeccione estas operaciones podrán comenzar a ejecutarse más como complementos entre sí para dar forma a la dinámica del campo de batalla.

Los esfuerzos nacionales para defenderse de las operaciones en el ambiente de la información de los adversarios casi siempre reflejan la necesidad de una respuesta de toda la nación. La tecnología seguirá siendo un elemento esencial y omnipresente del futuro ambiente operacional y un motor clave del cambio militar en los próximos 20 años.

Cada vez más, los sistemas de defensa y seguridad dependerán de la explotación de la investigación comercial y la innovación razón por la cual, en el nivel nacional, el sector privado e incluso el público, necesitan ser convocados, ya que hay oportunidades para ello. El intercambio de conocimientos entre diversas comunidades conducirá a tecnologías innovadoras. Hasta ahora se piensa que los efectos en el ambiente de la información son planificados por las personas, pero ¿cuál será el futuro rol de la Inteligencia Artificial en el ambiente de la información? ¿Quién comprobará los supuestos de los algoritmos?

En el siguiente capítulo se hará lo propio con países como la Federación de Rusia y la República Popular China quienes también tienen la percepción de que son igualmente tratados de influir por otros países o terceros interesados.

Capítulo 5

Las operaciones de información de la federación de Rusia y de la República Popular de China

Por CL (R) Mg. Gustavo A. Trama

1. **Introducción**

En este capítulo se analizarán las teorías de la Guerra de la Información *(informatsionnaya voyna)* y de la Confrontación de la Información *(informatsionnoe protivoborstvo)* de la Federación de Rusia y de las operaciones de las "Tres Guerras" (psicológica, de opinión pública y legal) de la República Popular China indagando en sus similitudes y diferencias y sus implicancias para Occidente como así también el rol que desempeñan las fuerzas armadas de dichos países en este tipo de operaciones.

2. **La federación de Rusia**

Siguiendo la línea de la investigación en esta sección se indagará sobre los distintos términos que la bibliografía occidental emplea para explicar las operaciones rusas en el ambiente de la información considerando que de la misma manera que Occidente percibe las operaciones rusas en el ambiente de la información como campañas de *desinformación* o de *propaganda* es necesario comprender que Rusia observa que las *campañas de información* son desarrolladas por Occidente para comprometer su soberanía nacional y facilitar el cambio de régimen de aquellos países que le son afines como en el caso de las Revoluciones de Colores y la llamada *Primavera Árabe.*

Para el Departamento de Estado de los EE.UU. las cinco principales narrativas persistentes de desinformación rusas son: Rusia es una víctima inocente; revisio-

nismo histórico; el colapso de la civilización occidental es inminente; los movimientos populares son "Revoluciones de color" patrocinadas por Estados Unidos y la realidad es lo que el Kremlin quiere que sea (DoE, 2022).

Con esta narrativa Rusia quiere mostrar que los Estados Unidos utilizan los medios y tecnologías de información y de otro tipo (incluidos los no tradicionales) con fines agresivos (expansionistas), para contribuir a la desestabilización de la situación político-militar rusa y la de los países afines a ella. En 2012, Igor Panarin[108] en una conferencia titulada: *The Information War against Russia: Operation Anti-Putin* (Panarin, 2012) expresaba:

> La creación de la Unión Euroasiática será una victoria en la primera fase de la Segunda Guerra Mundial de la Información. (Les recuerdo que la Primera Guerra Mundial de la Información terminó en el colapso de la URSS). Una condición importante para la victoria es la des-Gorbachovinización de la sociedad rusa. Después de que Vladimir Putin definiera la doctrina de la integración euroasiática como la nueva doctrina de Rusia, se convirtió en el objetivo principal de la guerra de información contra Rusia.

Para contrarrestar estas acciones en su contra, Rusia fue adaptando el pensamiento estratégico de larga data y las históricas doctrinas militares a las TIC´s procurando influir en naciones como Estados Unidos, Inglaterra y Francia o vecinos regionales como los Estados Bálticos, para causar confusión, manifestar tensiones étnicas y erosionar la confianza en las instituciones democráticas (Timur Chabuk y Adam Jonas, 2018) como en el caso de las interferencias rusas en el referéndum escocés de 2014, la votación de junio de 2016 sobre el Brexit y en las elecciones generales de diciembre de 2019 (Ellehuus, 2020), como así también en las elecciones presidenciales en los EE.UU. en 2016 (United States FBI, 2022).

La guerra de información de Rusia no es una amenaza aislada para Europa y los Estados Unidos, sino que es una estrategia global que afecta a cada región del mundo en diversos grados debido a su gran tamaño, masa y complejidad. El enfoque de Rusia de la guerra de la información es holístico, e incluye tanto los ataques cibernéticos como las operaciones de información como elementos cohesivos que trabajan en conjunto para lograr los objetivos de la política exterior rusa. Además, busca socavar no solo las fuerzas armadas de un adversario, sino también influir en las percepciones de la población objetivo de tal manera que favorezca los intereses rusos (Cunningham, 2020).

El objetivo estratégico de Rusia es socavar los cimientos del orden democrático liberal deslegitimando a los Estados Unidos como un socio creíble, intensificando

108 Igor Nikolaevich Panarin (n. 1958), decano de la escuela para futuros diplomáticos del Ministerio de Relaciones Exteriores de Rusia; https://rielpolitik.com/2020/09/29/from-information-warfare-to-the-break-up-of-the-usa-decoding-the-work-of-dr-igor-panarin-by-dr-kerry-bolton/

las divisiones dentro de la alianza transatlántica y erosionando el apoyo público a los valores y las instituciones. Su enfoque es confrontativo, destructivo y a menudo clandestino (Edward Lucas, 2021).

Términos como *propaganda, desinformación, medidas activas, control reflexivo* y otros conceptos relacionados fueron el lenguaje común entre los círculos civiles y militares soviéticos y occidentales a lo largo de la Guerra Fría. Al finalizar dicha guerra, algunos autores rusos comenzaron a utilizar el término "confrontación de la información" *(informatsionnoe protivoborstvo)* pero en el sentido de "superioridad de la Información" es decir, el estado que fuese capaz de recopilar, procesar y transmitir información más rápidamente y establecer el control sobre la información vital poseía una ventaja significativa (Michelle Grisé, 2022).

> Con el correr de los años y luego de haber analizado la guerra en Chechenia y las operaciones militares de los Estados Unidos y la OTAN, los analistas rusos fueron modificando la idea de que la confrontación de la información, solo se daría en los sistemas de Comando y Control, sino que también tendría lugar a través de los medios de comunicación y otras herramientas de poder blando.

En 1996 el General de División E. G. Korotchenko, subraya la importancia de lo que denominó "confrontación informativa-psicológica", un concepto relativamente amplio que combinaba elementos de las construcciones anteriores de guerra psicológica y propaganda. Korotchenko predijo que adversarios como los Estados Unidos intentarían influir en las percepciones y actitudes del liderazgo ruso, el público y el personal militar aprovechando los medios de comunicación extranjeros y otras herramientas de poder blando. Sin decirlo expresamente, insinuó que los medios de comunicación rusos estaban siendo utilizados como un instrumento de influencia, citando la difusión de falsedades como evidencia (Michelle Grisé, 2022)..

Desde principios de la década de 2000, las descripciones de las capacidades cibernéticas y la estrategia rusas giraban en gran medida en torno a dos términos: confrontación de información *(informatsionnoe protivoborstvo)* y guerra de información *(informatsionnaya voyna)*. En un artículo de 2003 titulado "Fuerzas de Confrontación de Información y Maskirovka", dos ex oficiales militares de alto rango, a la luz de la creciente atención de otros países para reforzar los "métodos y medios" para llevar a cabo la confrontación de información, sugirieron combinar elementos Maskirovka (engaño militar), operaciones psicológicas, inteligencia, guerra electrónica y operaciones de redes informáticas en un solo "sistema de confrontación de información" dentro del ejército; los autores agregaron que dicho sistema debería comenzar en niveles inferiores hasta que pudiera integrarse gradualmente en una estructura de personal unificada (Cheravitch, 2021).

> En 2003, un oficial de operaciones psicológicas afirmó que las dificultades que enfrentaron las fuerzas estadounidenses en Irak resultaron de la sobreesti-

> mación del ejército de sus tecnologías de "información avanzada" y su descuido de los factores psicológicos que afectan el campo de batalla. Dos años más tarde, el mismo oficial (junto con un coautor) señaló el "gran interés" que los especialistas prestaron al enfoque de China sobre los pilares técnicos y psicológicos de la "confrontación de información, "que complementa la tecnología moderna con los milenios de experiencia de China en la guerra asimétrica".

Según el mismo autor basado en la enciclopedia rusa militar y autoridades no militares, los términos *Confrontación de la Información* y Guerra (*warfare*) de la Información tienen dos significados diferentes como puede apreciarse en la siguiente ilustración:

ILUSTRACIÓN 50 . **Comparación de los términos "Confrontación de la Información" y "Guerra (warfare) de la Información" en la Federación de Rusia.**

Confrontación de la Información	Guerra (warfare) de la Información
Una parte integral de las relaciones y formas de conflicto entre las partes (gobierno, político-social, movimientos y organizaciones, fuerzas armadas y otros), cada uno de los cuales se esfuerza por infligir la derrota (destrucción) a través de la información». De acuerdo con esta definición, la derrota en el «ámbito de la información» se inflige a través de «armas de información», incluidos los medios de guerra electrónica y los efectos de «software electrónico». Las autoridades no militares sobre la confrontación de información la han definido como un «concurso de sistemas sociales» en el que un lado logra el predominio sobre el otro y cuyo propósito principal es «proporcionar seguridad psicológica de información» al estado. Estos expertos agregan que la confrontación de información sirve como una «respuesta asimétrica» a la «influencia externa de sujetos más fuertes».	La «colisión abierta y aguda» entre estados que explota los «ambientes de información» de los demás, que consisten principalmente en redes de telecomunicaciones, para «desestabilizar la sociedad y el gobierno». Los principales expertos no militares definen la guerra de información como una lucha abierta y encubierta entre sistemas de información en competencia para lograr una victoria decidida en el «ambiente material». En particular, el ministro de Defensa ruso, Sergey Shoygu, ha caracterizado los supuestos esfuerzos occidentales para socavar a Rusia a través de la tecnología de la información como «guerra de información», a menudo al describir el creciente potencial del ejército ruso para responder.

FUENTE: *(CHERAVITCH, 2021).*

Al igual que sucede en Occidente, la literatura militar rusa muy a menudo usa estos términos indistintamente, creando una ambigüedad que incluso los expertos rusos cercanos a estos temas reconocen y con frecuencia buscan corregir. Como afirmó un artículo de 2019 publicado por la Academia Rusa de Ciencias Militares, "casi todos los autores" mantienen una definición separada para la guerra de información y la confrontación, y agregó que la guerra de información debería excluirse de documentos oficiales, ya que el término warfare connota conflicto armado, que está

ausente en el tipo de competencia digital en tiempos de paz a la que suelen hacer referencia los autores militares rusos. En 2016, El jefe del Estado Mayor, Valery Gerasimov, anunció que los militares incorporaron con éxito la "confrontación de información" en un ejercicio militar estratégico por primera vez (Cheravitch, 2021).

Como corolario de esta sucinta sinopsis de la evolución del concepto ruso de la "Confrontación de la Información", según Grisé (Michelle Grisé, 2022), "los expertos militares rusos identificaron dos subtipos principales de Confrontación de la Información: informativo-psicológico e informativo-técnico".

> El primero incluye esfuerzos para influir en la población y las fuerzas militares del enemigo, incluso engañándolo, socavando su voluntad de resistir, produciendo pánico en sus filas y generando traición. Puede ser tanto ofensiva como defensiva y está dirigida a los pensamientos del enemigo y a la defensa de los propios pensamientos del mismo efecto del enemigo. El personal militar no solo participa activamente en la confrontación de información, sino que son ellos mismos un objeto de continua influencia informativa-psicológica Ofrece una forma de "controlar la mente del enemigo", ya sea directa o indirectamente, mediante la introducción de información específica, sobre la base de la cual [el adversario] toma una decisión.

> El subtipo informativo-técnico por otro lado, implica la manipulación física de redes y herramientas de información, incluida la "destrucción de información, redes radioelectrónicas, e informáticas, y obtener acceso no autorizado a los recursos de información del enemigo". La confrontación informativo-técnica busca influir en las redes de comunicación y las redes de información utilizadas por las organizaciones gubernamentales en el desempeño de sus funciones de gestión, la infraestructura de información militar, "las estructuras de información y gestión de las empresas industriales y de transporte, y los medios de comunicación. Consiste en ejercer un impacto técnico-software en los recursos de información del adversario y endurecer los propios recursos de información para evitar tal impacto.

Ello se concreta mediante la desinformación (*deziformatsiya*) diseñada para engañar y desorientar al oponente, influir en sus decisiones y socavar su eficiencia política, económica y militar, la combinación (*kombinatsiya*) con operaciones cibernéticas complejas que integran varios objetivos e instrumentos (Milosevich-Juaristi, 2017) y el engaño (*maskirovka*).

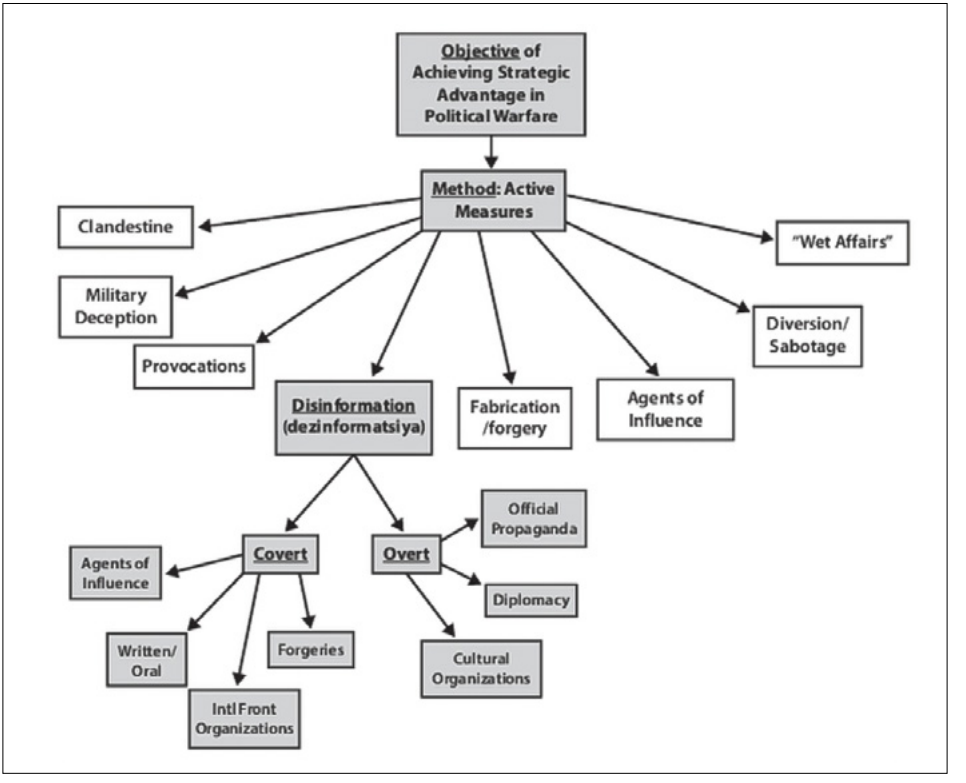
Con respecto a la desinformación Milosevich-Juaristi explica (Milosevich-Juaristi, 2017):

> Los instrumentos principales de todo tipo de desinformación rusa son los medios de comunicación convencionales como Sputnik (agencia estatal de noti-

cas), televisiones nacionales, RT (televisión internacional, antigua Russia Today), el periódico Russia Beyond the Headlines (que se publica en español para los países hispanohablantes), los ataques cibernéticos y los Internet trolls, personas que publican noticias falsas y ofensivas en las redes sociales (Facebook, Twitter o páginas web fantasma). Las características comunes de los mensajes de la desinformación son la dificultad de averiguar la exactitud de los hechos que tratan, la falta de equilibrio en la presentación de la información (se insiste más en las debilidades del oponente que en la información de los hechos) y la ausencia de credibilidad de las fuentes elegidas (se introducen con un "muchos dicen" o "se habla de", o se inventa un acontecimiento falso como el caso de una niña rusa supuestamente violada por dos refugiados en Alemania).

En la siguiente ilustración pueden verse el rol que desempeña la desinformación como parte de las medidas activas que emplea la Federación de Rusia para obtener una ventaja política.

ILUSTRACIÓN 51 . **Desinformation**



FUENTE: *(MEDIA AJIR, 2018)*

La desinformación puede entenderse como información falsa, engañosa o que distrae y que se difunde deliberadamente. Para ser eficaz, no debe ser atribuible a un gobierno. Es distinta de la propaganda, cuyo propósito es persuadir, y también de la desinformación, que es información falsa o engañosa que un gobierno produce oficial y abiertamente. Cuando un gobierno planta secretamente una historia falsa en un periódico y disfraza la autoría, eso es desinformación. Cuando proporciona públicamente "hechos alternativos" engañosos, eso es información errónea. En el caso de Rusia, lo que pretende es influir en un resultado específico y crear una amplia atmósfera de desconfianza (Walton, 2022).

Con la aparición del espacio cibernético, varias estrategias históricas rusas debieron adaptarse a él, especialmente la doctrina militar de la era soviética de *Maskirovka* (típicamente traducida como camuflaje o engaño) que está estrechamente alineada con el empleo de los servicios de inteligencia soviéticos de "medidas activas"[109] para coaccionar y subvertir durante la Guerra Fría, además de la estrategia militar soviética de "control reflexivo". El Control Reflexivo forma un componente crítico de la guerra de información rusa (Ainsworth, 2020).

En línea con Ainsworth, Jānis Bērziņš explica que la estrategia rusa de conducir la guerra considera una serie de elementos el último de los cuales es el Control Reflexivo, teoría desarrollada a partir de la investigación en psicología y cibernética, cuando el Ministerio de Defensa soviético trató de incorporar las técnicas de investigación operacional en la toma de decisiones. Al representar las partes cómo el sistema de un adversario, enmarcaba los problemas y procesaba la información, los planificadores rusos podían diseñar operaciones para cambiar las decisiones de ese adversario en una dirección favorable para ellos (Bērziņš, 2018).

Para Thomas la llamada Teoría de Control Reflexivo (RCT por sus siglas en inglés), una versión refinada de *Maskirovska* (engaño militar ruso), se refiere a una estratagema de guerra soviética que busca manipular y utilizar la mente del adversario con el fin de crear o exponer vulnerabilidades. Es un medio para interferir y manipular el ciclo de toma de decisiones de un oponente (Thomas, 2004). Luego lo define como "un medio de transmitir a una oponente información especialmente preparada para inclinarlo voluntariamente a tomar voluntariamente la decisión predeterminada deseada por el iniciador de la acción".

Para Juan Martínez Pontijas, más allá de la percepción simplista de que el control reflexivo (CR) es únicamente una técnica de desinformación, del análisis efectuado se concluye que el concepto abarca todo el conjunto de acciones enfocadas a predeterminar la decisión de un adversario en beneficio propio, mediante la modificación de aspectos claves de la percepción que dicho adversario tiene del mundo que le rodea. Define el control reflexivo como:

109 Otras "medidas activas" son la propaganda, la provocación, la manipulación de los medios de comunicación extranjeros, la infiltración de agentes y las operaciones paramilitares encubiertas.

> Un proceso por el que un enemigo transmite las razones o bases para la toma de decisiones a otro". Cuando un sistema alcanza el control reflexivo sobre otro adversario, puede influir en la forma que éste último percibe la situación, en sus planes y en la forma que actuará.
>
> Un ejemplo paradigmático de aplicación eficaz del CR, en el nivel estratégico y operacional, lo constituyen los frecuentes incidentes que ocurren entre aeronaves rusas y plataformas navales o aéreas de países de la OTAN o afines a la alianza atlántica. Cuando tienen lugar, Rusia se ofrece para negociar nuevos acuerdos para regular dichos incidentes. Se crea así la imagen de que las operaciones de la Alianza en, por ejemplo, el Báltico son provocativas y potencialmente peligrosas para la estabilidad de la región. Los dirigentes occidentales, preocupados por la posibilidad de un aumento de las tensiones entre bloques, reciben dicho ofrecimiento de forma favorable cuando ya existe una regulación internacional al respecto. Las naciones aliadas se encuentran, así, ante dos opciones. Ambas son favorables a los intereses rusos ya que, si se accede al dialogo, se entablarán unas conversaciones susceptibles de alterar el marco legislativo actual en favor del Kremlin y, si se rechaza, ello alimentará la narrativa de que las naciones de la OTAN mantienen una postura agresiva e intransigente frente a Rusia (Martínez Pontijas, 2020).

Otro ejemplo del empleo de las técnicas de control reflexivo son las amenazas rusas del uso de armas nucleares en el conflicto actual en Ucrania. Distintos analistas son de la idea que ello, si bien es posible para el caso de armas de carácter táctico, es improbable debido a las consecuencias negativas que podría acarrear tal decisión.

Para Paul Niland la idea es atemorizar (Niland, 2022):

> El escenario menos probable es el de un Armagedón nuclear que destruya el planeta, aunque algunos que han caído presa del control narrativo ruso están genuinamente aterrorizados por este resultado. Al hacer vibrar constantemente el sable nuclear, lo que Vladimir Putin está tratando de lograr se llama control reflexivo. La idea misma de un holocausto nuclear global es suficiente, en sí misma, para provocar temores de este resultado y, con ello, pide a Ucrania que se comprometa con Rusia.

Para Alberque, "la orden de alerta máxima de Putin tenía la intención de sembrar el miedo en Occidente, alentando a los analistas y tomadores de decisiones a centrarse en la creciente amenaza nuclear en lugar de ayudar a Ucrania. Este método de dar forma al pensamiento del adversario se conoce como "control reflexivo" (Alberque, 2022).

Por su parte, Mikhail Klimentyev, luego de analizar que de los tres elementos necesarios que debe poseer la disuasión nuclear que son capacidad, comunicación y credibilidad, Rusia posee los dos primeros, es de la opinión que "la cuestión de la credibilidad sigue abierta, dependiendo de las percepciones de los demás. En pocas

palabras, Estados Unidos y otros estados nucleares deben creer que Rusia usará armas nucleares bajo un cierto conjunto de condiciones, generalmente en represalia por un ataque similar o cuando enfrenta una amenaza para su supervivencia".

ILUSTRACIÓN 52 . **Armas nucleares de China**

FUENTE:*(IISS, 2022)*

Es por tal motivo que tiene mucho más que ver con sus intentos de intimidar y lograr un control reflexivo sobre Occidente. En otras palabras, está tratando de lograr que Estados Unidos y otros miembros de la OTAN teman tanto la perspectiva de una guerra nuclear que accedan a las demandas rusas. Eso lo convierte en una estrategia coercitiva, pero crucialmente una que se basa en nunca ser probada (Klimentyev, 2022) pero que, sin embargo, pareciera ser eficaz pues:

- En abril de 2022, el canciller alemán, Olaf Scholz, basó su decisión de no suministrar armas pesadas a Ucrania con la justificación de que "no debe haber una guerra nuclear".

- Varios comentaristas occidentales también han comenzado a reconsiderar el "tabú nuclear", preocupados de que Putin pueda recurrir a las armas nucleares en Ucrania si se siente arrinconado o para cambiar el rumbo de la guerra. Un artículo de opinión en el New York Times[110] pidió conversaciones inmediatas antes de que la guerra de las grandes potencias se volviera inevitable.

- El 28 de octubre, decenas de miles de checos se congregaron en el centro de Praga para exigir la dimisión del Gobierno, así como una política militar neutral que deje de apoyar a Ucrania y volver a negociar con Moscú la compra de gas natural (EFE, 2022).

El control reflexivo implica una amplia variedad de tácticas, como el engaño, la distracción, la disuasión y la provocación. Se han visto que estas tácticas se desarrollan en el creciente número de ataques cibernéticos contra los servidores del gobierno de Ucrania y la red de energía, hasta las campañas de desinformación patrocinadas por

110 Dicho artículo señalaba que: Si Rusia continúa avanzando hacia Ucrania, los socios occidentales probablemente proporcionarían aún más y mejores armas. Si esas armas permiten a Ucrania revertir las ganancias de Rusia, Moscú puede sentirse obligado a duplicar, y si realmente está perdiendo, bien podría considerar ataques directos contra la OTAN. En otras palabras, no hay un resultado mutuamente aceptable en este momento. Pero las conversaciones podrían ayudar a identificar los compromisos necesarios para encontrar uno.

el estado ruso destinadas a sembrar la desconfianza y la discordia en el país. Últimamente se está asistiendo a la amenaza del empleo de armas nucleares y a la posible destrucción de satélites occidentales que se utilizan para ayudar al esfuerzo de guerra de Ucrania que, aunque no se mencionó a compañías o individuos específicos, la aparente amenaza puede estar dirigida a Elon Musk, dado que a principios de este mes el multimillonario prometió que su compañía de cohetes SpaceX continuaría financiando su servicio de Internet Starlink en el país.

Para Aleksandr Dugin[111] "Estados Unidos ha sido capaz de crear una gigantesca red de intelectuales, académicos, instituciones, organizaciones y personalidades con la intención de difundir su narrativa en apoyo del orden mundial que surgió del final de la Guerra Fría, o el unipolar" (Allegri, 2021) y "La posmodernidad muestra que toda supuesta verdad es una cuestión de creer. Así que creemos en lo que hacemos, creemos en lo que decimos. Y esa es la única manera de definir la verdad. Así que tenemos nuestra verdad rusa especial que debes aceptar" (Gatehouse, 2016). En la estrategia de influencia de Dugin, los actores deben formar un "grupo especial" compuesto por oficiales, miembros de los servicios secretos, intelectuales, científicos, politólogos, periodistas "con una orientación patriótica". Una "red euroasiática" opuesta a una "red atlantista" (Mielcarek, 2015).

Lo importante son las formas de transmitir estratégicamente información a las audiencias objetivo de manera que cambien sutilmente los motivos y la lógica de sus decisiones con el propósito final de que las personas hagan algo haciéndoles creer que es lo mejor para ellos, incluso si no lo es. Para ello se utilizan "agentes de influencia" que siembran desinformación, desacreditan puntos de vista alternativos o simplemente causan confusión. Para multiplicar el poder de difusión, se suelen usar granjas de *trolls* que son grupos de hackers que emplean *bots*, es decir, programas que automatizan estas transmisiones de mensajes. Las granjas de *bots* a veces tienen varios miles de usuarios ficticios en las redes sociales. Las fábricas de *trolls* dan legitimidad a sus noticias falsas invitando a los medios de comunicación o a personalidades conocidas a ampliar su difusión.

Otros se presentan como agregadores de noticias inocentes, proporcionando "alertas de noticias de última hora" a acontecimientos en todo el mundo o en ciudades específicas. Este último grupo es una herramienta clave para trasladar la desinformación de los círculos principalmente influenciados por Rusia a la población general de las redes sociales (Weiburg, Watts, & Berger, 2016).

Desde 2014, Rusia ha llevado a cabo campañas de manipulación de redes sociales en al menos 70 países en siete idiomas en 300 plataformas y foros web, lo que marca un aumento continuo de la sofisticación y la intensidad. Las tácticas incluyen ocultar, disfrazar, cooptar, penetrar y manipular. La difusión de teorías de cons-

111 Especialista en operaciones psicológicas es autor de una veintena de libros que consideran todo el espectro de influencia: relaciones públicas, geopolítica, psicología, informática. Su hija fue asesinada en un atentado en Moscú, por una bomba adherida a su auto en agosto de 2022.

piración confunde el ambiente de la información y socava la confianza pública en la naturaleza de la verdad. Los representantes locales ayudan a Rusia a explotar las tensiones sociales y ofuscar los orígenes de su desinformación y también obstaculiza la regulación al plantear preocupaciones sobre la libertad de expresión. El Kremlin se basa principalmente en las plataformas de redes sociales occidentales (Edward Lucas, 2021).

ILUSTRACIÓN 53 . **Actividad rusa, abierta o encubierta en los medios**

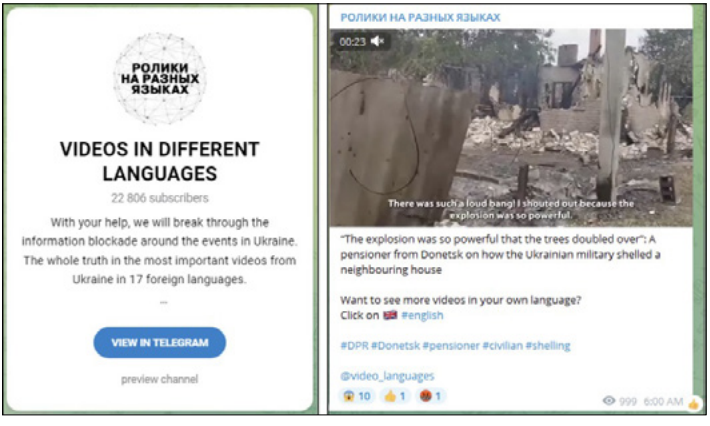
FUENTE: *(WEIBURG, WATTS, & BERGER, 2016)*

En los últimos días de octubre de 2022 Rusia denunció que Ucrania estaría evaluando el uso de una "bomba sucia" para luego responsabilizar a las tropas invasoras. Esas acusaciones fueron realizadas por Putin, altos funcionarios del Kremlin, el Ejército, y luego amplificadas por los principales medios que están bajo la órbita del Estado, como Russia Today (RT) y Sputnik, entre otros (Infobae, 2022).

Expertos de Nisos -una firma de inteligencia con sede en Estados Unidos que monitorea la desinformación y otras amenazas digitales- indicaron en un informe elaborado recientemente que cuentas vinculadas con la prensa estatal rusa emplearon el nuevo método para promover decenas de videos en 18 idiomas. El objetivo es esparcir el discurso oficial en el nivel global. Parte de esta campaña consiste en subir videos de propaganda a Telegram muchos de los cuales presentan entrevistas con civiles que expresan su gratitud a las fuerzas armadas rusas o lamentan las presuntas atrocidades ucranianas (NISOS, 2022):

En total, 275 usuarios de Twitter publicaron los videos RT con el identificador de @video_languages Telegram, pero centramos nuestra investigación en un núcleo de 123 cuentas con una sintaxis de publicación idéntica. Alrededor de una cuarta parte de estas cuentas exhiben un comportamiento similar al de un bot y la mayoría evita usar un rostro humano para una foto de perfil. Una cuenta programó hasta 16 tweets por día en intervalos de 15 minutos. Casi todas las cuentas están vinculadas a cuentas oficiales de ministerios, embajadas y / o los medios de comunicación de Rusia. Nisos descubrió que docenas de cuentas en esta red son los principales amplificadores de las cuentas de Twitter de varias embajadas rusas (particularmente Japón e Italia) y también de las ediciones en varios idiomas de RT (especialmente RT en español). Otro conjunto de cuentas aumenta el contenido de una cuenta pro-Kremlin que comparte contenido de guerra de un canal de propaganda de Telegram. En general, parece probable que la iniciativa de "lenguajes de video" aprovechó los activos existentes de Twitter que ya se estaban utilizando para amplificar el contenido prorruso.

ILUSTRACIÓN 54 . **La introducción del canal de Telegram videos en diferentes idiomas, además de una publicación de muestra en inglés**



FUENTE: *(NISOS, 2022)*

En 2020, el Almirante Faller, Jefe del Comando Sur, señalaba que los medios de comunicación rusos en español habían duplicado sus seguidores en las redes sociales de 7 millones a más de 18 millones. Según un informe de Insider de abril de 2022, RT en español y Sputnik Mundo acumulan el mayor número de seguidores en Latinoamérica que en otras partes del mundo como Europa o Estados Unidos. Por ejemplo, RT en Español tiene más de 3,5 millones de seguidores en Twitter y 18 millones en Facebook (Insider, 2022):

RT Online, la página en árabe de la cadena de televisión rusa en Facebook, experimentó un aumento del 187% en la participación durante el primer mes de la guerra, según Avaaz. Las cuentas de Sputnik en Brasil y Japón tuvieron repuntes menores. Un análisis similar realizado por Zignal Labs, una empresa que ras-

> trea la actividad en redes sociales, mostró un aumento en los enlaces compartidos de las publicaciones de RT y de las noticias de Sputnik en español. RT en Español, Sputnik Mundo y RT Play en Español han estado entre las 10 páginas más vistas en Facebook en América Latina, con decenas de millones de espectadores. En estos sitios, la guerra de Rusia se presenta falsamente como una causa justa contra un régimen fascista en Ucrania que buscaba armas nucleares y conspiraba con Estados Unidos para desarrollar armas biológicas a las puertas de Rusia. Las atrocidades bien documentadas en ciudades como Bucha son presentadas como exageraciones montadas para satanizar a Rusia.

Desde el comienzo de la guerra en Ucrania, la propaganda rusa comenzó a prosperar en español, árabe y otras lenguas. Un informe de la Fundación Bertelsmann del mes de junio indicó que el 42% del tráfico de la cadena española de RT correspondía a tres países que habían apoyado a Rusia o se habían mostrado neutrales en la guerra con Ucrania: la Argentina, Venezuela y México. "Parte del éxito de RT probablemente se deba no tanto a la promoción de la versión rusa de los acontecimientos, sino al cuestionamiento de la narrativa occidental", dijo Philip Kitzberger, politólogo de la Universidad Torcuato Di Tella. "Y eso encuentra cierta resonancia en ciertos grupos, vinculados en América Latina a una izquierda muy crítica con Estados Unidos (Steven Lee Myers y Sheera Frenkel, 2022).

Si bien en algunos casos, a las personas se les paga para construir y mantener perfiles falsos en las redes sociales, "lo que es realmente diferente en Rusia es la comprensión conceptual de una operación de información desde un punto de vista cultural, ideológico, histórico, científico y filosófico. Diferentes lógicas pueden ofrecer conclusiones totalmente diferentes sobre la intención, el propósito, la letalidad o la invasión de la soberanía de una operación de información; y esta lógica puede dar lugar a nuevos métodos para atacar objetivos de maneras totalmente no tradicionales y creativas" (Giles, Keir, 2016).

Paul y Posard señalan que existen evidencias de que las cuentas de Twitter vinculadas a Rusia enviaron más de mil tweets desde 3.800 cuentas que promovían un voto a favor del Brexit el día de la votación. Tales tuits parecían haber motivado a aquellos que eran pro-Brexit en Twitter a lo largo del tiempo, mientras que quienes se oponían reaccionaron solo unos días antes de las elecciones (Paul C. , 2020).

En el actual conflicto con Ucrania, Rusia también ha utilizado una serie de métodos, tanto abiertos como encubiertos: la desinformación, la generación deliberada o la amplificación de información falsa, han jugado un papel importante. Montó una actividad de engaño encubierta en forma de operaciones de "bandera falsa" destinadas a incriminar a Ucrania por ataques en el Donbass, creando un pretexto para la intervención (Aamer Madhani, 2022). Desde el punto de vista ruso, Rusia no está en guerra con Ucrania, está luchando contra un régimen títere fascista apoyado por Estados Unidos y la "operación militar especial" en Ucrania restaurará la estabilidad estratégica mundial.

Mucho antes de que los tanques rusos aparecieran en territorio ucraniano la propaganda del Kremlin comenzó a preparar el camino con la construcción de un relato que aún hoy intenta mantener en pie, a pesar de la incredulidad que ha generado en la propia Ucrania y en la mayor parte de la comunidad internacional. En él los militares rusos aparecen como defensores de Ucrania ante la "creciente rusofobia" y "nazificación" del país, mientras que la invasión no es el inicio de una contienda, sino una "operación militar especial" para finalizar el conflicto del Donbass.

Dmitry Feoktistov, embajador de la Federación de Rusia en la Argentina cuatro días después de la invasión, envió a LA NACION un artículo con la posición de su país respecto de la guerra. En él expresaba (Feoktistov, 2022):

- Las acciones de Rusia son legítimas:
  - > Rusia no lucha contra civiles;
  - > Contra las tropas rusas se utilizan bombas de fósforo;
  - > Kiev liberó criminales y distribuye armas sin control;
  - > La tarea de la operación es salvar a la población civil del Donbass.
- Rusia insiste en la desmilitarización y desnazificación de Ucrania:
  - > El proyecto de ley de pueblos originarios no otorga tal status a los rusos;
  - > Persecución de disidentes.
- Rusia se defiende ante la amenaza militar de la OTAN que utiliza el territorio de Ucrania contra Rusia:
  - > Entre mediados de enero y mediados de febrero Ucrania recibió 2000 Tns. de armas de la OTAN;
  - > Zelenski comenzó a amenazar abiertamente a Rusia con el uso de la fuerza y la adquisición del potencial nuclear.

Según un informe de amenazas adversas publicado por Meta (la empresa matriz de Facebook), esta aumentó en la fase inicial del conflicto (Nimmo, Ben, 2022):

> Estas operaciones parecen haberse intensificado poco antes de la invasión rusa. Por ejemplo, detectamos e interrumpimos la actividad reincidente del CIB vinculada a la KGB bielorrusa que de repente comenzó a publicar en polaco e inglés sobre las tropas ucranianas que se rindieron sin luchar y los líderes de la nación que huyeron del país el 24 de febrero, el día en que Rusia comenzó la guerra. Antes de eso, este actor de amenaza en particular se centró principalmente en acusar a Polonia de maltratar a los migrantes de Oriente Medio. El 14 de marzo, crearon un evento en Varsovia llamando a una protesta contra el gobierno polaco.

En un informe que la firma de ciberseguridad *Recorded Future,* desde al menos principios de mayo de 2022, "las redes de influencia rusas, incluidos los medios controlados por el estado, los conocidos medios de inteligencia encubiertos y los conocidos amplificadores de propaganda y desinformación, casi con certeza han estado lle-

vando a cabo varias operaciones de información multifacéticas para socavar y dividir a la coalición occidental sobre Ucrania e influir favorablemente en la opinión pública de manera favorable hacia Rusia" (Insikt Group, 2022):

> Hemos identificado múltiples narrativas de influencia que intentan socavar y dividir indirectamente a la coalición occidental, incluyendo: agitar el descontento interno hacia los líderes políticos occidentales; mostrar de manera negativa a los refugiados ucranianos y los impactos que tienen en sus países de recibimiento; culpar a los gobiernos occidentales de sus políticas negativas hacia Rusia de sus preocupaciones económicas, energéticas y de seguridad alimentaria; culpar a Ucrania como la fuente de los movimientos fascistas modernos; e incitar a la desconfianza en los medios de comunicación occidentales.

Una nota analítica no verificada del Quinto Servicio del Servicio Federal de Seguridad de Rusia (FSB), supuestamente interceptada y publicada por el Servicio de Seguridad de Ucrania (SBU) el 5 de junio de 2022, pero que para *Recorded Future* es auténtica, discute los fracasos de las operaciones de información rusas durante la guerra de contra Ucrania hasta el momento de redactar el informe, y proporciona recomendaciones para los esfuerzos de influencia en el futuro.

Dicho documento aconseja dirigirse a la "Comunidad Europea" con información sobre el deterioro de los niveles de vida como resultado de su apoyo a Ucrania, proponiendo narrativas específicas como armar a Ucrania a expensas de los contribuyentes europeos, enfatizar las dificultades económicas, pronósticos sobre el número de refugiados ucranianos y la carga creada sobre el presupuesto y la infraestructura socioeconómica. La nota analítica afirma que la intención de la operación de información *masiva* es provocar presión pública interna sobre los gobiernos y las élites políticas de los países occidentales.

La nota propone cinco *argumentos* específicos, en otras palabras, narrativas de influencia, para apoyar las acciones apuntadas anteriormente. Estos son:

- Armar a Ucrania a expensas de los contribuyentes europeos y, al mismo tiempo, cerrar algunos programas sociales dentro de la UE, aumenta la proporción de pobres en varios países;
- Previsiones sobre el número de refugiados ucranianos y la carga creada sobre el presupuesto y la infraestructura socioeconómica de la UE, donde ya hay muchos refugiados de Oriente Medio y Afganistán:
- Dificultades de la población debido a problemas con el transporte de energía;
- La falta de protección del capital de cualquier estado y persona ubicada en el sistema financiero y bancario occidental;
- Actualizar la información sobre los neonazis en Europa, hacer una comparación con Ucrania para mostrar a la comunidad europea cómo nace el nazismo y preguntar por qué prohíben a los nazis en sus países, pero los apoyan en Ucrania. Para estos fines, es aconsejable utilizar documentales de la BBC sobre

neonazis y nazis (por ejemplo, 'Nazis: cómo los marginales políticos se convirtieron en el partido gobernante', 'El Holocausto: historias no contadas de sobrevivientes', etc.).

ILUSTRACIÓN 55 . **El invierno será grande, sólo anochecer y nieve. Las apocalípticas imágenes muestran a Berlín, París, Londres y las instituciones europeas cubiertas de nieve blanca y niebla helada**

FUENTE: *(INFOBAE, 2022)*

A medida que se acerca el invierno, Rusia está librando renovadas operaciones de influencia en Europa diseñadas para socavar el apoyo occidental a Ucrania en un intento de cambiar el rumbo de una guerra. El esfuerzo incluye una campaña concertada a través de canales en idioma ruso o respaldados por Rusia en Europa, así como influir en los políticos simpatizantes como parte de una estrategia múltiple del Kremlin para utilizar la crisis del aumento de los precios de la energía antes del invierno para tratar de romper la unidad que hasta ahora ha permitido una avalancha de ayuda militar y económica occidental a Ucrania (Detsch, 2022).

Andrew Korybko (Korybko, Andrew, 2022)[112], en un artículo publicado en el portal *The AltWorld,* escribía que "el bombardeo del viernes 29 de julio por la mañana de un centro de detención en Donbass mató al menos a 50 personas e hirió a unas 75. Rusia y la República Popular de Donetsk (RPD) acusaron a Kiev de llevar a cabo este crimen de guerra contra sus propios soldados encarcelados que estaban detenidos allí, mientras que la ex República Soviética alegó ridículamente que sus oponentes se bombardearon a sí mismos. Objetivamente hablando, la inter-

ILUSTRACIÓN 56 . **Medios de Comunicación**

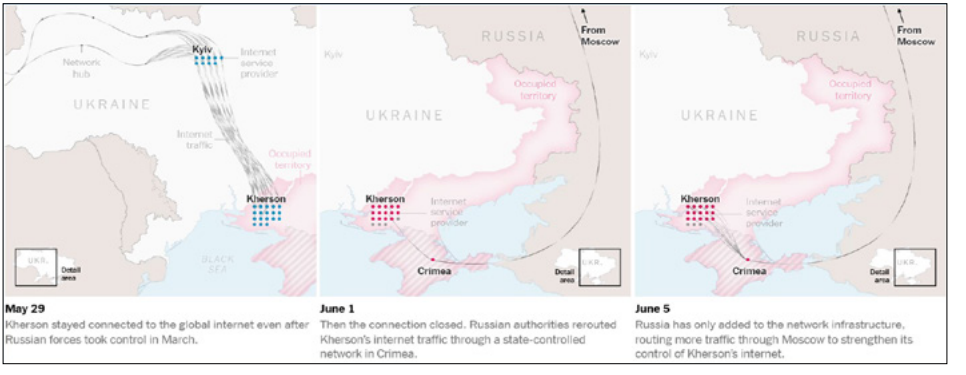
FUENTE: *(RT, 2022)*

pretación del incidente del primer mencionado es mucho más realista que la del segundo" (Korybko, Andrew, 2022):

> Para explicarlo, hay una cierta lógica inherente a que Kiev use el sistema HIMARS suministrado por Estados Unidos para matar a sus soldados encarcelados, incluidos los que fueron capturados durante la rendición de Azovstal, para que no derramen los frijoles[113] sobre sus crímenes de guerra. Quiere silenciar a sus militantes a toda costa para que no proporcionen pruebas que puedan usarse contra Kiev en el tribunal de justicia o al menos dar a Moscú una llamada victoria propagandística. Como dicen, los hombres muertos no cuentan cuentos.

En lo que respecta a las acciones cibernéticas, varias semanas después de tomar el control de la ciudad portuaria de Jherson, en el sur de Ucrania, los militares rusos obligaron a los proveedores locales de servicios de Internet a entregarles el control de sus redes, luego de lo cual desviaron los datos móviles y de Internet a través de las redes rusas, bloquearon el acceso a Facebook, Instagram y Twitter, así como a sitios web de noticias ucranianos y otras fuentes de información independientes y cerraron las redes de celulares ucranianas, obligando a los residentes a usar proveedores de servicios móviles rusos en su lugar (Satariano, 2022).

ILUSTRACIÓN 57 . **Cómo Rusia se apoderó de Internet de Ucrania en los territorios ocupados**



FUENTE: FACEBOOK (GLEICHER, ET AL., 2021)

112 Andrew Korybko es un analista político estadounidense con sede en Moscú, periodista y colaborador habitual de varias revistas online, así como miembro del consejo de expertos del Instituto de Estudios Estratégicos y Predicciones de la Universidad de la Amistad Popular de Rusia. Ha publicado varios trabajos en el campo de las guerras híbridas, incluyendo Guerras Híbridas. Revoluciones de Colores y Guerra No Convencional cuya edición en Argentina fue prologada por Juan Grabois.

113 La frase "derramar los frijoles" en inglés *"spill the beans"* significa revelar información que estaba destinada a mantenerse privada.

Rusia también separó a los ucranianos en Melitopol y Mariupol ocupados por Rusia del resto del país, limitando el acceso a las noticias sobre la guerra y la comunicación En algunos territorios, Internet y las redes celulares se han cerrado por completo.

Como puede verse, la Federación de Rusia, a través de una combinación de propaganda, noticias falsas y del control de la opinión pública a través de una ley de represión de "informaciones falsas", con el objetivo de hacer frente a una "guerra de información sin precedentes" que, considera, se está librando contra ella y que "provocó que varios medios internacionales -como la cadena pública británica BBC, las estadounidenses CNN y Bloomberg y la canadiense CBC- anunciaran la suspensión temporal del trabajo de todos sus periodistas en Rusia" (PILAR, 2022), creó una narrativa para justificar la invasión de Ucrania, la que fue cambiando con los avances del conflicto.

En cuanto a otras regiones, para Korybko, la última fase de la transición sistémica global a la multipolaridad, provocada por el Conflicto de Ucrania, envalentona a las masas a rechazar la hegemonía de la Gran Potencia que como nunca antes sienten su debilidad. Rusia no tiene nada que ver con el proceso que ha estado en marcha durante años por el cual las masas latinoamericanas han luchado constantemente contra el yugo de la hegemonía estadounidense desde la independencia de sus países hace dos siglos (Korybko A. , 2022).

> Los medios de comunicación rusos como RT y Sputnik, están informando activamente sobre sus respectivas luchas y mostrando a todos que no están solos, sino que cada uno está desempeñando su propio papel en sus regiones de origen en la búsqueda del objetivo colectivo de liberar al mundo entero a través de la Revolución Global que una vez más está en alza a medida que

> Ya sea el contenido en inglés, español o en cualquier idioma que produzca, los medios rusos han desempeñado el papel de articular la visión multipolar de las masas globales, lo que a su vez aclara el objetivo final de su lucha y educa a su público para que se involucre aún más activamente en la Revolución Global. Ninguna censura puede cambiar estos hechos. Por el contrario, cuanto más intenta Estados Unidos cerrar los medios de comunicación rusos, más envalentona a su audiencia internacional para hacer retroceder aún más ferozmente su hegemonía, ya que todos sienten cuán en declive, asustado y débil se ha vuelto dicho país.

El uso extensivo de Internet por parte de Rusia para difundir desinformación demuestra que su otra prioridad en el ciberespacio es apuntar a los corazones y las mentes de las audiencias nacionales e internacionales. (Nadiya Kostyuk, 2022).

Habrá que esperar los resultados del conflicto para saber cuán efectiva es la Guerra de Información rusa *(informatsionnaya voyna)* cuyas campañas de desinformación explotan la desunión social causada por la continua alza de los precios del petróleo, las

interrupciones del suministro de alimentos de Ucrania, y los aumentos resultantes de la inflación en los países occidentales, frente a la Comunicación Estratégica *(StratCom)* occidental de mistificar al presidente Volodimir Zelensky y el coraje y valor del pueblo ucraniano y rechazando el "nuevo orden" que trata de imponer la Rusia "imperialista" con la guerra de Ucrania.

3. **La República Popular de China y las "tres guerras"**

Para Vilmer, China ha habido en una "rusificación" de las operaciones de influencia china desde aproximadamente 2017: el paralelo se vio en 2018 durante las elecciones municipales taiwanesas, y más tarde durante la crisis de Hong Kong de 2019; pero el mundo solo tomó conciencia del problema en 2020 con la pandemia de Covid-19. Sin embargo, obviamente persisten diferencias entre los dos, y también hay un cierto grado de cooperación (Vilmer, 2021).

Antes de 2020, las operaciones de China eran más sutiles, pacientes y reacias al riesgo que las de Rusia, a pesar de que el presidente chino, Xi Jinping, aportó un enfoque más agresivo a la política exterior china. El PCCh comenzó a difundir desinformación en las redes sociales fuera de China continental ya en 2017, pero esto se centró en las élites, construyendo una imagen positiva de China y creando una narrativa consistente. Las campañas de influencia global incluyeron la promoción de contenido favorable a través de los medios de comunicación estatales y el cultivo o la compra de medios extranjeros como representantes (Edward Lucas, 2021).

> Antes de la pandemia, la desinformación china se centraba en temas candentes que afectaban a los reclamos centrales de legitimidad del PCCh: Hong Kong, Taiwán, Xinjiang y el Tíbet. En 2018, China utilizó la desinformación para interferir en las elecciones legislativas de Taiwán, aparentemente beneficiando al partido de oposición pro-Beijing, el Kuomintang (KMT). Las embajadas y embajadores chinos comenzaron a abrir cuentas de redes sociales en plataformas occidentales en 2019 durante las protestas en Hong Kong, contra un proyecto de ley propuesto por el gobierno que habría permitido las extradiciones a China continental, una tendencia que continuó en 2021 (Cook, 2020).

El informe ante el Congreso de los EE.UU. el Departamento de Defensa estadounidense señala que China lleva a cabo operaciones de influencia, dirigidas a instituciones culturales, organizaciones de medios, empresas, académicos y comunidades políticas en los Estados Unidos, otros países e instituciones internacionales, para lograr resultados favorables a sus objetivos estratégicos (DoD, 2021).

- Busca condicionar a los establecimientos políticos y a la opinión pública nacionales, extranjeros y multilaterales para que acepten las narrativas de Beijing y eliminen los obstáculos que impiden el logro de los objetivos.
- Los líderes del Partido Comunista Chino (PCC) probablemente consideran que

las democracias abiertas, incluido Estados Unidos, son más susceptibles a las operaciones de influencia que otros tipos de gobiernos.
- El Ejército Popular de Liberación (EPL) ha enfatizado el desarrollo de su concepto de "Tres Guerras", compuesto por guerra psicológica, guerra de opinión pública y guerra legal, en su planificación operacional desde al menos 2003.
- Es probable que el EPL continúe desarrollando sus capacidades de influencia digital mediante la incorporación de avances en inteligencia artificial (IA) para mejorar la calidad y la negación de sus mensajes.

Desde la perspectiva de China, las operaciones de influencia son emprendidas por todos los países, y son otros países, especialmente los Estados Unidos, los que utilizan las redes sociales para interferir en los procesos políticos de países como Irán y en el Medio Oriente. Cualquier acción que el Ejército Popular de Liberación (PLA por sus siglas en inglés) tome para contrarrestar esta subversión percibida se considera "defensiva" y necesaria para proteger y defender a los militares y al Partido (Beauchamp-Mustafaga & Chase, 2019). Para los autores, el ejército chino:

> Se está posicionando como uno de los principales actores de las operaciones hostiles de influencia china en las redes sociales. Ya se ha informado que está utilizando subrepticiamente Facebook y otras plataformas para socavar el proceso democrático en países extranjeros, incluido Taiwán, y los acontecimientos recientes indican que Estados Unidos podría ser el siguiente.

Para Alex Lo, la propaganda estatal china es principalmente de naturaleza defensiva y tiene como objetivo impulsar los puntos de vista y narrativas preferidos del país sobre sí mismo. Las operaciones comparables de Rusia y los Estados Unidos son generalmente ofensivas, ya que apuntan al cambio de régimen, la deslegitimación política y la desestabilización social y económica en el país objetivo (Lo, 2022).

Sin embargo, un artículo publicado por la red Al Jazeera, basándose en un informe la firma estadounidense de ciberseguridad Mandiant del 26 de octubre, revela una campaña de influencia activa, denominada DRAGONBRIDGE, en línea pro-China tratando de desacreditar la democracia de los Estados Unidos y desalentar a los ciudadanos de votar en las próximas elecciones de mitad de período, según investigadores de ciberseguridad (AlJazeera, 2022):

> La campaña de influencia tiene como objetivo "sembrar la división tanto entre Estados Unidos y sus aliados como dentro del propio sistema político de Estados Unidos", incluso poniendo en duda la efectividad de la votación.
>
> Entre otras actividades, el grupo ha difundido un video en inglés que sugiere que votar no es "la solución a los males de Estados Unidos", los legisladores estadounidenses no son productivos y el proceso legislativo no tiene un efecto significativo en la vida de los estadounidenses.

La operación de influencia, que implica el uso de cuentas falsas de redes sociales, así como artículos de noticias plagiados y fabricados, también ha retratado a un grupo de hackers chinos como un actor respaldado por el gobierno de Estados Unidos y afirmó que Estados Unidos es responsable de las explosiones del gasoducto Nord Stream.

¿Cuál es la narrativa de China? ¿Cómo se narra y por qué? De hecho, para responder a la primera pregunta, debemos tener claro que la historia de China dentro de la República Popular China bajo Xi Jinping es una cosa; la historia tal como se cuenta al mundo exterior es otra, a pesar de que los dos están íntimamente conectados. A principios de 2013, Xi Jinping ordenó a los líderes del país, sus medios de comunicación y el público, y su servicio diplomático para "contar la historia de China" y hacerlo de manera proactiva. El eslogan *"China Dream"* fue el principal medio para hacer esto, un sueño que fue presentado como uno que todos dentro y fuera del país podrían compartir (Brown, 2020).

ILUSTRACIÓN 58 . **DRAGONBRIDGE cuentas que alegan que varias agencias del gobierno de los Estados Unidos «desarrollaron» o financiaron APT41[114]:**

FUENTE: *(MANDIANT INTELLIGENCE, 2022)*

El mensaje subliminal en esta insistencia del Sueño de China es que todos viven en un planeta, todos deben ser tolerantes con los valores de los demás, vivir y dejar vivir

114 Los miembros acusados de conformar APT41son todos antiguos o actuales empleados de Chengdu 404 Network Technology, una compañía de seguridad cibernética que realiza pruebas de intrusión para personas o empresas para comprobar la vulnerabilidad de sus ordenadores.

es la mejor filosofía, y si el mundo logra eso, entonces puede centrarse en lograr lo principal compartido: enriquecerse materialmente y mejorar. *Huawei, Tiktok, Wechat* son una prueba de la oposición estadounidense a la creación de un ciberespacio pacífico, seguro, abierto y cooperacional mediante una cooperación internacional activa y eficaz basada en los principios del respeto y la confianza mutuos, y al establecimiento de un sistema multilateral, democrático y transparente de gobernanza de Internet.

ILUSTRACIÓN 59 . **Comunicación y el Público**

FUENTE: *(CHINA.ORG.CN, 2013)*

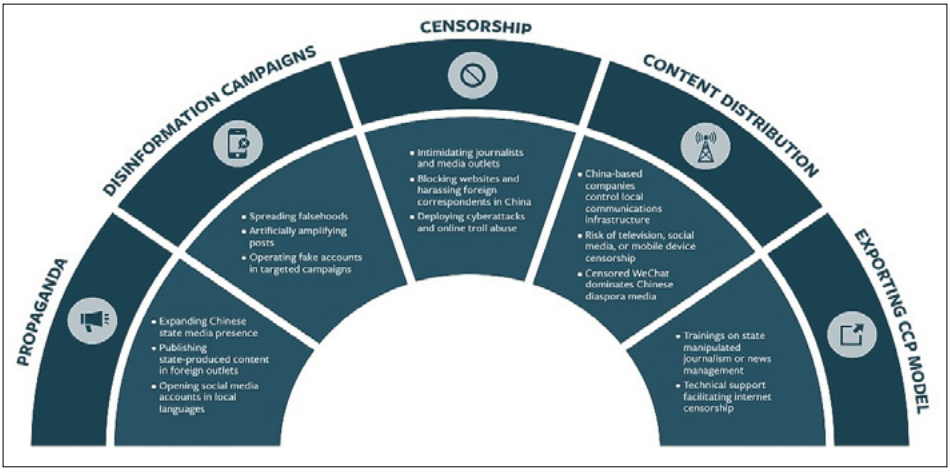
Según un informe de Freedom House[115], luego de la represión de las protestas a favor de la democracia en Hong Kong, el intento de encubrimiento del brote de COVID-19 por parte de funcionarios en Wuhan y la respuesta severa del gobierno chino a la pandemia, la contracción económica y la mala gestión relacionadas, y un incremento de denuncias creíbles sobre el trato brutal de las autoridades a las poblaciones de minorías étnicas en Xinjiang, los medios estatales, diplomáticos y otras entidades extranjeras de China tienen la tarea de abordar estos desafíos de reputación, expandir la influencia global de Beijing, garantizar la apertura a la inversión china y limitar cualquier discurso o acción internacional que se perciba como una amenaza para el control del PCCh sobre el poder (FreedomHouse, 2022).

> Sus esfuerzos incluyen tanto la promoción de narrativas preferidas (sobre China, su régimen o sus prioridades de política exterior) como intentos más agresivos de marginar, desacreditar o suprimir por completo cualquier voz anti-PCCh, comentarios políticos incisivos o exposiciones de los medios que presenten al gobierno chino y sus líderes bajo una luz negativa.

La RPCh lleva a cabo operaciones de influencia a escala global como parte de una gran estrategia que busca el *rejuvenecimiento* de China como una gran potencia y el EPL es un ejecutor clave. Las operaciones de influencia del EPL están comprendidas en la doctrina de *Tres Guerras*, vigente desde 2003, que incluye la de Opinión Pública, la Psicológica y la Legal.

115 Freedom House es una organización no gubernamental con sede en Washington D. C. y con oficinas en cerca de una docena de países. Conduce investigaciones y promociona la democracia, la libertad política y los derechos humanos. Desde 1972, mide el estado de los derechos políticos y libertades civiles en todos los países del mundo, incluyendo los 35 países de América, a través de su publicación anual *Freedom in the World*, así como el estado de la libertad de prensa a través de *Freedom of the Press*.

ILUSTRACIÓN 60 . **Tácticas utilizadas por el PCCh observadas en los 30 países estudiados de 2019 a 2021**



FUENTE: *(FREEDOMHOUSE, 2022).*

Si bien este enfoque domina su pensamiento estratégico actual, en 1999 los coroneles Qiao Lang y Wang Xiangsu ya hablaban del potencial de la estrategia de información como parte de una noción de una guerra que no respeta reglas ni límites (Liang, 1999).

Según Michael Clarke, los líderes y estrategas chinos analizaron el éxito de Estados Unidos durante la Primera Guerra del Golfo (1990 – 1991) y en Kosovo (1998 – 1999) no sólo desde el punto de vista del aprovechamiento eficiente de su superioridad tecnológica, sino también por su capacidad de "manipular" el derecho internacional y la opinión pública nacional e internacional en pos de sus objetivos políticos y estratégicos. En particular, desde la perspectiva china, observaron la capacidad de Estados Unidos para lograr un mandato de la Organización de las Naciones Unidas (ONU) para el uso de la fuerza durante la Primera Guerra del Golfo y su manipulación de la opinión pública occidental durante su intervención en Kosovo. La lección central para los estrategas militares chinos fue que *"las operaciones no militares y las capacidades no cinéticas"* eran fundamentales para luchar y ganar conflictos contemporáneos (Clarke M. , 2019).

Esas evaluaciones dieron lugar al desarrollo del concepto/estrategia de las "Tres Guerras", adoptado oficialmente por la Junta Militar Central (CMC) en noviembre de 2003. El mismo se basa en tres estrategias que se apoyan mutuamente: la manipulación de medios de manera abierta y encubierta; el uso coordinado de operaciones psicológicas estratégicas; y la guerra legal diseñada para manipular estrategias, políticas de defensa y percepciones de determinadas audiencias en el extranjero (Wibawa, 2019).

Al igual que se ha visto a lo largo de este capítulo, para los analistas occidentales existen diferentes definiciones para cada uno de estos tres tipos de guerra. En este caso se compararán las definiciones de Tasha Wibawa (analista australiana), del Departamento de Defensa de los Estados Unidos de América de 2021 (United States DoD, 2020) y de dos investigadores franceses Charon y Jeangène Vilmer quienes emplean las indicadas en el Diccionario de Terminología Militar China de 2011 (Vilmer, 2021).

ILUSTRACIÓN 61 . **Diccionario de Terminología Militar China de 2011**

	Tasha Wibawa	Departamento de Defensa	Paul Charon
Guerra Psicológica	Es la aplicación de medidas diplomáticas y militares destinadas a alterar la voluntad de los adversarios que se oponen a los objetivos de política exterior de China.	Utilizar la propaganda, el engaño, las amenazas y la coerción para afectar la toma de decisiones del adversario, al tiempo que contrarresta las operaciones psicológicas del rival.	Utilizar la información y medios específicos para acciones de combate que afecten la psicología y el comportamiento del público objetivo.
Guerra de Opinión	Es la implementación de manipulaciones abiertas y encubiertas de los medios, como, por ejemplo, el uso de información distorsionada, extendida a través de los medios de comunicación, con el objeto de influir en la audiencia nacional e internacional respecto de la rectitud de conducta de la política exterior China	Difundir información para el consumo público para guiar e influir en la opinión pública y obtener el apoyo de las audiencias nacionales e internacionales.	Crear un ambiente de opinión pública favorable a la iniciativa política y la victoria militar [a través] del uso de diversos medios y recursos de información para luchar contra el enemigo". Los chinos también traducen la "guerra de la opinión pública" como "guerra de consenso"
Guerra Legal	También denominada *"lawfare"*[116] se refiere a la explotación de todas las normas internacionales para asegurarse que cumplan con los objetivos de China mientras se socava los objetivos de la política exterior de otros Estados a través de los foros internacionales	La utilización de las leyes internacionales y nacionales para obtener apoyo internacional, gestionar las repercusiones políticas e influir en el público objetivo.	Permite limitar la libertad de acción del otro y aumentar la suya propia, porque ofrece a China una base para afirmar la legitimidad de sus reclamos.

FUENTE: *(VILMER, 2021).*

Del análisis de la ilustración anterior puede deducirse que con su concepto de las "Tres Guerras" China pretende actuar sobre aquellos que intentan oponerse a sus objetivos de política exterior, preparando el campo de batalla a través de la guerra de opinión pública y la guerra legal que operan principalmente en el nivel estratégico, y la guerra psicológica que se implementa en el nivel operacional y táctico.

La guerra de la opinión pública implica tres escenarios: atacar a los individuos más importantes en el campo del oponente, usar situaciones específicas y publicitar la difícil posición militar del oponente. Tales operaciones deben proporcionar una oportunidad para exponer la sabiduría de sus propias acciones y ganar superioridad moral, para mostrar su propia superioridad militar con el fin de socavar la moral del oponente y contradecir su propaganda. El mantenimiento de la iniciativa es importante en la guerra de la opinión pública (Sugiura, 2022).

Para librar una guerra exitosa de la opinión pública, es necesario ser el primero en reaccionar, en multiplicar las fuentes que defienden la propia versión de los hechos, mientras que posiblemente oculte (pero no sistemáticamente) los vínculos que podrían fortalecer al poder político, con el fin de influir en las percepciones y comportamientos de las audiencias objetivo (Vilmer, 2021).

Las operaciones de desinformación buscan crear y difundir mensajes beneficiosos para el Partido Comunista Chino. Los medios de comunicación, especialmente las redes sociales, se utilizan para mantener a la propia gente mal informada y suprimir cualquier voz crítica sobre las acciones de Beijing, tanto en el país como en el extranjero.

ILUSTRACIÓN 62 . **Opinión Pública**

FUENTE: *(BLOGABISSL, 2018)*

116 A diferencia de los Estados Unidos, a quien le preocupa que los opositores, sobre todo los insurgentes, puedan emplear los medios legales para garantizar victorias que de otra manera no pueden obtener en el campo de batalla, para la República de China (PRC) y, en particular, para el Ejército de Liberación Popular (PLA), lawfare es un arma ofensiva capaz de incapacitar oponentes y tomar la iniciativa política en tiempo de guerra; Cheng Dean; Winning Without Fighting: Chinese Legal Warfare; Disponible en: https://www.heritage.org/asia/report/winning-without-fighting-chinese-legal-warfare#_ftnref3

China maneja el "ejército de 50 centavos"[117] que son trabajadores empleados por el gobierno que se capacitan específicamente y producen más de 450 millones de publicaciones al año, con su objetivo principal de hacer de Estados Unidos el blanco de las críticas y minimizar la existencia de Taiwán. Ayudan a difundir la desinformación y estimulan los mensajes que China quiere impulsar, ya sea distrayendo a los ciudadanos de China de los problemas dentro de su propio país o enfatizando las fallas en otros países (Klevering, 2022).

> También utiliza otra táctica interesante para crear su propaganda: robar cuentas reales de las personas y reutilizarlas. Por ejemplo, los agentes chinos han podido hackear y robar cuentas de Twitter. Una vez que una cuenta es robada, comenzará una lenta metamorfosis en una máquina de propaganda china. Comenzará a tuitear tweets pro chinos, cambiará su foto de perfil a algo más genérico y eliminará a todos los seguidores, esencialmente borrando cualquier recordatorio de a quién perteneció una vez. La cuenta ahora será simplemente una cuenta de trolls pro chinos, publicando mensajes pro chinos con la esperanza de radicalizar o convertir a otras personas hacia su causa.
>
> Muchas de estas cuentas se publicarán en inglés, aunque muchas cambian al chino. Los mensajes están dirigidos tanto a los estadounidenses que son simpatizantes chinos como a los chinos étnicos que viven fuera de China. Muchas cuentas como estas son administradas por bots, que crean contenido automáticamente y lo comparten. Algunas son "cuentas principales" o cuentas que crean contenido. Otras son "cuentas amplificadoras", o cuentas que simplemente comparten las publicaciones de las cuentas principales para que parezcan legítimas y difundirlas a un público más amplio.

Los pilares de la guerra (warfare) de la opinión pública china son (Affaires, 2022):

- Seguir la guía de arriba hacia abajo:
  La guerra de opinión pública debe apoyar los objetivos políticos, diplomáticos y militares nacionales. Sus acciones deben ser coherentes con la estrategia nacional más amplia establecida por los niveles superiores de liderazgo.
- Enfatizar la prevención:
  La guerra de la opinión pública siempre está en marcha. El lado que planta su mensaje primero disfruta de una ventaja significativa. De hecho, los análisis chinos enfatizan repetidamente que "el primero en sonar atrapa a la gente, el primero en entrar establece el dominio. Esencialmente, los chinos buscan definir los términos del debate y los parámetros de cobertura.

117 Es un "ejército" de trolls de Internet que difunden propaganda en línea y desinformación para el gobierno chino. El nombre "50 centavos" proviene de un rumor de que el gobierno pagó a cada miembro 50 centavos chinos por publicación positiva realizada.

- Ser flexible y adaptable:
  Los mensajes de guerra de opinión pública deben implementarse de manera flexible, incorporando cambios en contextos estratégicos, políticos y militares. Al mismo tiempo, diferentes mensajes deben adaptarse a diferentes audiencias en lugar de seguir un enfoque único para todos.
- Explotar todos los canales de difusión de la información:
  Para garantizar la máxima eficacia, se deben aprovechar todos los recursos disponibles, de modo que un mensaje determinado sea reiterado, reforzado por diferentes fuentes y diferentes versiones. Los escritos militares chinos invocan regularmente los ideales de combinar operaciones en tiempos de paz y guerra, integración civil-militar y unidad militar-local.

Con respecto a los mensajes sobre la guerra en Ucrania, según el Swiss Institute for Global Affaires, "es evidente que los medios estatales chinos (Global Times / Beijing Review / CGTN, etc.) han estado adoptando el lenguaje y las narrativas de los medios estatales rusos en los últimos meses". Estos son algunos ejemplos (Affaires, 2022):

- La representación de Ucrania y la OTAN como agresores y la idea de que la expansión de la OTAN es la culpable del conflicto ha sido impulsada por funcionarios rusos y medios estatales. El razonamiento anti-OTAN fue recogido por varios canales controlados por el estado chino por medio de narrativas, difundidas a través de las cuentas de Twitter de Global Times y Beijing Review.
- El argumento de "qué pasa" es un tema constante en los mensajes de los medios estatales chinos. Los tweets de una cuenta diplomática en Japón (Consulado General de Rusia en Niigata) y una cuenta de medios estatales chinos (China-Q&A) esencialmente cuestionan por qué las actividades de los Estados Unidos y la OTAN en la ex Yugoslavia, Afganistán, Irak, Siria y otros, no llaman la atención.
- Otro ejemplo es la adopción narrativa de la "desnazificación" en Ucrania. La captura de pantalla de la izquierda muestra al medio de comunicación estatal chino Frontline retuiteando la cobertura de los medios estatales rusos de los grupos neonazis ucranianos. Es interesante señalar que en la plataforma china de microblogging Weibo, el término "Batallón Azov" parece más popular que "nazis" y recibió impulso por una publicación del 3 de marzo por parte de la cuenta de la Liga de la Juventud Comunista, presentando al grupo como una organización nazi y vinculándolo con el Movimiento contra la Ley de Extradición en Hong Kong (2019-2020)
- La alineación narrativa entre los mensajes chinos y rusos también se puede observar en el lenguaje específico utilizado para describir lo que está sucediendo en Ucrania. Como es el caso dentro de Rusia para usar términos como "operación especial" u "operación militar especial" en lugar de "guerra" e "invasión", vemos que los funcionarios chinos y los medios estatales adoptan el mismo lenguaje.

ILUSTRACIÓN 63 . **Narrativa**

FUENTE: *(AFFAIRES, 2022)*

La guerra psicológica tiene como objetivo amenazar y desmoralizar al oponente y, en consecuencia, romper su voluntad de luchar. Los objetivos de las operaciones psicológicas no son solo las personas y la sociedad, sino también las estructuras gubernamentales y de mando del enemigo. El propósito de las acciones en este nivel es interrumpir su buen funcionamiento. Al igual que en el caso de la guerra mediática, los medios de comunicación, liderados principalmente por Internet, desempeñan un papel importante en las operaciones psicológicas. Sin embargo, la caja de herramientas es mucho más amplia e incluye maniobras y ejercicios militares, exhibiciones de equipos y armas, intimidación, provocaciones y actividades en zonas grises por debajo del umbral de la guerra (Behrendt, 2022).

Para Cantalapiedra, emplea presión diplomática, rumores, narrativas falsas y el acoso para expresar descontento, afirmar la hegemonía y transmitir amenazas. La economía y las inversiones de la RPCh se utilizan con un efecto particular: China amenaza con la venta de deuda norteamericana; presiona a las empresas estadounidenses que invierten en el mercado de China; emplea boicots; restringe las exportaciones críticas (minerales raros); restringe las importaciones; amenaza con prácticas depredadoras para expandir la participación de mercado, e invierte en ciertas instituciones (Cantalapiedra, 2022)

El PLA distingue cuatro tipos de guerra psicológica (Vilmer, 2021):

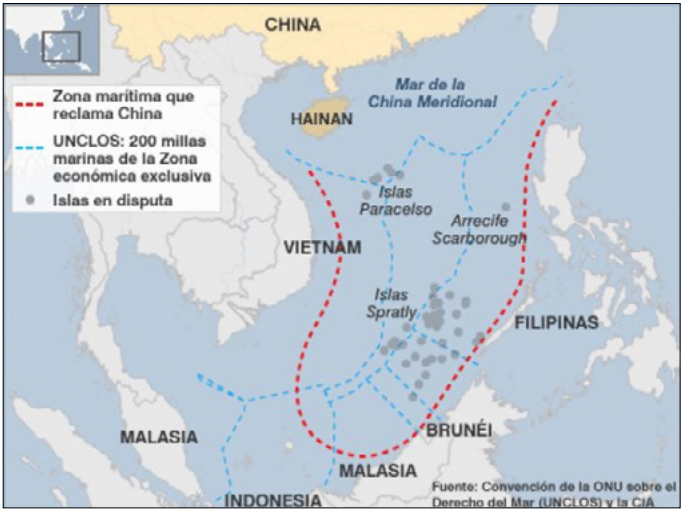
- coerción: obligar a un oponente a comportarse de cierta manera;
- mistificación: engañar al oponente para inducir un cambio en su percepción de la situación y, por lo tanto, en sus cálculos políticos y militares, y en consecuencia adoptar la actitud deseada por Beijing;
- división: sembrar la discordia en el campo del oponente. La ruptura de lazos y la destrucción de la confianza entre el gobierno y los gobernados, comandantes y subordinados. Este tipo de operaciones explota cualquier posible grieta entre los oponentes;
- defensa: prevenir las operaciones psicológicas llevadas a cabo por el enemigo, mantener y elevar la moral de las propias fuerzas y del pueblo. Los ofi-

ciales políticos desempeñan un papel clave en estas operaciones (como se describe más adelante).

El propósito de la guerra legal es crear la apariencia de legitimidad para las acciones de China, incluido el uso de la fuerza militar, mientras que al mismo tiempo retrata las acciones de la parte opuesta como ilegítimas, forzándola a la pasividad y bloqueando la intervención de cualquier tercer país. El objetivo principal de la guerra legal no es la victoria en los juicios ante tribunales internacionales. Los casos en sí mismos tienen la intención de retrasar y obstruir las acciones del enemigo y los juicios posteriores de criminales de guerra e individuos buscados para ayudar a dar forma a la realidad de la posguerra. Al final, una disputa legal está destinada a reforzar la estrategia militar, molestar al oponente y moldear la opinión pública en lugar de resolver el conflicto (Behrendt, 2022). Las operaciones de guerra mediática y legal se llevan a cabo durante el conflicto por los órganos políticos existentes del grupo en el nivel de ejército y superior (Sugiura, 2022).

Para mostrar cómo China lleva adelante la estrategia de las Tres Guerra se analizarán dos casos: el del Mar Meridional de China y Taiwán.

ILUSTRACIÓN 64 . **Espacio Marítimo reclamado por la RPCh**



FUENTE: CONVENCIÓN DE LA ONU SOBRE EL DERECHO DEL MAR (UNCLOS)

China controla hoy un espacio marítimo cinco veces mayor del que le correspondería de acuerdo con una lectura estricta de la Convención de las Naciones Unidas sobre Derecho del Mar (CONVEMAR) o la costumbre internacional. Un control logrado en muy pocos años, sin despertar una resistencia creíble por parte de los afectados (Elizondo, 2019).

Para Carpio, existe una campaña de propaganda, declarando al mundo que el Mar del Sur de China perteneció a China desde la antigüedad. En el documento de posición que presentó al Tribunal Arbitral de La Haya, China declaró: “Las actividades chinas en el Mar Meridional de China se remontan a hace más de 2.000 años. China fue el primer país en descubrir, nombrar, explorar y explotar los recursos de las islas del Mar

Meridional de China y el primero en ejercer continuamente poderes soberanos sobre ellas" (Carpio, 2021).

En lo que respecta a la Guerra Legal el argumento de China es que sus derechos soberanos sobre el Mar Meridional de China son anteriores a la Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR) de 1982:

> Sin embargo, el Tribunal dictaminó que todos los Estados que ratificaron la Convención de las Naciones Unidas sobre el Derecho del Mar habían acordado que todos los derechos históricos sobre los recursos marítimos más allá de lo que permite la Convención de las Naciones Unidas sobre el Derecho del Mar se extinguieron cuando la Convención sobre el Derecho del Mar entró en vigor.

La República Popular China inicialmente utilizó la guerra legal en el Mar Meridional de China apelando a los organismos legales internacionales para legitimar sus reclamos territoriales. Cuando esos organismos rechazaron las reclamaciones, la República Popular China calificó las resoluciones de ilegítimas y se negó a acatarlas. Para Martin, esto socava la legitimidad de estos organismos y disminuye la estabilidad en la región, ya que las naciones vecinas se vuelven más inciertas sobre el estado legal del Mar Meridional de China. Aunque los Estados Unidos no se han visto directamente afectados por las acciones de la República Popular China, están incurriendo en costos en forma de mayores operaciones de libertad de navegación (Martin M. , 2020):

> Las actividades de guerra psicológica de la República Popular China en el Mar Meridional de China tienen como objetivo principal disuadir a los países vecinos de invadir su territorio reclamado. Cuando los buques y aviones de las naciones vecinas llegan a las áreas en disputa, se han encontrado con una violenta resistencia china, incluidos buques que embisten a los barcos pesqueros vietnamitas, interrumpen las actividades de exploración petrolera de Malasia y acosan verbalmente a los pilotos militares filipinos por radio.
>
> Estas acciones pueden ser vistas como acciones de operaciones psicológicas (PsyActs) es decir, acciones realizadas para influir en los pensamientos y percepciones del público objetivo en la búsqueda de un fin; en este caso, la República Popular China reacciona violentamente a supuestas violaciones de su soberanía para crear la percepción entre sus vecinos de que el Mar Meridional de China es de hecho territorio chino legítimo.

Taiwán es el país más vulnerable del mundo a los ataques de desinformación y China es probablemente el principal culpable. Taiwán es un tema importante para Beijing no solo como "asuntos pendientes de la guerra civil" de la década de 1940. La isla es una amenaza para el poder del PCCh en la esfera ideológica. El éxito de la democracia de Taiwán contradice la tesis promovida por las autoridades de la República Popular

China de que las sociedades basadas en el confucianismo son incompatibles con la democracia liberal (Tzu-ti, 2019).

En el caso de Taiwán, la República de China, Behrendt señala que, invariablemente considerada por Beijing como una provincia rebelde durante más de siete décadas, también es un objetivo de las operaciones de 3W y como ejemplo, debido a la vastedad del tema expresa (Behrendt, 2022):

> La guerra legal tiene como objetivo privar a la República de China del reconocimiento diplomático, bloquear cualquiera de sus actividades en organizaciones internacionales y obtener una sanción legal para la posición de la República Popular China. Los medios de comunicación y la guerra psicológica están destinados a convencer a la opinión internacional de la legitimidad de las demandas chinas, para disuadir a los isleños de declarar la independencia - como Taiwán independiente de China continental - y convencer a los Estados Unidos sobre la inutilidad de intervenir en caso de una invasión.

> Las armas de guerra en este campo son, por ejemplo, las constantes violaciones de la Zona de Identificación de Defensa Aérea (ADIZ) de Taiwán por parte de la fuerza aérea china, ejercicios militares cuyos escenarios incluyen desembarcos en las islas, presión diplomática sobre países que reconocen a la República de China o incluso abrir oficinas de representación para Taipei bajo el nombre de Taiwán. El ejemplo más reciente de esto es el conflicto diplomático y económico en curso con Lituania.

Otro ejemplo de la guerra legal podría ser el caso de la queja, mediante una nota del agregado militar adjunto de la República Popular de China enviada a las autoridades de la Armada Argentina, reclamando el alquiler de un salón privado, por parte del Centro Naval, a la representación de Taiwán para la realización de una ceremonia llevada a cabo el pasado 5 de octubre (Izquierdo, 2022).

Para Izquierdo (2022).:

> Las presiones por temas políticos, económicos y hasta culturales del régimen conducido por Xi Jinping a los países de la región no son nuevas. Se enmarcan en la diplo-

ILUSTRACIÓN 65 . **Ejercicios Militares de China**

FUENTE: XINHUA, GLOBAL SECURITY.

macia de *Wolf Warrior*[118] que emprendió Beijing desde hace algunos años y que tienen como principal objetivo que los gobiernos se allanen a las exigencias diplomáticas tal como salen de la oficina del canciller Wang Yi, uno de los funcionarios más cercanos al jefe de la autocracia. Las notas de quejas, los llamados y las presiones son cada vez más habituales y no sólo se remiten a sedes gubernamentales sino también a redacciones periodísticas y empresas.

La guerra la opinión pública china tiene como objetivo influir en las opiniones y actitudes públicas para generar apoyo para las acciones políticas y militares y disuadir a un adversario de llevar a cabo acciones contrarias a sus intereses. Aprovecha todas las capacidades relacionadas con la información que informan o influyen en la opinión pública, incluyendo películas, programas de televisión, libros, Internet y la red global de medios. Los objetivos son preservar la moral, generar apoyo público en el país y en el extranjero, y debilitar la voluntad de un enemigo de luchar. Particularmente para audiencias externas, la propaganda del PCCh presenta a China como un país con una larga historia de "amistad con personas amantes de la paz en todo el mundo" y cuyos líderes son dignos de confianza (Cochran, 2020).

La guerra psicológica es de alguna manera la más amplia de las "Tres guerras". Implica la aplicación de información y medios especializados de acuerdo con un objetivo estratégico y en apoyo de objetivos políticos y militares. Tales esfuerzos están dirigidos a una variedad de audiencias potenciales y generalmente involucran misiones operacionals contra la psicología y las capacidades cognitivas de un oponente.

Como herramienta política y diplomática en los conflictos internacionales, los sistemas legales pueden usarse para ofrecer la justificación de las propias reclamaciones, decisiones y comportamientos en ciertas disputas político-militares. Mientras tanto, los sistemas legales también pueden movilizarse para controlar y socavar la libertad de acción del adversario al negar la legitimidad de sus reclamos, decisiones y comportamientos en tiempos de paz y guerra.

4. **Convergencias y diferencias**

Para Kilman, aunque es probable que persistan las diferencias clave en los enfoques chino y ruso, existe una creciente evidencia de que los dos países están aprendiendo uno de otro y mejorando su coordinación, lo que lleva a una creciente convergencia en sus esfuerzos de influencia digital (Daniel Kliman, 2020).

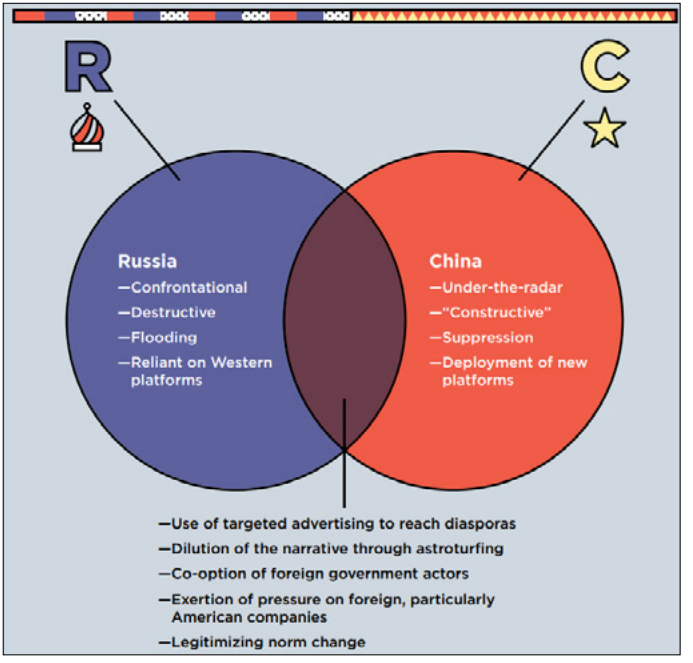
Como lo muestra la figura, las convergencias serían: Uso de publicidad dirigida para llegar a las diásporas; dilución de la narrativa a través del astroturfing;[119] cooptación de actores gubernamentales extranjeros; ejercer presión sobre empresas extranjeras, particularmente estadounidenses y legitimar el cambio de normas.

---

118 En los últimos años, las directivas del presidente Xi y la opinión pública china han establecido un tono diplomático más agresivo. Este estilo de diplomacia asertiva, apodado "lobo guerrero", lleva el nombre de una serie de películas patrióticas de 2017. En última instancia, los diplomáticos "lobos guerreros" buscan "defender los intereses nacionales de China, a menudo de manera confrontativa".

Considerando otros autores podría decirse que además:

ILUSTRACIÓN 66 . **Convergencias de las campañas de influencia digital chinas y rusas.**



FUENTE: *(DANIEL KLIMAN, 2020).*

a. Las campañas de China buscan proteger su propia imagen nacional, teniendo objetivos más enfocados, mientras que Rusia persigue la desestabilización de otros países (Miriam Matthews, 2021);

b. En 2020, la mitad de los informes de los medios estatales chinos en inglés fueron sobre China, mientras que solo el 5% de los informes de los medios estatales en inglés ruso se centraron en Rusia. A pesar de los cambios posteriores, estas estadísticas confirman que Rusia buscó fortalecerse en términos relativos debilitando a Occidente, mientras que China buscó fortalecerse en términos absolutos (Daniel Kliman, 2020).

c. Las operaciones de información chinas alcanzaron una posición de prominencia en 2020, los botnets aumentaron enormemente en escala y alcance, pero los ataques cibernéticos se centraron en el espionaje industrial en lugar de las elecciones. De casi ninguna presencia en Facebook en 2016, China ahora posee cinco de las seis

119 *Astroturfing* es un término referido a campañas de relaciones públicas en el ámbito de la propaganda electoral y los anuncios comerciales que pretenden dar una impresión de espontaneidad, como nacida de una fuerte relación con el entorno social. El nombre proviene de un doble juego de palabras en inglés, partiendo del concepto de *grassroots* (literalmente "raíz de hierba", figurativamente "de base"). Este concepto sirve para calificar a los movimientos «con base social», que surgen «de abajo», de la interacción de los miembros de una comunidad. Por otro lado, *AstroTurf* es una conocida marca estadounidense de césped artificial, cuyos productos están diseñados para parecer hierba natural. Así, *astroturfing* hace referencia a esa artificialidad, a esa falsa base social de ciertas campañas comerciales.

páginas de noticias más seguidas en la red social, aunque China no logró crear el tipo de contenido viral altamente dirigido que Rusia logra consistentemente (Omelas, 2020).

d. China confía, mientras que Rusia duda de su poder blando. China tiene sus propias fortalezas en los medios y el espacio de la información e insertó contenido en las principales publicaciones extranjeras, mientras que Rusia influyó en gran medida en el ambiente de la información a través de las redes sociales, los representantes marginales y sus propios medios de comunicación (Cook, Sarah, 2020).

e. Las operaciones de Información de Rusia son más confrontativas, mientras que las de China están más controladas. El Kremlin estuvo dispuesto a asumir las consecuencias de interferir en las elecciones y difundir desinformación mientras que China actúa con más cautela con la esperanza de que la construcción de influencia de una manera menos abierta y disruptiva le traerá beneficios futuros (Daniel Kliman, 2020).

f. Una parte clave de la declaración conjunta del mes de febrero de 2022 fue un llamado a la "internacionalización de la gobernanza de internet", con lo que Xi y Putin quieren decir que internet debería estar sujeta al control de estados soberanos. Esta posición está en desacuerdo con una Internet libre y abierta gobernada con la participación de los ciudadanos y la sociedad civil. Al unir fuerzas con Rusia para buscar una revisión de la gobernanza global de Internet, China busca legitimar sus restricciones internas sobre el discurso y las tecnologías que las respaldan y establecer lo que llama "soberanía cibernética". (Bandurski, 2022).

Para Kliman, Beijing y Moscú han invertido considerables recursos institucionales para activar sus operaciones de información en línea a través de medios cada vez más encubiertos y sofisticados dejando a los Estados en gran medida a la defensiva. Tanto individual como conjuntamente, Beijing y Moscú están aprovechando los recursos tecnológicos y mediáticos de sus países para disminuir la influencia global de los Estados Unidos y avanzar en sus propios objetivos geopolíticos, y es probable que la atracción gravitacional de estos enfoques simbióticos se fortalezca. A través de un conjunto de herramientas cada vez más diverso y tecnológicamente avanzado, que va desde *astroturfing* y publicidad en línea dirigida hasta falsificaciones profundas y aplicaciones virales de redes sociales, tanto China como Rusia pueden movilizar sus campañas en línea de manera más ágil y encubierta para afianzarse en las sociedades de todo el mundo y disminuir la influencia global de los Estados Unidos (Daniel Kliman, 2020).

5. **Conclusiones**

Las definiciones rusas de *informatsionnaya voyna* divergen de las definiciones occidentales de comunicaciones estratégicas principalmente en la descripción de los objetivos finales perseguidos durante estas actividades. A diferencia de sus contrapartes occidentales que se esfuerzan por modelar el comportamiento del público objetivo para promover intereses o políticas, el pensamiento ruso subraya que los objetivos finales de *informatsionnaya voyna* son desestabilizar y coaccionar o influir negativamente en el ambiente informativo del adversario.

Para ello busca complicar la política interna de un país objetivo, sus alianzas, y la deslegitimación de las instituciones democráticas. Esto lleva a Moscú a actuar sobre temas específicos, como la promoción de la campaña del Brexit en el Reino Unido o los separatismos o las elecciones en determinados países o más generales como la Revolución Global. Para ello emplea tres herramientas que se complementan e interrelacionan: la desinformación, la combinación con operaciones cibernéticas y el enmascaramiento (*maskirovka*).

Mediante el uso de la teoría del "control reflexivo", el enemigo es manipulado para tomar decisiones que han sido previamente decididas por el manipulador. Tal confrontación de información se utiliza para ganarse a la opinión pública mundial e incentivar a la población nacional.

Sus dos prioridades incluirían la creación de una percepción positiva en las regiones donde prioriza las relaciones económicas y estratégicas (África, América Latina y Oriente Medio) y fragmentar el orden internacional liderado por Estados Unidos para lo cual se vale de campañas de desinformación, engaño y propaganda que han ido incrementándose de manera importante desde los comienzos de esta década.

Aunque la tecnología que Rusia está desplegando hoy para difundir desinformación es nueva, su estrategia es la misma que la de su predecesora, la Unión Soviética.

Al igual que Rusia, China también considera que las operaciones de información son fundamentales. De hecho, el Partido Comunista Chino (PCCh), y por extensión el Ejército Popular de Liberación (EPL), ve las operaciones de información a través del espacio, la cibernética y la guerra electrónica como fundamentales en cualquier conflicto futuro para dar forma a la narrativa y obtener superioridad de información, paralizando así a un enemigo más poderoso.

China por su parte centra sus actividades de influencia, en dar forma a narrativas positivas que promoverán las relaciones de cooperación con países clave y apagarán las voces críticas. Con este fin, busca penetrar en la política y las sociedades de los países objetivo en todos los niveles invirtiendo en relaciones a largo plazo y construyendo redes de dependencia.

Conceptualmente la estrategia de las Tres Guerras organiza diferentes operaciones no cinéticas relacionadas con la información para influir en el comportamiento del adversario en tres categorías: operaciones psicológicas estratégicas, manipulaciones abiertas y encubiertas de los medios de comunicación y explotación de los sistemas jurídicos nacionales e internacionales.

La doctrina de las "tres guerras" consiste en una guerra de opinión pública para influir en la opinión pública nacional e internacional, una psicológica para conmocionar y desmoralizar a los soldados y civiles enemigos, y otra legal para obtener apoyo internacional a través del derecho internacional y nacional.

De lo analizado, puede verse que China y Rusia no son lo mismo cuando se trata de guerra de la información. Si bien tanto uno como otro poseen capacidades similares, explotan la asimetría de los sistemas democráticos apuntando a ambientes de información abiertos, para influir en actividades que buscan explotar las vulnerabilidades democráticas para manipular políticas y sociedades y emplean compañías comerciales, "hackers patrióticos" o ciberdelincuentes en nombre del estado dejando el espacio suficiente entre el estado y estos grupos proxy para que puedan negar su participación y sea difícil la atribución de un ataque, los objetivos estratégicos fundamentales de las operaciones de información de ambos países son significativamente diferentes.

Por lo tanto, podemos concluir que las intenciones de China serían las de emerger como líder mundial mediante la manipulación de los medios de comunicación mientras que la de Rusia, por otro lado, sería la de buscar la división en los Estados Unidos y la UE agravando las tensiones mediante la difusión de noticias falsas y mensajes diseñados para erosionar la forma democrática de gobierno.

Capítulo 6

Interacciones de la comunicación estratégica y la planificación estratégica militar

Por CR Dr. Márcio Saldanha Walker

1. El problema de definir comunicación estratégica

No hay consenso sobre la definición de comunicación estratégica en las doctrinas militares. Además, el concepto de comunicación estratégica puede adquirir una connotación diferente en el entorno civil que en el militar. Quizás la tensión más significativa y perniciosa en la discusión es la de aquellos que dan a entender que el objetivo de la comunicación estratégica o diplomacia pública es influir, y aquellos que sostienen que el objetivo es sólo informar, sin influir (Paul C. , 2011).

Según la Real Academia Española (2022), el término comunicación puede ser definido por:

1. f. Acción y efecto de comunicar o comunicarse.
2. f. Trato, correspondencia entre dos o más personas.
3. f. Transmisión de señales mediante un código común al emisor y al receptor...

La segunda parte del concepto estaría dirigido a un significado, mediante un adjetivo que agrega algunas especificidades a una definición militar del término:

1. adj. Perteneciente o relativo a la estrategia.
2. adj. Que posee el arte de la estrategia.
3. adj. Dicho de un lugar, de una posición, de una actitud, etc.: de importancia decisiva para el desarrollo de algo.

4. adj. Dicho de un arma: capaz de causar gran destrucción, alcanzando un objetivo estratégico.

Así, de una definición inicial, en español, podría suponerse que se trata de una comunicación amplia con fines estratégicos, en el contexto del término de estrategia nacional o estrategia militar.

Los estudios doctrinarios del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO) en 2019 buscaron establecer una definición, sin embargo, esta no fue adoptada doctrinariamente y no está incluida en el manual de la República Argentina, en el *Glosario de Términos de Empleo Militar para la Acción Militar Conjunta* 2019 del EMCO.

La propuesta de definición de comunicación estratégica según el jefe de Estado Mayor Conjunto sería:

> El empleo planificado, coordinado e integrado de todas las capacidades y medios de comunicación que tiene a su disposición el Nivel Estratégico Militar con el objeto de generar percepciones/adhesiones favorables, en los ámbitos de interés conducentes al logro de los objetivos y desafíos estratégicos de la Defensa Nacional. (Sosa, 2019)

Se puede ver en esta definición que restringe la propuesta a los medios de comunicación o incluso a las acciones de información, no considerando medios de la política de defensa nacional, tales como programas, diplomacia y acciones integradas entre las instituciones del Estado.

Estados Unidos definió la Comunicación Estratégica como:

> Los esfuerzos enfocados del Gobierno de los Estados Unidos para comprender e involucrar a audiencias clave para crear, fortalecer o preservar condiciones favorables para el avance de los intereses, políticas y objetivos del Gobierno de los Estados Unidos mediante el uso de programas, planes, temas, mensajes y productos sincronizados con las acciones de todos los instrumentos del poder nacional (United States, 2009, pág. I.2).

Este concepto extiende el término a la política de defensa nacional, entendiendo que el establecimiento de programas, planes y productos es también una cuestión de comunicación estratégica entre los pueblos y los estados, de manera institucional e integrada involucrando a todos los instrumentos del poder nacional.

La OTAN ha estado buscando la mejora de la Comunicación Estratégica y creó un Centro de Excelencia de Comunicaciones Estratégicas (StratCom CoE). Así, la OTAN definió la Comunicación Estratégica como "el uso coordinado y apropiado de las actividades y capacidades de comunicaciones de la OTAN en apoyo de las políticas, operaciones y actividades de la Alianza, y con el fin de avanzar en los objetivos de la OTAN" (NATO Centre for Global Studies , 2019). Sin embargo, aun así, OTAN ha enfrentado

dificultades para definir cómo integrará las capacidades relacionadas con la información. Esto se debe a la diferencia de propósitos en las estrategias nacionales de cada uno de los componentes de la organización de la OTAN.

En el nivel de comunicación estratégica, los conceptos adecuados a las capacidades de Operaciones de Información no son suficientes, pues se proponen para el nivel operacional circunscrito a las operaciones militares. El nivel de comunicación estratégica trasciende el nivel operacional, incluso antes de que exista un nivel operacional, ya que la comunicación estratégica está relacionada con los intereses nacionales en el nivel político. Dentro del concierto de países que son miembros de la organización militar, existen distinciones en relación al marco normativo en el nivel político, así como en relación a cuestiones jurídicas o legales entre ejercer la comunicación estratégica interna o externamente.

Como ejemplo de la dificultad de propósito en las definiciones de este nivel estratégico, la "Doctrina para el empleo de las Fuerzas Armadas" del Reino de España define la Comunicación Estratégica de la Defensa como "el empleo coordinado y apropiado de todas las capacidades de comunicación de la Defensa en apoyo de sus políticas, operaciones y actividades, con el fin de contribuir a la consecución de los objetivos de la Defensa Nacional" (España Ministerio de Defensa, 2018). Sin embargo, cuando desee involucrar todas las capacidades de comunicación nacionales, debe considerar el impacto y la importancia de los medios que están fuera del control militar. Esta situación complica la estandarización de metodologías o estrategias de comunicación.

El Reino Unido, en 2019 la definió como la forma de "promover los intereses nacionales mediante el uso de la Defensa como medio de comunicación para influir en las actitudes, creencias y comportamientos de las audiencias" (United Kingdom MoD, 2019). De acuerdo con este enfoque, UK considera influir en las audiencias militares y no militares, lo que complica el marco legal para la capacidad de comunicación. Como puede verse, los intereses y estrategias nacionales a este nivel, en cada uno de los países pertenecientes a la OTAN, tienen diferentes propósitos y metodologías, con diferentes organizaciones en relación a la autonomía de cada estado en la elección de sus prioridades.

Como ejemplo, los documentos estratégicos, como la Estrategia de Seguridad Nacional (NSS) de EE. UU., brindan una comunicación estratégica duradera, se establecen dentro de un marco contextual e identifican el objetivo o el estado finales. Esta comunicación estratégica duradera con contexto, razón/motivo y meta/estado final a menudo se denomina narrativa. Los mensajes deben respaldar los temas en ese nivel, los temas deben respaldar (o anidarse debajo de) los siguientes temas de nivel superior, y los temas en todos los niveles deben respaldar los temas estratégicos y la narrativa nacional ser perdurable. Esto asegura comunicaciones consistentes a audiencias globales a lo largo del tiempo (United States, 2009).

Para eliminar la confusión causada por la definición amplia de Comunicación Estratégica y el bagaje intelectual del término estratégico, se puede considerar el uso del término - Estrategia de Comunicación - para la construcción general, dejando

intactos los términos específicos de comunicación estratégica que describen esfuerzos en los diferentes niveles de la guerra. La estrategia de comunicación es el modelo adoptado por cada estado para poner su narrativa de acuerdo con sus propios objetivos nacionales, mientras que la comunicación estratégica es el esfuerzo de comunicación organizado en niveles de acción. En otras palabras, el éxito de la comunicación estratégica depende de elegir una estrategia de comunicación eficiente, la cual dependerá de objetivos estratégicos y nacionales bien definidos.

Otro punto importante para considerar con relación a la definición de Comunicación Estratégica es la capacidad de influencia, debido a la diferencia de percepción. El término influencia en la comunicación estratégica, tal como está presente en la doctrina del Reino Unido, puede adquirir una connotación peyorativa y por lo tanto ser utilizado con una intención ofensiva. En ese sentido el término influir el término está presente en doctrinas de operaciones de información en el nivel operacional militar, y estrategia de información en el nivel político, como en la estrategia de campaña de información de Reino Unido.

> Acciones coordinadas emprendidas para influir en un adversario o adversario potencial en apoyo de objetivos políticos y militares, socavando su voluntad, cohesión y capacidad de toma de decisiones, afectando su información, procesos basados en información y sistemas protegiendo a los propios tomadores de decisiones y procesos de toma de decisiones (United Kingdom Joint Forces, JWP 3-80, 2002, p. 2.1).

Es importante resaltar que la intención de usar el término comunicación estratégica en el sentido militar del nivel operacional, como en los EE. UU. y Reino Unido, es influir en un público externo y blancos militares, particularmente cuando es enemigo, y no está dirigido a acciones contra un público interno. Sin embargo, el carácter integral de la comunicación estratégica va más allá de los límites físicos de las operaciones militares, tradicionalmente limitadas a los Teatros de Operaciones. La comunicación estratégica involucra a otros actores en la estructura política de un estado, considerando que el vector militar es uno de los vectores de comunicación. Así, la comunicación estratégica se relaciona al más alto nivel del Estado con la política diplomática, con el fin de orientar el conjunto de esfuerzos nacionales hacia el logro de los objetivos nacionales.

Durante una situación de conflicto de intereses, la comunicación estratégica estará enmarcando las operaciones de información con una campaña de información, basada en una narrativa. El término campaña de información fue definido hace más de veinte años por el manual del Ministerio de Defensa del Reino Unido, JWP 3-80, como: "salida de información coordinada de toda la actividad gubernamental emprendida para influir en los tomadores de decisiones en apoyo de los objetivos políticos, protegiendo al mismo tiempo los propios tomadores de decisiones " (United Kingdom Joint Forces, JWP 3-80, 2002, p. 1.2).

Por lo tanto, parece que el Reino Unido busca coordinar la actividad de influenciar al más alto nivel, comenzando a planificar sus acciones en el nivel de la Estrategia Nacional. De esta forma, el nivel estratégico determina el formato necesario para las operaciones de información, encaminando el esfuerzo a la consecución de los intereses de forma favorable.

En esta era de la información, el Reino Unido puso su intención de forma expuesta en su publicación con el título "CP 411: Defensa en una era competitiva" (United Kingdom MoD, 2021), al elegir las operaciones de información, o campaña de información, como estrategia en conjunto con las Relaciones Internacionales. Esto demuestra que las acciones militares de comunicación propuestas también pueden lograr los efectos deseados en el nivel estratégico y político. Así, el Reino Unido trabaja su comunicación estratégica sincronizando con una operación de información desde el nivel estratégico militar.

Basado en lo anterior, para comprender el concepto de comunicación estratégica, es necesario definir cómo el nivel estratégico militar debe vincularla con las operaciones de información. Las operaciones de información son acciones en las dimensiones física, humana e informativa que se realizan durante una operación. La comunicación estratégica, a su vez, se ejerce de manera más amplia y holística, de acuerdo con la intención de un estado político final deseado. La comunicación estratégica se basa en la comprensión inherente de que todas las actividades diplomáticas, de información, militares y económicas (DIME) están dirigidos al mismo esfuerzo estratégico para lograr metas nacionales.

La definición de comunicación estratégica para usos militares, por lo tanto, es comunicar el alineamiento de las intenciones políticas y su relación con las acciones militares. La comunicación estratégica debe admitir que tiene que ver con la intención estratégica del comandante, y debe contener un compromiso con la verdad, un compromiso con la credibilidad, y debe emprenderse como informar con una persuasión virtuosa.

2. **Coordinación de la comunicación estratégica**

En general, la comunicación estratégica actúa en una sola dirección, en forma de información pública, en el nivel político y estratégico, entendiendo los mismos intereses de la diplomacia. La comunicación estratégica en esta situación no es un tema estrictamente militar, sino por el contrario, es un tema holístico que involucra a diferentes departamentos del Estado.

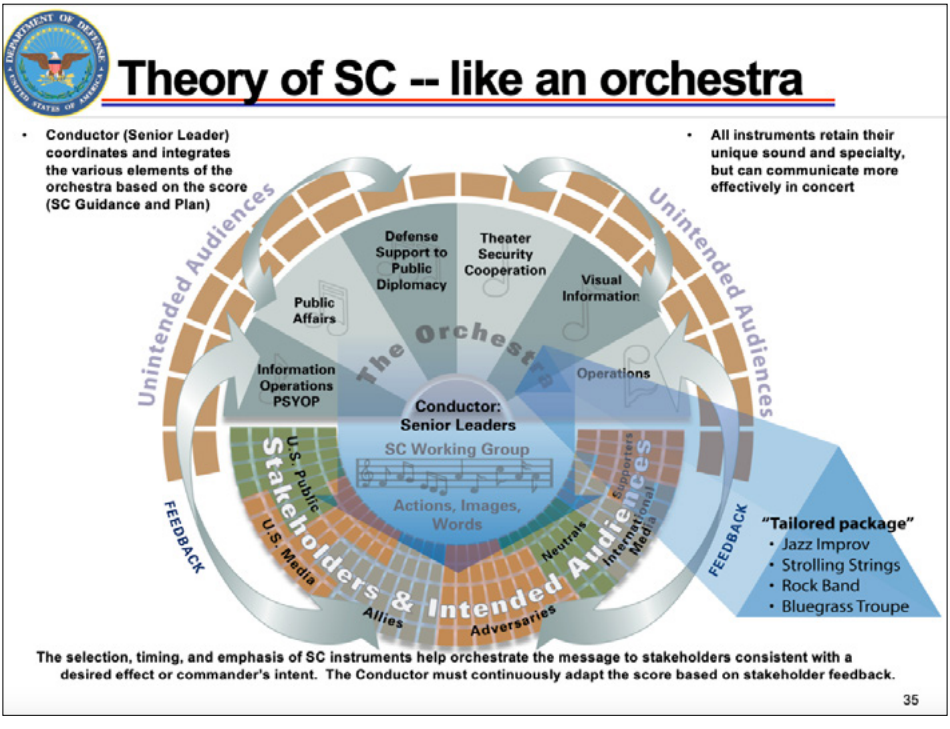
En términos militares, la comunicación estratégica se organiza en dos niveles. El primero es la comunicación institucional, incluida la diplomacia pública (para audiencias extranjeras) y los asuntos públicos (para la escena nacional). En el segundo, en el campo militar, puede dar lugar a una forma de comunicación operacional lo más cerca posible del teatro. Ambos se centran en promover la acción militar ante el público, los medios de comunicación y los responsables de la toma de decisiones (representación parlamentaria, socios extranjeros) (Tenenbaum, 2021).

Debido a la importancia de controlar la narrativa y mantener la superioridad de la información, la intención de la información y el estado final deseado en el nivel político nacional deben ser llevados a cabo por el Comandante Supremo en una campaña militar. La comunicación estratégica en términos militares comunicará esa intención para que las acciones tácticas tengan fines estratégicos. Debido a la gama de efectos posibles, resultantes de acciones heterogéneas y, a veces, no sincronizadas, la integración y la coordinación de las acciones de comunicación estratégica son fundamentales para la resolución de los conflictos.

La coordinación de la comunicación estratégica depende de un esfuerzo de mando centralizado con acciones descentralizadas. Las doctrinas militares extranjeras occidentales presentan características de amplio acceso a la información, muchas veces dificultando el establecimiento de protección contra ataques a la información, necesitando coordinar acciones informativas con diferentes organizaciones.

En contraste, doctrinas más centralizadas como Rusia y China tienen una estructura altamente controlada y cerrada, en sistemas y metodologías, lo que en cierto modo simplifica el proceso de protección de la información. Sin embargo, hoy en día,

ILUSTRACIÓN 67 . **Comunicación Estratégica relacionada a una orquestra produciendo harmonía**



FUENTE: (UNITED STATES DOD, 2009)

debido a la amplia capacidad tecnológica, la comunicación estratégica cerrada no ha sido efectiva, con el ejemplo de la Guerra de Ucrania de 2022. Esto se debe a que la estrategia no resiste la contraprueba de la libre prensa en el entorno de comunicación occidental.

Como ejemplo de un intento de organizar la comunicación estratégica desde los niveles más altos, dentro del gobierno de los EE. UU., la Oficina del Subsecretario de Diplomacia Pública y Asuntos Públicos del Departamento de Estado (DOS) tiene el liderazgo en Comunicación Estratégica. Para apoyar el esfuerzo del gobierno de los EE. UU. dirigido por DOS, el Departamento de Defensa ha establecido organizaciones y procesos de personal para guiar y brindar apoyo al esfuerzo de comunicación estratégica (United States, 2009). En esta estructura, no EE. UU., para fines militares, la comunicación estratégica militar tiene lugar durante una campaña militar.

En una visión general holística de los EE. UU., la acción de coordinación informativa puede explicarse utilizando una metáfora de comparación con una orquesta sinfónica, ver figura. El director de la comunicación (líder principal) coordina e integra los varios elementos como un director dirigiendo una orquesta, basándose en la partitura (orientación y plan de comunicación estratégica). Las audiencias objetivo de la comunicación estratégica pueden ser aliados o neutrales, así como adversarios, tanto de los medios estadounidenses como internacionales. Esta relación que involucra a diferentes audiencias es importante porque significa que las acciones militares tendrán un impacto en la comunicación más allá del contexto militar propiamente dicho.

Todo debe estar coordinado con las acciones físicas y con las operaciones de información en el teatro de operaciones, como la información pública y las operaciones psicológicas. Por su efecto, la comunicación estratégica apoyará las acciones físicas de las operaciones militares agregando al esfuerzo del apoyo de la diplomacia. Esta coordinación proporcionará la base para lograr los efectos deseados para lograr la intención del comandante. El resultado final debe lograr la armonía sinfónica de la intención del comandante.

Este concepto de coordinación de la información en tiempo de guerra o paz puede variar según la doctrina militar de cada país. Para Rusia, según Mark Laity, jefe de Comunicaciones Estratégicas de la Organización del Tratado del Atlántico Norte (OTAN), Cuartel General Supremo de Allied Powers Europe (SHAPE), la guerra de comunicación ocurre desde el tiempo de paz:

> Los rusos usan información de una etapa encubierta a través de seis fases de la guerra hasta el restablecimiento de la victoria. La confrontación de información se lleva a cabo en todas las fases, incluso de forma encubierta, en paz y en guerra. Nuestras doctrinas no nos permiten hacer muchas de estas cosas hasta que básicamente comienza la lucha.[120]

120 Russia: Implications for UK defence and security," First Report of Session 2016–17, House of Commons Defence Committee, UK Parliament, 5 July 2016, p. 17.

Esta comunicación estratégica actual de Rusia sufre el efecto de la estrategia de Gerasimov, con la doctrina de la guerra híbrida (Chivvis, 2017). Todas las acciones militares y no militares están centralizadas y dentro de los propios canales de información del país. A pesar de esta estrategia de comunicación habría sido efectivo en un escenario localizado con Georgia en 2008 y Ucrania en 2014, sin embargo, no resistió a la guerra informativa abierta globalizada de 2022 en Ucrania. Rusia ha enfrentado grandes dificultades para controlar los efectos de su comunicación estratégica, que ha demostrado perder el control de la narrativa en el nivel estratégico y generar efectos no deseados en el nivel operacional de la guerra de Ucrania.

En China, el Partido Comunista Chino y los líderes militares están de acuerdo en que las guerras futuras conducirán a la coordinación más allá de guerras orientadas a la información y guerras inteligentes. En la lucha contra la guerra de la información, la idea es que los militares integren las dimensiones terrestres, marítimas, aéreas, espaciales, cibernéticas y electromagnéticas en un sistema basado en tecnologías de la información. Esto se considera cuando el poder militar evoluciona aún más hacia una forma de operaciones conjuntas, eliminando los límites entre el Ejército, la Armada y la Fuerza Aérea, con un comando unificado informativo (Japón, 2021).

En la etapa de que la guerra evolucione hacia la forma inteligente, la intención de China es de construir un sistema de comando y coordinación informativa que integre humanos y máquinas, que utilice tecnologías como la inteligencia artificial, facilitando la toma de decisiones. Los objetivos de ataque también incluirán objetos intangibles como el espacio cognitivo. El espacio operacional de guerra inteligente superará el de la guerra de información actual (Japón, 2021).

Por lo tanto, independientemente de las ideologías o los sistemas políticos, coordinar los términos de la información es crítico para que los efectos esperados de la comunicación estratégica estén perfectamente alineados en los diferentes niveles de conducción militar. Para evitar ataques de los adversarios o el fratricidio de información en la comunicación estratégica hay que emplear elementos de operaciones de información de una manera que cause efectos en el entorno de información que impidan la realización de operaciones enemigas o afecten negativamente a las fuerzas amigas. Las acciones deben realizarse en campaña, respetando el grado de intencionalidad, antes, durante y después de cada acción militar en el teatro de operaciones.

En la coordinación de comunicación estratégica, las acciones hablan más que las palabras. Esta perogrullada es absolutamente fundamental para una construcción de comunicación estratégica efectiva. Esto se duplica para las acciones cinéticas (maniobra y fuego) de las fuerzas militares en una campaña militar. Si una imagen puede valer más que mil palabras, entonces una bomba puede valer diez mil. La comunicación estratégica debe coordinarse con las acciones físicas de las tropas en el terreno, apoyándose en operaciones de información.

La comunicación estratégica es la comunicación de la intención del comandante desde los niveles más altos, por lo que no es cualquier comunicación. Cualquier implementación de comunicación estratégica incluye coordinar la comunicación tradicio-

nal, la mensajería militar y los comunicados de prensa, en una perfecta sintonía entre los medios de comunicación militares y no militares. Las acciones de comunicación más simples necesitan ser coordinadas, esto evitará el fratricidio informal.

Cada componente militar realiza tareas y estas acciones se realizan conforme a fines. Los propósitos de cada tarea están dirigidos a una sola línea de esfuerzo informativo. Por lo tanto, la comunicación estratégica impulsa las acciones físicas, informando a las audiencias objetivo amigables y neutrales, e influyendo en los enemigos para lograr comportamientos deseables. El comportamiento deseado es la alteración de una situación anterior no deseada, en el nivel político, modificando elementos informativos para obtener una situación final favorable después de la acción militar.

La coordinación de la comunicación estratégica requiere, por lo tanto, una estrategia de comunicación única. Una estrategia clara requiere una estrategia del más alto nivel, así como una estrategia que vaya más allá de la comunicación estratégica militar: una estrategia clara de política exterior que la comunicación estratégica pueda respaldar.

3. **Niveles de la comunicación estratégica**

Debido a los aspectos ya mencionados en estos estudios en relación con la capacidad de coordinar los efectos, la comunicación estratégica es establecida por los más altos niveles de conducción militar. Esto requiere efectos de coordinación a través de diferentes niveles, dirigiendo acciones operacionales y tácticas en el niveles más bajos.

La comunicación estratégica militar está incrustada por debajo de los niveles más altos bajo responsabilidad política. En el nivel Estratégico Nacional, la Comunicación Estratégica se ejerce directamente por el presidente de la Nación, desde la paz hasta la resolución de un conflicto. Su propósito es comunicar las restricciones y límites a los componentes del poder para lograr los objetivos políticos. Todos los aspectos de la política nacional y como el poder militar será empleado están bajo esta comunicación estratégica. La finalidad es definir el estado final político deseado. Las acciones militares en el campo de la comunicación se llevarán a cabo en la dirección de estos objetivos estratégicos y políticos.

En el nivel Estratégico Militar, la Comunicación Estratégica se ejerce directamente por el presidente de la Nación o indirectamente por el ministro de la Defensa o por el jefe de Estado Mayor Conjunto. Esto se debe a los efectos transversales entre las acciones militares y los diferentes ministerios encargados de alguna acción de defensa nacional. La comunicación estratégica en este nivel contribuye para el esfuerzo militar y su coordinación con los otros recursos de la nación. La finalidad es definir el estado final militar deseado (United States DoD, 2016). El concepto puede variar de acuerdo con la organización de cada país, sin embargo, lo importante es entender la importancia del nivel estratégico para lograr el éxito de una estrategia de comunicación. El nivel estratégico es el encargado de interpretar la intención política y así determinará los objetivos estratégicos en materia de comunicación. Estos objetivos estratégicos se lograrán mediante acciones físicas y no físicas en el nivel operacional y táctico.

En el nivel Operacional, tomando la definición de nivel de conducción militar según la doctrina militar argentina (España Ministerio de Defensa, 2018), la Comunicación Estratégica se ejerce directamente por los comandantes de nivel operacional. Esto significa que el comandante operacional es responsable de toda la comunicación producida por acciones físicas y no físicas en este nivel de conducción. En este nivel, la comunicación lleva a cabo contribuir con el esfuerzo militar para el logro del estado final militar deseado. Normalmente, la comunicación estratégica operacional se lleva a cabo bajo el Comando unificado de un comandante de Nivel Operacional. Por lo tanto, el comandante operacional necesita coordinar, entre las fuerzas, todas las formas de comunicación que se puedan generar. Se trata de emisiones electromagnéticas, cibernéticas, comunicativas o incluso acciones físicas que generarán impactos o efectos en el resultado de cada operación.

Sin embargo, esta subdivisión de la comunicación estratégica puede no ocurrir naturalmente. Aún con la necesidad de coordinación e integración, existen estructuras que terminan subdividiendo los esfuerzos de comunicación estratégica en los más altos niveles. Normalmente los niveles o umbrales no son visibles. Las acciones pueden ser tácticas y tener efectos estratégicos. La comunicación estratégica puede tener un impacto inmediato en el entorno operacional. Todo esto caracteriza el aplanamiento de los niveles de toma de decisiones y conducción militar en los aspectos de los efectos comunicativos. Asimismo, dentro de caden el nivel de conducción, ya sea estratégico u operacional, no existe un límite transversal claro que pueda determinar el control de efectos de la comunicación.

Como ejemplo, en los EE. UU. la comunicación estratégica puede encontrar subdivisiones en los niveles más altos de los departamentos de estado. En el Departamento de Estado (DOS) debe ser el hogar de sólidas capacidades de comunicación estratégica y diplomacia pública, la fuente de estrategias y temas relacionados, y prominente en los esfuerzos para coordinar y resolver conflictos (United States, 2009). En este nivel, ya sea en el ámbito interno o externo, existen distintas percepciones e intereses a coordinar en relación con los temas prioritarios de la defensa nacional.

El ámbito militar necesita coordinar la defensa nacional integrada en los aspectos humanos, como la gestión en el ámbito ambiental o económico y financiero. El contexto de la comunicación estratégica es muy cercano a las acciones diplomáticas y, por tanto, necesita adaptarse a los diferentes intereses nacionales. En este nivel estratégico de conducción, la estrategia de comunicación necesita adaptar tanto la comunicación militar estratégica como las acciones diplomáticas no militares.

Esta dificultad de integración, igualmente, se encuentra dentro del ámbito militar en el nivel estratégico y operacional. En la comunicación estratégica del Departamento de Defensa (DoD), los comandantes en otros niveles están haciendo de la comunicación estratégica una prioridad bajo a las amenazas y a los conflictos. Todos los comandos combatientes establecen algún tipo de estructura para la coordinación de la comunicación estratégica (United States, 2009). Esto se debe a la gran dificultad de controlar los impactos electromagnéticos, cibernéticos y comunicativos dentro de los

límites de una operación militar. Asimismo, debido a las estructuras compartimentadas de la inteligencia militar, la información es impactada por percepciones cognitivas que pueden diferenciar prioridades dentro de cada una de las fuerzas militares componentes.

Existe una constante evolución tecnológica que amplía la cantidad y capacidad de los sistemas en un entorno multicapa. Los entornos espaciales, aéreos, terrestres, acuáticos, cibernéticos, virtuales o cognitivos son vectores de posibilidades comunicativas. El entorno multicapa representa la amplitud de las capacidades militares y no militares y las posibilidades físicas y no físicas presentes en escenarios de conflicto, o incluso fuera de él.

A la luz de lo anterior, existen diferentes niveles de conducta donde se debe aplicar una estrategia de comunicación en una forma y estructura vertical adecuada para una comunicación estratégica eficiente. Es decir, linear acciones en el nivel político, estratégico, operacional y táctico. Asimismo, los niveles de conducción son un conjunto de esferas horizontales o transversales que tienen diferentes componentes distribuidas en cada uno de estos niveles. Tales como las estructuras de los departamentos ministeriales, en el nivel estratégico, y de las fuerzas militares componentes, en el nivel táctico. Por lo tanto, la correcta coordinación de la comunicación estratégica pasa por considerar las diferencias y similitudes que existen entre cada uno de los niveles de la comunicación estratégica, tanto en su forma en el nivel vertical como en su forma en el nivel transversal.

Todavía las preocupaciones en la fuerza de comunicación más se amplían en los escalones más bajos. Fuera de los entendidos en comunicación estratégica, existe una falta general de certeza sobre qué es realmente la comunicación estratégica y cómo hacerla. Los niveles inferiores del rango militar no pueden sufrir la falta de orientación para la comunicación estratégica. Todos los temas y mensajes de mayor nivel necesitan llegar a los niveles más bajos ya definidos.

4. Objetivos y límites de la comunicación estratégica en planeamiento militar estratégico

Los objetivos de la comunicación estratégica militar dependerán de los aquellos de nivel nacional y de los intereses claramente establecidos. Estos deben contener objetivos subordinados anidados, que contengan otros de tipo intermedio o de apoyo asentados en el nivel operacional y táctico. De esta forma se facilitará al decisor apreciar qué objetivos pueden lograr una ventaja sobre los adversarios a través de la influencia o la disuasión, y cuáles se pueden apoyar a través de dichos esfuerzos informativos, para contribuir al fortalecimiento de los intereses nacionales.

Los límites en la comunicación estratégica son físicamente invisibles. La rápida evolución de la tecnología contribuye a la expansión de los límites no físicos a un entorno multidominio indefinido. Corresponde al estratega identificar los puntos de vinculación, intereses, responsabilidades, valores y legalidad de las acciones militares que dependen de la percepción histórica y cultural de cada país. La sociedad cons-

truye en la evolución epistemológica los límites militares aceptables en tiempos de paz y guerra *jus ad belum.* Estos límites deben estar dirigidos a la postura estratégica de defensa de los intereses nacionales.

Además, la comunicación estratégica necesita considerar en el nivel de conducción estratégica la alineación transversal de objetivos, como los intereses y acciones que cruzan y entrelazan los intereses de cada componente en el nivel estratégico nacional. Cada componente organizativo de la estructura política del Estado tendrá sus propios objetivos estratégicos, los cuales podrán coincidir o tener sólo puntos de interés o acciones entrelazados. Para que el nivel estratégico de conducción pueda llevar a cabo la lista de objetivos a conquistar, necesita separar aquellos que son de interés y acción militar. Así, el nivel estratégico militar se enfoca en determinar cuáles son los objetivos estratégicos militares para la comunicación estratégica.

La estrategia de comunicación multicapa de la comunicación considera que el primer nivel de defensa está en la comunicación estratégica. Este nivel se relaciona con la diplomacia en las tareas de comunicar la narrativa de defensa de los intereses nacionales. La comunicación estratégica militar contribuye a fortalecer la disuasión de amenazas incluso en tiempos de paz, buscando evitar la evolución a una situación desfavorable.

En el ámbito militar del nivel de conducción estratégica, la estrategia de comunicación debe involucrar acciones alineadas verticalmente en una sola dirección, como si fuera una función de combate propia, es decir, función de combate de información. Los objetivos militares comunicativos y sus efectos deben ser considerados en los aspectos físicos y no físicos de las acciones militares. Esta alineación de objetivos considerará una clara estrategia de actitud defensiva u ofensiva multicapa, ya sea en el entorno electromagnético, cibernético, informativo o cognitivo.

De acuerdo con los intereses de la República Argentina (República Argentina Ministerio de la Defensa, 2021), la comunicación estratégica debe estar alineada con objetivos defensivos, considerando las posibilidades de proteger intereses y obtener una postura de alerta temprana. La actitud defensiva se ejerce naturalmente en tiempos de paz. Aun así, las acciones comunicativas en comunicación estratégica tendrán efectos activos y permanentes que serán necesarios para garantizar el statu quo y evitar perjuicios a las futuras metas nacionales. El establecimiento de objetivos depende de una estrategia que involucra el fortalecimiento de la capacidad cibernética, electromagnética y cognitiva, con una importante participación de la inteligencia artificial.

Los comandos operacionales activados en tiempo de paz o de guerra tienen la misión de asegurar el desarrollo permanente de la capacidad operacional de la defensa nacional. Todas las declaraciones de la intención del comandante también deben incluir el estado final de la información deseada por el comandante. La inclusión de un estado final de información guiará los planes subordinados. La comunicación estratégica incluye propósito e intencionalidad en la comunicación en todos los niveles.

Los objetivos estratégicos de comunicación estratégica planteados en tiempos de paz permiten fortalecer una defensa proactiva en múltiples capas, con la posibili-

dad de evitar acciones físicas militares innecesarias ante amenazas. Un objetivo bien definido para la comunicación estratégica depende de limitar los efectos deseados. Las acciones deben circunscribirse en un centro de gravedad informativo. Este centro de gravedad es el contenido central, es decir, la idea central a transmitir. Todas las acciones informativas necesitan orbitar esta idea central, contribuyendo al esfuerzo de reforzar la idea central. Las acciones informativas deben proteger la idea central deseada, reduciendo las vulnerabilidades críticas. Para ello, deberá actuar con capacidades críticas relacionadas con la información para fortalecer y proteger la comunicación estratégica.

Limitar los blancos militares en el aspecto de defensa nacional externa facilita el control del daño narrativo o efectos comunicativos no deseados. Fundamentalmente, toda oportunidad de comunicación debe estar centrada en buscar la superioridad informativa, es decir, procurar que la narrativa sea a favor de la defensa nacional. El análisis de la audiencia objetivo aparece como una parte limitada esencial de la respuesta al problema que enfrentan los comandantes militares en los teatros: "la tarea vital de cómo comunicar con éxito información e ideas a múltiples audiencias, locales e internacionales, de forma individual y simultánea" (Steiger, 2011). Es necesario limitar las acciones informativas al público deseado adversario para obtener el efecto deseado, con una estrategia de comunicación involucrando todos los niveles de conducción militar.

La comunicación estratégica ocurre en toda la gama de operaciones militares (United States, 2009). Sin embargo, el rango debe ser definido. Normalmente, la comunicación estratégica tiene la característica de transversalidad de efectos y las acciones tácticas pueden tener rangos y efectos estratégicos internacionales. Por lo tanto, la comunicación debe limitarse a los efectos deseados para cada objetivo estratégico y que contribuyan al estado final después de la operación militar. Es importante recalcar que, en términos de comunicación estratégica, el evento de conflicto militar es una situación temporal y que existe la necesidad de normalizar las acciones para una actitud de paz y estabilidad después de cada acción militar.

Durante una operación militar, las fuerzas combinadas o conjuntas se comunican estratégicamente con amigos, adversarios y otros por igual. Las fuerzas conjuntas se comunican estratégicamente con las poblaciones en general, los gobiernos y otras organizaciones nacionales. O sea, las fuerzas conjuntas se comunican estratégicamente en el contexto de conflicto, competencia y cooperación entre agencias (United States, 2009). Los límites de las acciones para influir en audiencias opuestas deben ser muy claros en la planificación militar. Las atribuciones militares no pueden confundirse con las acciones diplomáticas realizadas por otras esferas del poder nacional. Por lo tanto, se vuelve imprescindible que la conducción estratégica militar sepa integrarse con la comunicación estratégica nacional, orientando hacia cuál es la responsabilidad de las acciones militares comunicativas, físicas o no físicas.

La comunicación estratégica incluye esfuerzos para comunicarse con audiencias nacionales dentro de las restricciones legales, principalmente a través de asun-

tos públicos (United States, 2009). En este acto de comunicación estratégica interna al país, el verbo a utilizar por la estrategia de comunicación es informar. Esto caracteriza la intención blanda y democrática, con transparencia y legalidad, de las acciones informativas militares. Otras instituciones y la población nacional necesitan apoyar las acciones militares, de acuerdo con el interés nacional establecido a lograr.

Durante acciones militares en operaciones contra países enemigos, en el ámbito de la directiva de política nacional, el verbo a utilizar por la comunicación estratégica es influir. El significado de la palabra influir es muy cercano al término disuadir las acciones militares de los adversarios. Por eso, incluso si la palabra influir suele tener una connotación negativa, como engaño o manipulación, la palabra influencia debe entenderse con un aspecto más amplio de influir en la voluntad contraria en relación con la necesidad de defender los propios intereses nacionales. La manipulación y otras son formas inapropiadas de influencia que son insostenibles en el entorno de información contemporáneo (serán expuestas, generalmente con bastante rapidez) y socavan la credibilidad de los mensajes y esfuerzos actuales y futuros.

El problema es que la comunicación estratégica no puede entenderse como un esfuerzo de influencia, en el sentido de causar daño psicológico, más si como una acción técnico-especializada. El nivel estratégico necesita enumerar objetivos claros y factibles para la información, dado que serán el resultado de acciones físicas y no físicas en niveles inferiores. En la actividad de comunicación estratégica la acción de influir necesita ser entendida con una connotación positiva, como la de explicar las intenciones e intereses del estado nacional frente a las adversidades estatales conflictivas. En otras palabras, influir con comunicación estratégica es modificar una situación de estado actual no deseada en relación con un estado adversario, con el fin de obtener una situación favorable a los intereses nacionales.

La elección de los objetivos de comunicación estratégica es un proceso metodológico y detallado que considera las relaciones entre los actores estatales. Por un lado, habrá actores favorables, que podrán multiplicar el discurso de la comunicación, y por otro, los desfavorables, que harán el esfuerzo contrario para desprestigiar los intereses de un determinado Estado. En la comunicación estratégica no existe una percepción general de neutralidad, ya que están en juego los intereses de los estados. La posición neutra es temporal y en relación con un hecho determinado. Así, aún en el nivel estratégico, se inicia la selección del esfuerzo de comunicación que debe seguir apoyando, reforzando y complementando el esfuerzo principal de un país frente a una situación de conflicto.

La comunicación estratégica requiere entonces superar su propio sesgo cultural y tenga un enfoque moderado de la influencia como un concepto virtuoso, basado en la información y no en la manipulación. La comunicación estratégica necesita reconocer que hay limitaciones de percepción en otros estados y debe contribuir para disminuir fricciones debidas a las sensibilidades de otros estados.

Por lo tanto, cuando se seleccionan blancos en la comunicación estratégica en términos universales durante las operaciones militares se deben integrar y sincroni-

zar disciplinas informativas u organizaciones específicas relacionadas con la información. No prescribirá la ejecución individual de asuntos públicos (PA) y apoyo de defensa a la diplomacia pública (DSPD) (United States, 2009), sino que debe complementar la narrativa para obtener superioridad informativa.

5. Interacciones de la comunicación estratégica con las operaciones de información

Clausewitz definió que la guerra está envuelta por una niebla oscura y cegadora que dificulta la definición de actores, acciones e intenciones. En un entorno operacional multidimensional, sumamente afectado por las tecnologías de la información, se están estableciendo muchas definiciones en distintas doctrinas. El objetivo es tratar de definir conceptos informacionales muy utilizados en las operaciones militares actuales, como son la Comunicación Estratégica y las Operaciones de Información. Tanto las operaciones estratégicas de comunicación como las de información tienen objetivos informativos que interactúan con diferentes sistemas de información y acciones físicas durante una operación militar.

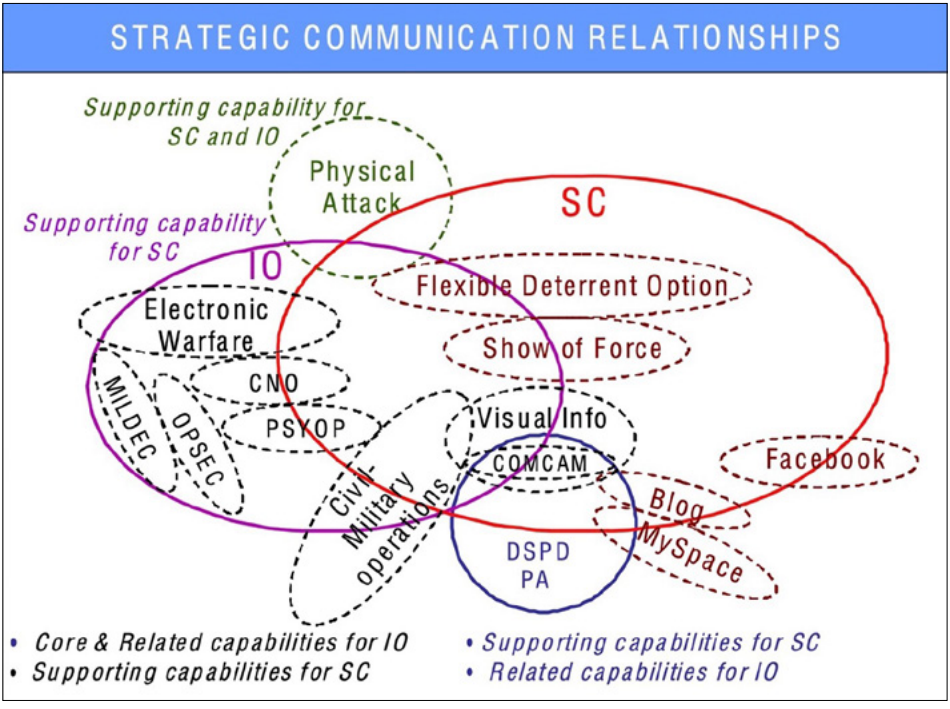
Un ejemplo de esta interrelación entre sistemas en la comunicación puede obtenerse de la doctrina estadounidense. La comunicación estratégica es acción al más alto nivel de conducción. Abarcará la interconexión transversal con las tareas de diferentes organismos estatales que puedan contribuir a la opción estratégica y necesidad de disuasión. La comunicación estratégica apoyará las acciones físicas y protegerá los intereses nacionales.

La comunicación estratégica militar está directamente relacionada con la tarea de apoyar los objetivos nacionales en un esfuerzo de múltiples dominios y multicapa. Frente a los adversarios, la comunicación estratégica actúa para disuadir las amenazas a los intereses. Su acción se apoya en acciones físicas militares y en el esfuerzo técnico especializado de comunicación con los medios, en particular apoyándose en los medios resultantes de la evolución de la tecnología cibernética.

En la comunicación estratégica los esfuerzos de un estado son enfocados para comprender e involucrar a audiencias clave para crear, fortalecer o preservar condiciones favorables. El desempeño de la comunicación estratégica militar brindará lineamientos para el uso de capacidades de la información en el nivel de la conducción operacional, tales como operaciones de seguridad y operaciones de engaño, entre otras, contribuyendo a las Operaciones de Información. Las tareas realizadas por los diferentes cuerpos de las fuerzas armadas tendrán efectos que tienen puntos de contacto y áreas de acción superpuestas.

En la comunicación estratégica existe una cierta jerarquía de ideas clave que no puede ser cambiada por niveles inferiores de comunicación. Esto se debe a que es necesario coordinar y sincronizar la acción para evitar el fratricidio de ideas. Todo esfuerzo debe estar bajo una dirección estratégica que aprobará cualquier cambio en la línea de acción o línea de esfuerzo en la función de guerra de información. La función de combate de la información estará siempre dirigida al estado final deseado en

ILUSTRACIÓN 68 . **Relaciones de la Comunicação Estratégica**



FUENTE: (UNITED STATES DOD, 2009)

cualquier situación de conflicto de intereses entre estados. El nivel estratégico tiene una línea muy fina entre la paz y la guerra, la zona gris, en el juego de los intereses estatales, provocando competencia por utilizar instrumentos militares relacionados con alguna forma de comunicación no física, todo para que la narrativa dominante sea permanente en tiempos de paz.

Mientras que las Operaciones de Información son el resultado de tareas realizadas durante una operación militar por capacidades relacionadas con la información, como Guerra Electrónica, Operaciones Psicológicas, Operaciones de Seguridad, Operaciones de Engaño, Operaciones de Asuntos Civiles y Operaciones Cibernéticas, así como acciones físicas (United States Joint Chiefs of Staff, JP 3-13, 2014). En este nivel de conducción, la forma de agresión es clara, lo que simplifica la actividad de comunicación de combate. Esto se debe a que las acciones de comunicación estarán encaminadas a lesionar la capacidad de decisión del oponente. Su relación de apoyo con la comunicación estratégica tiene lugar durante las operaciones militares y puede ser llevada a cabo por los más altos niveles de liderazgo militar, de acuerdo con el estado estratégico militar final deseado.

Las operaciones de información se planifican desde el nivel más alto de la operación, el estratégico militar. En este nivel, se define el estado final estratégico militar deseado. Luego, el nivel estratégico operacional orientará las líneas de esfuerzo para cumplir con los objetivos estratégicos enumerados. Así, el nivel táctico realizará tareas orquestadas en el espacio y el tiempo, dentro de cada fase operacional, para lograr objetivos y efectos. La comunicación estratégica estará interconectada en estos tres niveles de conducción militar.

El enlace de la comunicación estratégica con Operaciones Psicológicas durante una operación militar, contra un adversario, ocurre por su definición: las operaciones psicológicas se dirigen únicamente a audiencias extranjeras. La forma en que esto ocurre en la doctrina estadounidense puede explicarse analizando la Ley de Intercambio de Información y Educación de EE. UU. de 1948 (Ley Pública 80-402) que prohíbe la difusión nacional de información destinada a audiencias extranjeras (Estados Unidos, 2009). El efecto deseado de las operaciones psicológicas puede ser un comportamiento observable o una emoción, opinión, creencia o actitud no observable. Por lo tanto, las operaciones psicológicas se llevan a cabo solo durante las operaciones militares, dentro del plan de operaciones de información en apoyo de las necesidades de comunicación estratégica y contra un estado adversario.

Los ejemplos de efectos de influencia en comunicación estratégica se destinan exclusivamente en audiencias particulares. Incluyen asegurar a los aliados y simpatizantes existentes, atraer nuevos aliados y simpatizantes, disuadir a los enemigos potenciales y desacreditar a los adversarios. Informar e influir con comunicación estratégica en apoyo de la política nacional requiere que el objetivo de la política sea claro y que esté determinado conjunto de actitudes, comportamientos o percepciones que la audiencia apoyará esos objetivos. Como la doctrina de los EE. UU., la influencia y el concepto de comunicación estratégica abordan el desafío de convencer a otros estados para que actúen de manera compatible con los intereses y objetivos nacionales. O sea, influenciar significa las acciones informativas de la comunicación estratégica adopten un curso de acción específico o simplemente que nos comprendan mejor y nos acepten más (United States, 2009).

Por lo tanto, la comunicación estratégica es un concepto más amplio que se encuentra en un nivel superior del poder de decisión militar, en el que interactúa con otros organismos nacionales dedicados a la diplomacia e información pública. Mientras que las Operaciones de Información están en un nivel inferior, en la conducción operacional, utilizando los lineamientos y la dirección de la comunicación estratégica.

6. **Conclusiones**

La Comunicación Estratégica debe incorporarse a la doctrina militar. No es posible concebir una estrategia de comunicación eficiente en términos militares sin definir claramente sus objetivos y acciones en cualquier situación de conflicto entre estados. El concepto doctrinario de comunicación estratégica está en desarrollo en el mundo, y

no existe una estandarización. Corresponde a cada país definir su concepto y su mejor aplicabilidad dentro de su realidad jurídica política y administrativa.

Los intereses nacionales que constituirán la política de defensa nacional están determinados por la voluntad humana que se construye a partir de los parámetros de información. La Comunicación Estratégica del Estado está concebida por la clara actitud de defensa. La política de defensa necesita comunicar su estrategia de defensa y el instrumento militar necesita comunicar cómo estructurará sus acciones para contribuir al propósito general de defensa.

Diseñar una estrategia de defensa multicapa depende de escalonar adecuadamente la misión de cada uno de los elementos constitutivos de la estructura de defensa nacional. La Comunicación Estratégica está al nivel de las acciones directivas como la diplomacia de defensa, estas directivas son fundamentales para estructurar las operaciones en el ambiente de la información. Las operaciones conjuntas necesitan integrar sus capacidades especiales relacionadas con la información para contribuir a los efectos esperados de una estrategia de comunicación.

El ambiente de la información está presente en los niveles de conducción de la guerra y requiere de infraestructura, organización, educación y especialistas capacitados. Los parámetros de comunicación se construyen dentro de parámetros cognitivos, por lo que la estructuración de los sistemas depende de un formato y una metodología adecuados para ser efectivos. No se espera que la Comunicación Estratégica sea generada por iniciativas puntuales, sino que sea el resultado de un complejo sistema de coordinación de ideas y propósitos. Esto sólo será posible con la correcta preparación del personal involucrado en los procesos, en los diferentes niveles de mando militar.

Epílogo

La real capacidad de las interacciones en el ambiente de la información y su estrategia, dependen de la congruencia entre la estrategia nacional y las sectoriales; para el caso particular de la defensa, la unidad lógica, permitirá alcanzar los objetivos fijados, tanto para atraer como para proteger a la audiencia propia, ya que su adecuada implementación conlleva a una cultura social consistente, desde la estrategia de la comunicación, por la capacidad de ejecución y la credibilidad del accionar.

La Estrategia Comunicacional, es duradera cuando se establece en un marco contextual que identifica objetivos y estados finales, dando motivos o razón, metas y fines, que constituyen la base de una narrativa firme, atractiva y consistente en el tiempo para la audiencia objetivo.

Las operaciones en el ambiente de la información, no son nada nuevo bajo el sol, en los conflictos y las guerras. Podemos rastrear conceptos asociados a ella en autores ancestrales como Sun Tzu, que advierten que “lograr cien victorias en cien batallas no es pináculo de la excelencia. Sojuzgar al enemigo sin luchar es el verdadero pináculo de la excelencia” (Sun, 2015), o bien las acciones de San Martín en la liberación del Perú son una demostración práctica de ello.

Todo lo expuesto en este aporte, refleja la necesidad del accionar mancomunado de todas las fuerzas del estado, en particular la sinergia que producen la diplomacia y la defensa, donde la primera sin la segunda, sería "como una sinfonía sin orquesta", pocos podrían entender de que se tratan esos papeles, pero una adecuada estrategia comunicacional, constituiría la dirección adecuada de esa orquesta sinfónica.

Podríamos emplear páginas y páginas de ejemplo propios y universales sobre este aspecto, pero un evento netamente científico tecnológico como es la irrupción del ciberespacio, ha cambiado de manera exponencial los modos de hacer la guerra a partir del empleo de este ambiente que combina de manera sinérgica el espectro electromagnético, cibernético y de la información. Allí se generan mútiples interacciones donde la narrativa, la comunicación estratégica y el empleo de la información/desinformación, se convierten en un arma no cinética a tener en cuenta. Como se menciona en uno de los capítulos que se han desarrollado, la matriz bélica ha cambiado y, en este cambio, la tecnología asociada al ciberespacio ha sido clave.

El campo de batalla tradicional, donde se enfrentan las fuerzas para dirimir el fin de una guerra, puede ser reemplazado o al menos afectado, por las percepciones que una sociedad y sus fuerzas militares tienen de la realidad, convirtiendo al cerebro en el verdadero ámbito de lucha.

Esta contribución académica exploró desde diferentes perspectivas la problemática de la información y sus interrelaciones. Al abordar las conclusiones de diferentes países, aporta conocimiento sobre los diferentes ambientes en donde se ejecuta, las formas en que la ciencia y tecnología con sus avances profundizan su capacidad de empleo.

Se ha buscado dar al lector una conciencia amplia y general que le permitan definir en su campo de acción, como dinamizar de manera favorable su estrategia en el empleo de esta vieja herramienta, a la cual, los avances tecnológicos le han otorgado capacidades extraordinarias y que sin duda impactan de manera directa en el ámbito de la estrategia militar, operacional y de la táctica.

El concepto multidominio de las operaciones en el ambiente de la información estará cada vez más presente en los conflictos futuros. En una postura defensiva activa, corresponde a cada Estado desarrollar una estrategia cognitiva en el campo de la información para la construcción de líneas de acción adecuadas en el nivel estratégico militar y estratégico operacional.

La vieja frase de Clausewitz en cuanto a que la guerra es un "camaleón" que varía su carácter en forma permanente parece cobrar nueva relevancia. Cómo se enfrenta un futuro complejo e incierto, recae en las élites de un estado que deberán definir las mejores estrategias para alcanzar sus fines últimos que no son otros que el bienestar y la seguridad de la sociedad a la que pertenecen.

Bibliografía

9/11 memorial. (S.F.). *Operation Neptune Spear.* Retrieved from National September 11 Memorial & Museum: https://www.911memorial.org/learn/resources/digital-exhibitions/digital-exhibition-revealed-hunt-bin-laden/operation-neptune-spear#:~:text=Two%20helicopters%20piloted%20by%20Army,U.S.%20base%20in%20Jalalabad%2C%20Afghanistan.

Aamer Madhani, L. C. (2022). *US says new intel shows Russia plotting false flag attack.* Retrieved from https://apnews.com/article/russia-ukraine-business-europe-belarus-jens-stoltenberg-43c9151532de706a2edec5684dfcf07d

Affaires, S. I. (2022, 5 27). *Public Opinion Warfare: Chinese Narratives about the War in Ukraine.* Retrieved from https://www.globalaffairs.ch/2022/05/27/public-opinion-warfare-chinese-narratives-about-the-war-in-ukraine/#:~:text=According%20to%20Chinese%20analysts%2C%20public%20opinion%20warfare%2C%20also,radio%2C%20newspapers%2C%20movies%2C%20and%20other%20forms%20

Ainsworth, S. (2020). *The evolution of the Russian way of informatsionnaya voyna.* Retrieved from https://www.researchgate.net/publication/346429957_The_evolution_of_the_Russian_way_of_informatsionnaya_voyna

Albero, J. L. (2020). *Implicaciones del ámbito cognitivo en las Operaciones Militares.* Retrieved from https://emad.defensa.gob.es/unidades/CCDC/ACTIVIDADES/2020_COGNITIVO.html#:~:text=Inevitablemente%2C%20las%20nuevas%20posibilidades%20en%20el%20intercambio%20de,de%20forma%20que%20se%20consiga%20la%20influencia%20deseada.

Alberque, W. (2022, 10 10). *Russia is unlikely to use nuclear weapons in Ukraine.* Retrieved from https://www.iiss.org/blogs/analysis/2022/10/russia-is-unlikely-to-use-nuclear-weapons-in-ukraine

Aljazeera. (2022, 9 22). Retrieved from https://www.aljazeera.com/gallery/2022/9/22/photos-iran-protests-spread-as-internet-curbed

AlJazeera. (2022, 10 27). Pro-China influence campaign targeting US midterms: Report. pp. https://www.aljazeera.com/economy/2022/10/27/pro-china-influence-campaign-targeting-us-midterms-report#:~:text=Pro-China%20influence%20campaign%20targeting%20US%20midterms%3A%20Report%20Cybersecurity,according%20to%20a%20new%20report%20%5BFile%3A%20Kacper.

Allegri, R. (2021, 10). *Aleksandr Dugin, il Cremlino e l'Occidente.* Retrieved from https://www.osservatoriorussia.com/2021/10/01/aleksandr-dugin-il-cremlino-e-loccidente/

Althuis, Jente. (2022). OW U.S. GOVERNMENT FELL IN AND OUT OF LOVE WITH STRATEGIC COMMUNICATIONS. *DEFENCE STRATEGIC COMMUNICATIONS,* 71.

AMIA. (2021). *Luego de seis años Israel vuelve a tener un jefe de Hasbará.* Retrieved from https://www.amia.org.ar/2021/09/24/luego-de-seis-anos-israel-vuelve-a-tener-un-jefe-de-hasbara/

Amoroso, C. (2018, abr 18). *https://tn.com.ar.* Retrieved from vivir-solos-la-tendencia-que-alcanza-al-356-por-ciento-de-los-portenos: /sociedad/vivir-solos-la-tendencia-que-alcanza-al-356-por-ciento-de-los-portenos_862370/

Asimov, I. (1989). *Circulo Vicioso.* (D. Santos, Trans.) Barcelona, España: Martinez Roca.

Babarinde, M. (2022). *Strategic communication in times of war: Lessons from Ukraine's masterful control of its own narrative;*. Retrieved from https://businessday.ng/bd-weekender/article/strategic-communication-in-times-of-war-lessons-from-ukraines-masterful-co

Bandurski, D. (2022, 3 11). *China and Russia are joining forces to spread disinformation.* Retrieved from The Guardian: https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/

Barak, M. (2021, Abril 27). *A new intifada wave on TikTok.* Retrieved from ILTV Youtube: https://youtu.be/IOQwJ6hpZL8

Barbé, E. (1987). El papel del realismo en las Relaciones Internacionales. *Revista de estudios políticos, ISSN 0048-7694*(57), 149-176. Retrieved agosto 18, 2019, from https://dialnet.unirioja.es/servlet/revista?info=descripcion&codigo=1166

Barlow, J. (2018, Feb 8). *Declaración de Independencia del Ciberespacio.* Retrieved from https://www.weforum.org: https://www.weforum.org/agenda/2018/02/a-declaration-of-the-independence-of-cyberspace/?DAG=c1&gclid=CjwKCAjw46CVBhB1EiwAgy6M4ou6sEQ-pKwU_0l8kdfU9sKb1QDEPvpZWigr7wMMYnqN-Znd5xOsBURoC5mcQAvD_BwE

Bartlett, H. C., Holman, G. P., & and Somes, T. E. (1995). The Art of Strategy and Force Planning. *Naval War College Review, 48*(2, Article 9). Retrieved from https://digital-commons.usnwc.edu/nwc-review/vol48/iss2/9

Bartolomé, M. (2017, Mayo 30). El empleo actual del concepto guerra en las relaciones internacionales. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 12*(2), 43-66. Retrieved from http://www.scielo.org.co/pdf/ries/v12n2/v12n2a03.pdf

Beauchamp-Mustafaga, N., & Chase, M. S. (2019). *Foreign Policy Institute Johns Hopkins SAIS.* Retrieved from Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations: https://www.fpi.sais-jhu.edu/_files/ugd/b976eb_ad85a42f248a48c7b0cb2906f6398e71.pdf

Beaufre, A. (1963). *Introducción a la Estrategia.* (C. L. Roldan, Trans.) París, Francia: Rioplatense.

Behrendt, P. (2022, 4). *San Zhong Zhanfa or Three Warfares. Chinese Hybrid Warfare.* Retrieved from Instytut Boyma: https://instytutboyma.org/en/san-zhong-zhanfa-or-three-warfares-chinese-hybrid-warfare/

Bell, T. (2018, Mar 06). *¿Qué es el procesamiento del lenguaje natural?* Retrieved from CIO España: https://www.ciospain.es/gobierno-ti/que-es-el-procesamiento-del-lenguaje-natural

Bentzen, N. (2018, 10 22). Retrieved from Computational propaganda techniques: https://epthinktank.eu/2018/10/22/computational-propaganda-techniques/

Bērziņš, J. (2018). *The Russian Way of Warfare; Current Russian Military Affairs Conference Executive Summaries* . Retrieved from Edited by John R. Deni July 2018 Strategic Studies Institute U.S. ARMY WAR COLLEGE: https://ssi.armywarcollege.edu/pubs/display.cfm?

Betz, D., & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyeberpower.* (T. I. Studies, Ed.) London, United Kingdom. Retrieved julio 01, 2020

blogabissl. (2018). pp. https://blogabissl.blogspot.com/2018/07/nzz-artikel.html.

Boone Bartholomees Jr., J., McShane, T., Troxell, J., Jablonsky, D., Cunningham, G. K., Cook, M., & Meinhart, R. (2006). U.S. Army War College Guide to National Security Poliucy and Strategy. *Guía de Estudios Estratégicos, 2nd Edition revised and expanded.* (J. Boone Bartholomees Jr., Ed.) Carlisle, Pensilvania, EEUU: U.S. Army War College.

Boone, M. (2021, 8 26). *Strategic Influence Operations: A Call to Action.* Retrieved from https://jpia.princeton.edu/news/strategic-influence-operations-call-action

Boston, S., & Massicot, D. (2017). *The Russian way of warfare A primer.* Retrieved from Rand Corporation: https://www.rand.org/pubs/perspectives/PE231.html

Brasil Exército Brasileiro, EB70-MC-10.213. (2019). *OPERAÇÕES DE INFORMAÇÃO: EB70-MC-10.213.* Retrieved from Comando de Operações Terrestres: https://bdex.eb.mil.br/jspui/bitstream/123456789/5286/1/EB70-MC-10.213.pdf

Brasil Exército Brasileiro, EB70-MC-10.213. (2019). *OPERAÇÕES DE INFORMAÇÃO: EB70-MC-10.213.* Retrieved from Comando de Operações Terrestres: https://static.poder360.com.br/2021/10/manual-de-campanha-exercito-operacoes-informacao.pdf

Brasil Ministério da Defesa, MD 30-M-01. (2020). *Doutrina de Operações Conjuntas: MD 30-M-01* (Vol. I). Brasília.

British Army. (2021, noviembre). *Future Soldier - Transforming the British Army.* Retrieved from https://www.army.mod.uk/media/15057/adr010310-futuresoldierguide_30nov.pdf

Brooks, D. (2018, Oct 26). *The Philosofy of data.* Retrieved from https://www.nytimes.com: https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html

Brown, K. (2020). *Chinese Storytelling in the Xi Jinping Era.* Retrieved from Hague Journal of Diplomacy: https://www.academia.edu/45682219/Chinese_Storytelling_in_the_Xi_Jinping_Era

Calderón Concha, P. (2009). Teoría de conflictos de Johan Galtung. *Revista Paz y Conflictos*(2), 60-81.

Cantalapiedra, D. G. (2022, 3 28). *La estrategia de las Tres Guerras: la Guerra Política con características chinas dentro de la Gran Estrategia de la República Popular de China.* Retrieved from https://www.ieee.es/contenido/noticias/2022/03/DIEEEO29_2022_DAVGAR_China.html

Carnegie Mellon University. (2022). *GLOBAL ISSUE Cybersecurity.* Retrieved from Strategic Intelligence: https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

Carpio, A. T. (2021). *China's three warfares strategy for the South China Sea: Inquirer columnist.* Retrieved from https://www.straitstimes.com/asia/east-asia/chinas-three-warfares-strategy-for-the-south-china-sea-inquirer-columnist

Cdo Cjto de Ciberdefensa. (S.f.). Retrieved from https://fuerzas-armadas.mil.ar: https://fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx

CEEP Think Tank Ejército del Perú. (2019, Jul 11). *El papel de los militares en el ciberespacio como dominio: implicancias, retos y oportunidades.* Retrieved from https://ceeep.mil.pe: https://ceeep.mil.pe/2019/06/11/el-papel-de-los-militares-en-el-ciberespacio-como-dominio-implicancias-retos-y-oportunidades/

Center, J. W. (2010). *Commander's Handbook for Strategic Communication and Communication Strategy.* Retrieved from https://archive.org/details/DTIC_ADA525371

Chamorro, F. (2012). *"Las redes sociales como herramienta de comunicación estratégica de las Fuerzas de Defensa de Israel durante la operación Pilar Defensivo en Gaza"; Real Instituto Elcano; ARI 94/.* Retrieved from http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elc ano_es/zonas_es/ari94-2012_fojon-hernandez-colom_redes_sociales_israel_pilar_defensivo

Chamorro, G. C. (2015). *¿OPORTUNIDAD O RIESGO? REDES SOCIALES Y FUERZAS ARMADAS.* Retrieved from REVISTA DE AERONÁUTICA Y ASTRONÁUTICA: https://www.academia.edu/25950091/_Oportunidad_o_riesgo_Redes_sociales_y_fuerzas_armadas

Cheravitch, J. (2021). *The Role of Russia's Military in Information Confrontation.* Retrieved from https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf

Chile Ministerio de Defensa Nacional, DNC 3-7. (2014). OPERACIONES DE INFORMACIÓN.

China, State Council Information Office of the People's Republic of. (2019, julio 24). *China's National Defense in the New Era.* Retrieved from https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

china.org.cn. (2013). *Think tank urged to research 'Chinese dream'.* Retrieved from http://www.china.org.cn/china/2013-05/28/content_28952587.htm

Chivvis, C. S. (2017). *Understanding Russian "Hybrid Warfare".* (R. Corporation, Ed.) Retrieved from https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Clarke, M. (2019). *China's Application of the 'Three Warfares' in the South China Sea and Xinjiang;* . Retrieved from https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2019-05/chinas_app_of_the_3_warfares_in_xj_and_scs.pdf

Clarke, R. D. (2019). *Statement of US Special Operations Command before House Armed Services Committee Intelligence, Emerging Threats and Capabilities Subcommittee.* Retrieved from https://armedservices.house.gov/_cache/files/7/9/7970f176-0def-4a2d-beb3-a7d5d69e513b/9C80F888EEE40D8E82ABFF5336C012C3.hhrg-116-as26-wstate-clarker-20190409.pdf#:~:text=The%20Joint%20MISO%20WebOps%20Center%20%28JMWC%29%20is%20operating,broader%20portion%2

Clausewitz, C. (1992). *De la Guerra* (Vol. I). Capital Federal: Editorial Círculo Militar.

Cochran, E. S. (2020, 7 9). *China's "Three Warfares": People's Liberation Army Influence.* Retrieved from https://commons.erau.edu/ibpp/vol20/iss3/1/

Cohen, E. A., & Gooch, J. (1998). *"Infortunios Militares: La anatomía del fracaso en la guerra".* Buenos Aires, Argentina: Instituto de Publicaciones Navales.

Comité de Ciberseguridad. (2019, may 24). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA.* Retrieved from https://www.argentina.gob.ar: https://www.argentina.gob.ar/normativa/323594_res829-01_pdf/archivo

Confessore, N. (2018, Abril 4). *https://www.nytimes.com.* Retrieved from Cambridge Analytica y Facebook: el escándalo y las consecuencias hasta ahora: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Cook, S. (2020). *Beijing's Global Megaphone.* Retrieved from https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone

Cook, Sarah. (2020, 4 20). *Beijing's Coronavirus Propaganda Has Both Foreign and Domestic Targets.* Retrieved from Freedom House: https://freedomhouse.org/article/beijings-coronavirus-propaganda-has-both-foreign-and-domestic-targets.

Corbacho, A. L. (2011, Diciembre). Evolución del pensamiento estratégico en las Relaciones Internacionales. CABA, Argentina: Universidad del CEMA.

Courter, I. J. (2022). Russian Preinvasion Influence Activities in the War with Ukraine. *MILITARY REVIEW,* 16. Retrieved from https://www.armyupress.army.mil/Portals/7/PDF-UA-docs/Courter-2022-UA.pdf

Crosbie, T. (2019). Getting the Joint Functions Right. *JFQ 94, 3rd Quarter ,* 96.

Cunningham, C. (2020, 11). *A Russian Federation Information Warfare Primer.* Retrieved from https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#top

D.N. de Ciberseguridad. (S.F.). Retrieved from https://www.argentina.gob.ar: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad

Dance, M., & Rosenberg. (2018, abril 10). *https://www.nytimes.com.* Retrieved from Así funcionaba la recolección de datos de Cambridge Analytica: https://www.nytimes.com/es/2018/04/10/espanol/facebook-cambridge-analytica.html

Daniel Kliman, A. K.-T. (2020, 5). *CENTER FOR A NEW AMERICAN SECURITY |*. Retrieved from Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Dangerous-Synergies-May-2020-DoS-Proof.pdf?mtime=20200506164642&focal=none

David Siman-Tov y Ofer Fridman. (2020). *DEFENCE STRATEGIC COMMUNICATION*, 8, 18.

de Sousa, R. R., & Carvalho de Oliveira, G. (2021). *CONFLICT RESOLUTION INTERVENTIONS IN THE CONFLICT CYCLE.* Retrieved from Research Gate: https://www.researchgate.net/publication/354697798_Conflict_Resolution_Interventions_in_the_Conflict_Cycle/link/614882673c6cb310697fb74e/download

de Vergara, E. (2010). El estudio de la historia, evolución del pensamineto estartégico. *Visión Conjunta*(2), 4-18.

de Vergara, E. (2012). *Estrategia, métodos y rutinas.* Buenos Aires, Argentina: Editorial Universitaria del Ejército.

de Vergara, E. (2017). *Estrategia: el camino.* Buenos Aires, Argentina: Editorial Universitaria del Ejército (EUDE).

Defence, U. M. (2019). *Joint Doctrine Note 2/19* . Retrieved from Defence Strategic Communication: an Approach to Formulating and Executing Strategy: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf

Detsch, J. (2022, 21 10). *Russia Wages Winter Information War Against the West.* Retrieved from https://foreignpolicy.com/2022/10/21/russia-winter-information-war/

Díaz-Caneja, J. M. (2022). *OPERACIONES DE INFLUENCIA: LA CLAVE ESTÁ EN EL ANÁLISIS.* Retrieved from Inteligenciayliderazgo: https://inteligenciayliderazgo.com/contrainteligencia/operaciones-de-influencia-analisis-de-inteligencia/

DNI. (2021). *GlobalTrends_2040.* Retrieved from https://www.dni.gov: https://www.dni.gov/files/images/globalTrends/GT2040/GlobalTrends_2040_for_web1.pdf

DoD. (2021). Military and Security Developments Involving the People's Republic of China. https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

DoE. (2022, 1). Russia's Top Five Persistent Disinformation Narratives. pp. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/.

Drew, D., & Snow, D. (2006). *Making Twenty First-Century Strategy - An introduction to modern National Security processes and problems.* Maxwell, Alabama, EEUU: Air University Press.

Dubois, G. (2020, 09 13). *Guerra electrónica cognitiva, el espectro electromagnético es el campo de batalla.* Retrieved from Aviacionline: https://www.aviacionline.com/2020/09/guerra-electronica-cognitiva-el-espectro-electromagnetico-es-el-campo-de-batalla/

Duperron, A. (2022). *Guerre de l'information : Comment elle agit et comment s'en protéger ?* Retrieved from https://blog.mailfence.com/fr/guerre-de-l-information-sen-proteger/#:~:text=La%20guerre%20de%20l%E2%80%99information%20vise%20%C3%A0%20employer%20des,que%20la%20guerre%20de%20l%E2%80%99information%20%28ou%20infoguerre%29%20%3F

Edward Lucas, J. M. (2021). *Information Bedlam: Russian and Chinese Information Operations During the Covid-19 Pandemic.* Retrieved from https://cepa.org/comprehensive-reports/information-bedlam-russian-and-chinese-information-operations-during-the-covid-19-pandemic/#identifier_1_12815

EFE. (2022, 10 28). Multitudinaria protesta en Praga contra el Gobierno y su apoyo a Ucrania, contra la UE y la OTAN. *Euronews*. Retrieved from https://es.euronews.com/2022/10/28/multitudinaria-protesta-en-praga-contra-el-gobierno-y-su-apoyo-a-ucrania-contra-la-ue-y-la

Elder, R. (2021, 9). *Information in Joint Operations: Insights for Commanders and Planners From Competitive Risk Modeling.* Retrieved from https://nsiteam.com/information-in-joint-operations-insights-for-commanders-and-planners-from-competitive-risk-modeling/

Elina Treyger, Joe Cheravitch, Raphael S. Cohe. (2022). Retrieved from https://www.rand.org/pubs/research_reports/RR4373z2.html

Elizondo, S. (2019). *Boletín del Centro Naval 852.* Retrieved from ESTRATEGIA DE ZONA GRIS Y LIBERTAD DE NAVEGACIÓN : https://centronaval.org.ar/boletin/BCN852/852-ELIZONDO.pdf

Ellehuus, R. (2020). *Did Russia Influence Brexit?* Retrieved from https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

EMCO . (2015). *PC 00-02 Glosario de términos de empleo militar para la Acción Militar Conjunta.* BsAs: Ministerio de Defensa.

EMCO, PC 00-01 (proyecto). (2018). *Doctrina Básica para la Acción Militar Conjunta: PC 00-01 (proyecto).* CABA: Estado Mayor Conjunto de las FFAA.

Escribano, J. C. (2022, 10 15). La posverdad en el mundo de hoy. *La Nación,* p. 34.

España Jefe de Estado Mayor de la Defensa, PDC-01 (A). (2018, febrero). *Doctrina para el Empleo de las FAS: PDC-01 (A).* (M. d.-J. España, Ed.) Retrieved junio 15, 2022, from Ministerio de Defensa: https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html

España Mando de Operaciones. (2022). *Unidades dependientes del EMAD* . Retrieved from Estado Mayor de la Defensa: https://emad.defensa.gob.es/unidades/mops/

España Ministerio de Defensa. (2018). *Doctrina para el empleo de las Fuerzas Armadas: PDC-01(A).* Retrieved from https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-pdf.html

España Ministerio de Defensa. (2019). *Entorno Operativo 2035, Ministerio de Defensa, 2019.* Retrieved from https://emad.defensa.gob.es/Galerias/CCDC/files/ENTORNO_OPERATIVO_2035_reducido.pdf

España Ministerio de Defensa, 201. (2019, diciembre). *Cuadernos de Estrategia 201 - Límites jurídicos de las Operaciones: nuevos desafíos.* (M. d.-S. Técnica, Ed.) Retrieved junio 15, 2022, from Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/cuadernos/CE_201.pdf

España Ministerio de Defensa, PDC-01. (2018). *MINISTERIO DE DEFENSA.* Retrieved from Doctrina para el empleo de las Fuerzas Armadas de España: https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-pdf.html

Facebook. (2021, 5). *The State of Influence Operations 2017-2020* . Retrieved from https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

Farrell, T., Rynning, S., & Terriff, T. (2013). *Transforming Military Power since Cold War.* Cambridge BB2 8BS: Cambridge University Press.

Farwell, J. P. (2020). *Information Warfare: Forging Communication Strategies for Twenty-first Century Operational Environments; Marine Corps University Press Quantico, Virginia; 2020.* Retrieved from https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2884442/information-warfare/

Feliú, O. L. (2012). *"La Confusa Terminología de la Seguridad y la Defensa, Instituto Español de Estudios Estratégicos, "Documento de Opinión" 06/2012.* Retrieved from http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO06-2012_ConfusaTerminologia

Feoktistov, D. (2022, Marzo 4). *Guerra con Ucrania. "A Rusia la escuchan, pero no le hacen caso", dijo el embajador ruso en la Argentina.* Retrieved from https://es.noticias.yahoo.com/guerra-ucrania-rusia-escuchan-caso-202622280.html

Figueroa, A., & Taján, G. (2018, Diciembre). La Guerra: Sustancia y Accidente ¿Las categorías son úiles? (A. Argentina, Ed.) *Revista de la Escuela de Guerra Naval* (64), 93/112. Retrieved febrero 21, 2020

Finney , N. (2020). *On Strategy: A Primer.* Fort Leavenworth, Kansas, EEUU: Combat Studies Institute Press U.S. Army.

France Ministère des Armées, L 21. (2021). *Éléments publics de doctrine militaire de lutte informatique d'influence (L21).* Retrieved from https://acteurspublics.fr/upload/media/default/0001/37/d5e6378b60c469c0133b4b726740c35403d03999.pdf

FreedomHouse. (2022, 9). *Beijing'S Global.* Retrieved from https://freedomhouse.org/sites/default/files/2022-09/BGMI_final_digital_090722.pdf

Freund, J. (1979). Observaciones sobre dos categorías de la dinámica polemógena - De la crisis al conflicto. In R. tarn, E. Le Roy Ladurie, R. Thorn, J. Freund, A. Béjin, H. Brochier, . . . E. Morin, *El concepto de crisis - Traducción de "Communications" Nro 25.* Megalópolis.

Friedman, T. L. (2022). *La invasión de Ucrania es la verdadera primera guerra mundial;* . Retrieved from https://edicionimpresa.lanacion.com.ar/la-nacion/20220405/page/6/textview

Frischknecht, F., Lanzarini, M., Alonso, R., Moya Latrubesse, E., & Hernandez Otaño, F. (1995). *Lógica, teoría y práctica de la estrategia.* (A. Argentina, Ed.) Buenos Aires: Escuela de Guerra Naval.

Galán, C. (2018). *Real Instituto Elcano, Documento de trabajo 20/2018.* Retrieved from “Amenazas híbridas: nuevas herramientas para viejas aspiraciones”, : http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CO

GALVIN, T. P. (2019). *TWO CASE STUDIES OF SUCCESSFUL STRATEGIC COMMUNICATION CAMPAIGNS.* (S. S. (SSI), Ed.) The United States Army War College. Retrieved from https://publications.armywarcollege.edu/pubs/3679.pdf

GAO. (2010, sep 10). *Hybrid Warfare.* Retrieved from https://www.gao.gov: https://www.gao.gov/assets/gao-10-1036r.pdf

GAO-22-104714. (2022, 9). Retrieved from https://www.gao.gov/assets/730/722922.pdf

Gatehouse, G. (2016). *The Russians who fear a war with the West.* Retrieved from https://www.bbc.com/news/world-europe-37766688

Gerasimov, V. (2016). The Value of Science Is in the Foresight - New Challenges Demand Rethinking the Forms and Mehods of Carrying out Combat Operations. (M. Review, Ed.) *Military Review.* Retrieved enero 2019, from https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

Gil, M. (2017). *LA INTEGRACIÓN DEL CIBERESPACIO EN EL ÁMBITO MILITAR.* Retrieved from http://www.seguridadinternacional.es/?q: http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar

Giles, Keir. (2016). *THE NEXT PHASE OF RUSSIAN INFORMATION WARFARE.* Retrieved from https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176

Gill, M., Heap, B., & Hansen, P. (2021, 9 8). *STRATEGIC COMMUNICATIONS HYBRID THREATS TOOLKIT.* Retrieved from https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

Girardi, E. (2023, mayo). Complejo Digital y Defensa Nacional. *Doctorado en Defensa* . CABA, Argentina.

Gleicher, N., Franklin, M., Agranovich, D., Nimmo, B., Belogolova, O., & Torrey, M. (2021, May). *Threat Report The State of Influence Operations 2017-2020.* Retrieved from Facebook: https://images.app.goo.gl/iE3TH4nDDEFQ36cu9

Gobierno EEUU (NSS). (2022, octubre 12). *National Security Strategy 2022.* (T. W. House, Ed.) Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Gonzáles, M. (2018, Abril 13). *https://www.xataka.com.* Retrieved from Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes: https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes

Gordon, N. (2022, 9 26). Retrieved from https://fortune.com/2022/09/26/iran-protests-starlink-internet-elon-musk-sanctions-us/

Gray, C. (1999, summer). Why Strategy is so Difficult. *Joint Forces Quaterly, Summer,* 6-12. Retrieved enero 20, 2019, from https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-22.pdf

Gray, C. (2009). Out of the Wilderness: Prime time for Strategic Culture. In J. Johnson, K. Kartchner,, & J. Larsen, *Strategic Culture and Weapons of Mass Destruction.* New York, EEUU: Palgrave mcmillan.

Grisé, M. A. (2022). *Rivalry in the Information Sphere - Russian Conceptions of Information Confrontation.* (R. Corporation, Ed.) Retrieved septiembre 5, 2022, from RAND Corporation: https://www.rand.org/pubs/research_reports/RRA198-8.html

Gualán, T. (2018). *En la era de la post-verdad.* Retrieved from https://tamya900477721.wordpress.com/2018/07/18/en-la-era-de-la-pos-verdad/

Halliday, F. (2006). *Las Relaciones Internacionales y sus debates.* FUHEM - Centro de Investigación para la Paz. Madrid: Centro de Investigación para la Paz (CIP-FUHEM).

Han, B. C. (2016). *Sobre el Poder.* Barcelona: Herder.

Han, B.-C. (2013). *El enjambre.* Barcelona: España.

Han, B.-C. (2017). *What is power?* México: Herder.

Hasbara. (2022). *Advocating for Israel and Combating Antisemitism.* Retrieved from Hasbara: https://hasbaraisrael.com

Hern, A. (2022, 9 27). *Meta takes down 'influence operations' run by China and Russia.* Retrieved from https://www.theguardian.com/technology/2022/sep/27/meta-takes-down-influence-operations-run-by-china-and-russia

Hoffman, F. (2015, octubre 5). *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War.* (T. H. Foundation, Ed.) Retrieved mayo 17, 2022, from https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray

Hoffman, F. (2020, agosto 10). *Distilling the Essence of Strategy.* (NDU, Editor) Retrieved febrero 5, 2021, from Institute for National Strategic Studies: https://inss.ndu.edu/Media/News/Article/2307863/distilling-the-essence-of-strategy/

Hoffman, Maayan. (2022). Obtenido de Cold War 2.0: Russia and Ukraine's information warfare campaigns: https://www.jns.org/cold-war-2-0-russia-and-ukraines-information-warfare-campaigns/#:~:text=Russian%20information%20warfare%20began%20weeks%20before%20the%20invasion,showing%20the%20size%20and%20strength%20of%20its%20force.

Hughes, K. (2007). *Strategic Communication and Public Diplomacy: Interagency Coordination.* Retrieved from Remarks at Department of Defense Conference on Strategic Communication: https://2001-2009.state.gov/r/us/2007/88630.htm

Huntington, S. (1995). *El soldado y el estado.* Buenos Aires : Grupo Editor Latinoamericano.

Huw Dylan, David V. Gioe and Joe Littell. (2022, 10 12). *THE KHERSON RUSE: UKRAINE AND THE ART OF MILITARY DECEPTION.* Retrieved from https://mwi.usma.edu/the-kherson-ruse-ukraine-and-the-art-of-military-deception/?fbclid=IwAR3nmaqqbRJevF4klT-AqQU_dDZJn4PfcvoKCqF-84jh07X5cal9DMHTv7Y

IISS. (2022, 10 10). *International Institute for Strategic Studies.* Retrieved from https://www.iiss.org/blogs/analysis/2022/10/russia-is-unlikely-to-use-nuclear-weapons-in-ukraine

Infobae. (2022, 9 7). *El video con el que Rusia amenaza con congelar a Europa: "El invierno será grande".* Retrieved from https://www.infobae.com/america/mundo/2022/09/07/el-video-con-el-que-rusia-amenaza-con-congelar-a-europa-el-invierno-sera-grande/

Infobae. (2022, 10 30). La estrategia propagandística de Vladimir Putin para encubrir las atrocidades cometidas en Ucrania. pp. https://www.infobae.com/america/mundo/2022/10/30/la-estrategia-propagandistica-de-vladimir-putin-para-encubrir-las-atrocidades-cometidas-en-ucrania/#:~:text=La%20estrategia%20propagand%C3%ADstica%20de%20Vladimir%20Putin%20para%20encubrir,de%20la%20mentira.

Insider. (2022). *Russian propaganda outlets have amassed a huge audience in Spanish-speaking countries.* Retrieved from https://www.insider.com/russian-disinformation-ukraine-espanol-spanish-facebook-twitter-social-media-2022-4

Insikt Group. (2022, Julio). Retrieved from https://s3.documentcloud.org/documents/22080550/ta-2022-0707-1.pdf

Institute, L. (2021, 5 5). Retrieved from https://www.lisainstitute.com/blogs/blog/socmint-inteligencia-redes-sociales

Izquierdo, L. P. (2022, 10 13). *El régimen chino se quejó ante la Armada argentina por el alquiler de un salón privado a la representación de Taiwán.* Retrieved from https://www.infobae.com/america/america-latina/2022/10/13/el-regimen-chino-se-quejo-ante-la-armada-argentina-por-el-alquiler-de-un-salon-privado-a-la-representacion-de-taiwan/

Jake Sherman & Albert Trithart. (2021, 8). *International Peace Institute.* Retrieved from Strategic Communications in UN Peace Operations: https://www.ipinst.org/wp-content/uploads/2021/08/IPI-RPT-Strategic-Communications.pdf

Janowitz, M. (1960). *El Soldado Profesinal, retrato político y social.* (B. Lerner, Ed.) BsAs, Argentina: Bibliográfica Omeba.

Japón. (2021). *Informe de seguridad de China 2021, la estrategia militar de China en una nueva era.* Instituto de Investigación de la Defensa Nacional.

Jean-Dominique Lavoix-Carli. (2022). *Information Warfare and the war in Ukraine.* Retrieved from https://redanalysis.org/2022/05/24/information-warfare-and-the-war-in-ukraine/#infowarfare

Jen Weedon, W. N. (2017, 4 27). *Information Operations and Facebook.* Retrieved from https://about.fb.com/wp-content/uploads/2017/04/facebook-and-information-operations-v1.pdf

Jessie Yeung, J. K. (2022, 9 22). Retrieved from https://cnnespanol.cnn.com/2022/09/22/mahsa-amini-protestas-iran-trax/

JGM Dec Adm 641/2021. (2021). *Requisitos mínimos de Seguridad de la Información para Organismos.* BsAs: https://www.boletinoficial.gob.ar/detalleAviso/

primera/246104/20210628.

JGM Res 1523/2019. (2019). *Definición de infraestructuras Críticas.* BsAs: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918.

JGM Res 580/2011. (2011). *Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.* Objetivos. BsAS: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-580-2011-185055/texto.

JGM Res 829/2019. (2019). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.* BsAs: https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528.

JID. (2020). *GUÍA DE CIBERDEFENSA Orientaciones para el diseño. Planeamiento, Implantación y Desarrollo de una ciberdefensa Militar.* Ontario: Copyright © 2020 Junta Interamericana de Defensa. .

Johnson, D. (2019, noviembre 02). *Review of Speech by General Gerasimov at the Russian Academy of Military Science.* Retrieved from NATO Defense College: https://www.ndc.nato.int/research/research.php?icode=585

Jones, B., & Cherif, F. (Septiembre de 2003). Evolving Models of Peacekeeping policy & responses. Nueva York, EEUU: Naciones Unidas. Obtenido de http://www.operationspaix.net/DATA/DOCUMENT/5880~v~Evolving_Models_of_Peacekeeping__Policy_Implications_and_Responses.pdf

Jordán , J. (2022). Conflicto en la zona gris y estrategias híbridas. Granada, Reino de España.

Jordán, J. (2017). "Un modelo explicativo de los procesos de cambio en las organizaciones militares. La respuesta de Estados Unidos después del 11-S como caso de estudio". *REVISTA DE CIENCIA POLÍTICA - Universidad de Granada,* 27(1), 203-226. Retrieved julio 31, 2019, from http://www.ugr.es/~jjordan/procesos-cambio-militar.pdf

Katzenstein, P. (1996). *The Culture of Natioanl Security: Norms and Identity in World Politics.* New York, New York, EEUU: Columbia University Press.

Keohane, R., & Nye, J. (1988). *Poder e Interdependencia. La política mundial en transición.* Buenos Aires, Argentina: Grupo Editor Latinoamericano.

Kiesler, J. (2021, 9 13). *Belfer Center for Science and International Affairs, Harvard Kennedy School.* Retrieved from A Next Generation National Information Operations Strategy and Architecture: https://www.belfercenter.org/publication/next-generation-national-information-operations-strategy-and-architecture

Klevering, G. (2022, 1 26). *Small Wars Journal.* Retrieved from A Brief Look at Chinese Cyberwarfare: https://smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare

Klimentyev, M. (2022, 7 28). *Are Vladimir Putin's nuclear threats a bluff? In a word – probably.* Retrieved from https://theconversation.com/are-vladimir-putins-nuclear-threats-a-bluff-in-a-word-probably-187689

Koontz , H., Weihrich , H., & Cannice, M. (2012). *Administración- Una perspectiva global y empresarial* (14° ed.). México, D.F., México: McGraw Hill.

Koribko, A. (2015). *Guerras Híbridas.* BsAs: Batalla de Ideas.

Korybko, A. (2015). *Guerras Híbridas - De las Revoluciones de colores a los golpes.* San Pablo, Brasil: Expresión Popular.

Korybko, A. (2022, 7 28). *Estados Unidos teme que los medios rusos liberen a millones de mentes latinoamericanas.* Retrieved from Boletín de Andrew Korybko: https://korybko.substack.com/p/the-us-is-scared-that-russian-media

Korybko, Andrew. (2022, Julio). *Dead Men Tell No Tales: Why Kiev Bombed Its Own Imprisoned Soldiers In Donbass.* Retrieved from https://thealtworld.com/andrew_korybko/dead-men-tell-no-tales-why-kiev-bombed-its-own-imprisoned-soldiers-in-donbass

Korybko, Andrew. (2022, Julio 28). *The US Is Scared That Russian Media Will Liberate Millions Of Latin American Minds.* Retrieved from https://oneworld.press/?module=articles&action=view&id=3115

Lantis, J. (2009). Strategic Culture: From Clausewitz to Constructivism. In ,. J. Johnson, K. M. Kartchner, & J. A. Larsen, *Strategic Culture and Weapons of Mass Destruction.* New York, EEUU: Palgrave - Macmillan.

Larson, E. (2009). *Foundations of Effective Influence Operations: A Framework for Enhancing Army.* Retrieved from https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf

Lavoix, H. (2022, 5 24). *Information warfare and the war in Ukraine.* Retrieved from https://redanalysis.org/2022/05/24/information-warfare-and-the-war-in-ukraine/

LePage, R. (2014, October). *Understanding NATO Strategic Communications.* Retrieved from https://images.app.goo.gl/UU37m6FvURkVzfGe9

Ley 26.904. (2013, dic 4). Retrieved from http://servicios.infoleg.gob.ar: /infolegInternet/anexos/220000-224999/223586/norma.htm

Liang, Q. X. (1999). *"Unrestricted Warfare".* Retrieved from https://www.oodaloop.com/documents/unrestricted.pdf

Liddel Hart, B. (2019). *Estrategia. El estudio clásico sobre la estrategia militar.* (R. Romero, Trans.) Madrid, España: Arzalia.

Lind, W., Nightengale, Schimtt, Sutton, & Wilson. (1989). El rosotro cambiante de la Guerra, hacia la cuarta generación. *Military Review, LXIX,* 2-11.

Lo, A. (2022). *Why Chinese information warfare is different from those of the US and Russia.* Retrieved from https://www.scmp.com/comment/opinion/article/3166138/why-chinese-information-warfare-different-those-us-and-russia

Loney, C. T. (2009). *Drafting a New Strategy for Public Diplomacy and Strategic Communication.* Retrieved from https://apps.dtic.mil/sti/pdfs/ADA497804.pdf

Lynn III, W. (2011, Jul 27). *https://www.bbc.com.* Retrieved from Ciberespacio: el nuevo ámbito de la guerra para el Pentágono: https://www.bbc.com/mundo/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm

Malan, M. (2018). Action adpated to circumstance: Peacekeeping doctrine and the use of force. In P. Nardin, & otros, *The use of force in Peacekeeping Operations.* Nueva York, EEUU: Rouledge. Retrieved julio 6, 2020, from https://books.google.com.ar/books?id=g8JKDwAAQBAJ&pg=PT379&lpg=PT379&dq=Nordic+UN+-

Tactical+Manual+and+use+of+force&source=bl&ots=wD3bKsdDFT&sig=ACfU3U17f7pUmkrYKFnerA55i82uAzT1KQ&hl=es-419&sa=X&ved=2ahUKEwim_dShg6rsAhV4HrkGHSk2D_sQ6AEwGnoECAwQAg#v=onepage

MANDIANT INTELLIGENCE. (2022, 10 26). Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections. pp. https://www.mandiant.com/resources/blog/prc-dragonbridge-influence-elections.

Mariel, V. (2019). *L'influence militaire pour créer la surprise dans un champ de bataille transparent ?* Retrieved from https://www.penseemiliterre.fr/ressources/30100/29/influence_militaire.pdf

Mark Laity. (2018). The Story So Far Strtaegic Communication. *The Three Swords Magazine* (33), 73. Retrieved from https://jwc.nato.int/newsroom/selected-articles-from-the-three-swords

Martin, G. (2015, Junio 15). *La paz de Westfalia y el Nuevo orden internacional.* Retrieved from https://dehesa.unex.es: https://dehesa.unex.es/bitstream/10662/3319/1/TFGUEX_2015_Galan_Martin.pdf

Martin, M. (2020). *China's Three Information Warfares.* Retrieved from US Naval Institute: https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares

Martínez Pontijas, J. (2020). *Control reflexivo: mucho más que desinformación a la rusa.* Retrieved from http://www.ieee.es/publicaciones-new/documentos-de-opinion/2020/DIEEEO159_2020JUAMAR_controlreflexivo.html

Mc Fate, S. (2019). *Las nuevas Reglas de la Victoria en la era del Desorden Permanente* (1ra ed.). (G. E. Vergara, Trans.) Buenos Aires: Circulo Militar.

McConoly. (2021, jun 21). *What is Network-Centric Warfare?* Retrieved from https://navalpost.com: https://navalpost.com/what-is-network-centric-warfare/

McMahon. (2006). *International Tables for Crystallography (2006). Vol. G, ch. 3.1, pp. 73-91.* Retrieved from General considerations when defining a CIF data item: https://onlinelibrary.wiley.com/iucr/itc/Ga/ch3o1v0001/sec3o1o1.pdf

Media Ajir, S. H. (2018). *Russian Information Warfare & Implications for Deterrence Policy.* Retrieved from https://docslib.org/doc/6225232/russian-information-warfare-implications-for-deterrence-policy

Michael Starr. (2021). *The Jerusalem Post.* Retrieved from Bennett reestablishes Public Diplomacy Directorate to coordinate Hasbara: https://www.jpost.com/israel-news/article-690014

Michelle Grisé, A. D. (2022). *Rivalry in the Information Sphere Russian Conceptions of Information Confrontation.* Retrieved from https://www.rand.org/pubs/research_reports/RRA198-8.html

Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe. (2022). Rivalry in the Information Sphere Russian Conceptions of Information Confrontation. Retrieved from https://www.rand.org/pubs/research_reports/RRA198-8.html

Mielcarek, R. (2015). *Russie: Militaires, diplomates et médias unis dans la stratégie*

d'infl uence. Retrieved from http://www.guerres-influences.com/wp-content/uploads/2017/02/DSI_111_MIELCAREK.pdf

Milosevich-Juaristi, M. (2017). *El poder de la influencia rusa: la desinformación.* Retrieved from https://media.realinstitutoelcano.org/wp-content/uploads/2017/01/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion.pdf

Miriam Matthews, K. M. (2021). *Superspreaders of Malign and Subversive Information on COVID-19.* Retrieved from https://www.rand.org/pubs/research_reports/RRA112-11.html

Moresi, A. (2018). Los ámbitos no terrestres en la Guerra futura Aeroespacio. In CESEDEN, *Los ámbitos no terrestres en la guerra futura: espacio* (pp. 57 - 169). Madrid: Ministerio de Defensa de España.

Moresi, A. (2021). Una visión sobre el conflicto presente y futuro . CABA, Argentina. Retrieved mayo 18, 2022

Motta, G. (2020). Las buenas lecturas como formadoras del liderazgo. (E. d. FFAA, Ed.) *Visión Conjunta*, 64 - 68.

MS Res 1107-E/. (2017). *Comité de Respuesta de Incidentes de Seguridad Informática del MINISTERIO DE SEGURIDAD.* BsAs: https://www.boletinoficial.gob.ar/detalleAviso/primera/172434/20171018.

Murray, W., Knox, M., & Bernstein, A. (1994). *The making of strategy-Rulers, states, and war.* (W. I. RAY, M. A. X, & A. L. N, Eds.) Cambridge, UK: Cambridge University Press.

Nabokov, V. (s.f.). *https://www.muyinteresante.es/.* (S. Romero, Ed.) Retrieved Abril 27, 2021, from https://www.muyinteresante.es/cultura/articulo/8-frases-celebres-de-vladimir-nabokov-151435834554

Nadiya Kostyuk, E. G. (2022). *The Strategist.* Retrieved from Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine: https://texasnsr.wpenginepowered.com/wp-content/uploads/2022/06/TNSR-Journal-Vol-5-Issue-3-Kostyuk-Gartzke.pdf

Nakamura, K. H. (2009). *U.S. Public Diplomacy: Background and Current Issues .* Retrieved from https://sgp.fas.org/crs/row/R40989.pdf

Nakashima, E. (2022, 19 9). *Pentagon opens sweeping review of clandestine psychological operations.* Retrieved from https://www.washingtonpost.com/national-security/2022/09/19/pentagon-psychological-operations-facebook-twitter/

NATO. (2012, November 28). *Strategic Communications: How NATO Shapes and Manipulates Public Opinion.* Retrieved from Public intelligence: https://publicintelligence.net/nato-stratcom-shaping-public-opinion/

NATO. (2018). *Inaugural Meeting of the NATO Military Committee Working Group on Strategic Communications;.* Retrieved from https://www.nato.int/cps/en/natohq/news_152567.htm?selectedLocale=en

NATO ACT. (2016). *Military Strategic Communication in Coalition Operations - A Practitioners Handbook (MilStratCom Handbook).* Retrieved from https://info.publicintelligence.net/MCDC-MilStratComHandbook.pdf

NATO CCDCOE . (2020). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* (K. F. A. Ertan, Ed.) NATO Cooperative Cyber Defense Centre of Excelence.

NATO Centre for Global Studies . (2019). *Strategic communications in the focus of Ukraine – EU – NATO.* Retrieved from https://www.kas.de/documents/270026/4625039/ENG+2019+Stratcom+in+the+focus+of+Ukraine+%E2%80%93+EU+%E2%80%93+NATO+cooperation+under+the+present+conditions.pdf/0a9670cc-6760-be1a-35d0-b87033d7cd7f?version=1.0&t=1571730247519

NATO European Centre of Excellence. (2022). *Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas.* Retrieved abril 2022, from European Centre of Excellence for countering hybrid threats: https://www.hybridcoe.fi/

NATO N19. (2019, 10 25). *Transición de la estabilización a la paz: un examen estratégico independiente de la Misión de Estabilización de las Naciones Unidas en la República Democrática del Congo.* Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/337/63/PDF/N1933763.pdf?OpenElement

NATO StratCom. (2016). *Social Media as a Tool of Hybrid Warfare.* Obtenido de http://www.stratcomcoe.org/social-media-tool-hybrid-warfare

NATO, AAP-06. (2019). Glossary of Terms and Definitions (AAP-06). Retrieved from https://www.coemed.org/files/stanags/05_AAP/AAP-06_2019_EF.pdf

NATO, AJP-01. (2017, febrero). *Allied Joint Doctrine: AJP-01.* (N. S. (NSO), Ed.) Retrieved septiembre 13, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905877/20200728-doctrine_nato_allied_joint_doctrine_ajp_01.pdf

NATO, JP 3-10. (2015, 12). Retrieved from ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS: https://cld.pt/dl/thumb/40e71e02-28d0-4c6e-b2f4-248aebd8ca49/CPOS_HERANCA/Fase%20Conjunta/Anexos/6-AEOM/%28DCM%29%20-%20Doutrina%20Militar%20Conjunta/DMC%2010%20-%20Opera%C3%A7%C3%B5es%20de%20Informa%C3%A7%C3%A3o%20%28INFO%20OPS%29/AJP-3.10-InfoOps%20Ed%2

NCSC. (2020, 2 10). *NCSC Unveils the National Counterintelligence Strategy of the U.S. 2020-2022.* Retrieved from https://www.dni.gov/index.php/ncsc-newsroom/item/2099-press-release-ncsc-unveils-the-national-counterintelligence-strategy-of-the-u-s-2020-2022?tmpl=component&print=1

Newman, N. (2000). Asymmetric Threats to British Military Intervention Operations. (R. 2000, Ed.) *RUSI Whitehall Paper 49,* 92.

Ney Fajardo, J. (S/F). *https://www.unaj.edu.ar/pueblo/re.* Retrieved from disonancias-la-desigualdad-intergeneracional-y-sus-efectos-estructurales/: https://www.unaj.edu.ar/pueblo/revista-pueblo-7/revista-pueblo-7-colaboraciones-internacionales/disonancias-la-desigualdad-intergeneracional-y-sus-efectos-estructurales/

nic.ar. (2018, Mayo). *como-se-conecta-argentina-a-internet.* Retrieved from https://nic.ar: https://nic.ar/es/enterate/novedades/como-se-conecta-argentina-a-internet

Nickels, B. (2009). Mary Kaldor. New & Old Wars: Organized Violence in a

Globalized Era. (J. o. Studies, Ed.) *Journal of Military and Strategic Studies, 12* (1), primavera.

Nietzsche, F. (2012). *Así habló Zaeatustra* (1ra ed.). Ediciones Lea, Buenos Aires: Ediciones Lea.

Nietzstche, F. (2011, octubre 26). *La gaya Ciencia* (primera ed.). (G. Cano, Trans.) Madrid, ESpaña: Gredos. Retrieved from La gaya ciencia aforimo 125 1882: https://www.dialogoexistencial.com/nietzsche-la-gaya-ciencia-%C2%A7125-1882/

Nievas, F. H. (2021, junio). Hacia una nueva geopolítica. La cuarta revolución espacial. (n. d. Germani, Ed.) *Cuadernos de Marte* (20), 395-429.

Niland, P. (2022, 10 19). *How to Deal with Russia's Nuclear Threat over Ukraine.* Retrieved from https://bylinetimes.com/2022/10/19/how-to-deal-with-russias-nuclear-threat-over-ukraine/

Nimmo, B. (2022, 9). Retrieved from https://about.fb.com/wp-content/uploads/2022/10/CIB-Report_-China-Russia_Sept-2022-1-1.pdf

Nimmo, Ben. (2022). *Meta's Adversarial Threat Report, First Quarter 2022.* Retrieved from https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

NISOS. (2022, 10 5). Russian 'Information Militia' Report. pp. https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/Nisos-Report-on-RT-Global-Information-Militia.pdf.

oasys. (2022, Jul 12). *Diferencias entre IT y OT y su convergencia.* Retrieved from https://oasys-sw.com: https://oasys-sw.com/diferencias-entre-it-y-ot/

Observatory, S. I. (2022, 8). *Unheard Voice.* Retrieved from https://purl.stanford.edu/nj914nx9540

Omelas. (2020, 12). *Minds Besieged: Digital Warfare Against the American Electorate.* Retrieved from https://www.omelas.io/mb-report.

ONTI Dispo 3/2013. (2013). *Política de Seguridad de la Información Modelo".* BsAs: https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-3-2013-219163/texto.

O'Sullivan, D. (2022, 9 27). *https://edition.cnn.com/2022/09/27/tech/meta-china-russia-influence-campaigns/index.html.* Retrieved from https://edition.cnn.com/2022/09/27/tech/meta-china-russia-influence-campaigns/index.html

Paleo, J. (2022, septiembre 27). Exposición al Curso Superior de la FFAA argentinas año 2022 . CABA.

Panarin, I. N. (2012). *The Information War Against Russia: Operation Anti-Putin.* Retrieved from https://www.schiller-institut.de/seiten/201202-berlin/panarin-english.html

Patrikarakos, D. (2017). In D. Patrikarakos, *War in 140 Characters: How social media Is Reshaping Conflict in the Twenty-First Century.* New York: Basic Books.

Paul Cornish, J. L.-F. (2011). Strategic Communications and National Strategy. https://www.researchgate.net/publication/318531532_Strategic_Communications_and_National_Strategy/link/59a8f0bca6fdcc23983885d7/download.

Paul, C. (2011). *Getting Better at Strategic Communication.* Santa Monica, CA: RAND Corporation.

Paul, C. (2020). *Artificial Intelligence and the Manufacturing of Reality.* Retrieved from https://thestrategybridge.org/the-bridge/2020/1/20/artificial-intelligence-and-the-manufacturing-of-reality

Peirano, M. (2020). *Implicaciones del ámbito cognitivo en las Operaciones Militares.* Retrieved from https://emad.defensa.gob.es/unidades/CCDC/ACTIVIDADES/2020_COGNITIVO.html#:~:text=Inevitablemente%2C%20las%20nuevas%20posibilidades%20en%20el%20intercambio%20de,de%20forma%20que%20se%20consiga%20la%20influencia%20deseada.

PEN dto 1558/2001. (2001). *Apruébase la reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.* BsAs: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm.

PEN Dto 2628/2002. (2002). *Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenci.* BsAs: http://servicios.infoleg.gob.ar/infolegInternet/anexos/80000-84999/80733/norma.htm.

PEN Dto 577/2017. (2017, jul 28). *COMITÉ DE CIBERSEGURIDAD.* Retrieved from https://www.argentina.gob.ar: https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518/actualizacion

PEN Dto457/2021DPDN. (2021, JUL 6). *Directiva Política de Defensa Nacional.* Retrieved from http://servicios.infoleg.gob.ar: http://servicios.infoleg.gob.ar/infolegInternet/anexos/350000-354999/352107/dec457.pdf

PEN Ley 25.326. (2000). *PROTECCION DE LOS DATOS PERSONALES.* BsAs: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm.

PEN Ley 25.506. (2001). *Firma Digital.* BsAs: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm.

PEN Ley 26.388. (2008). *Delitos* . Buenos Aires: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

Pepin, J. (2018, May 14). *Information Warfare Offensive.* Retrieved from Authoblog by Okta: https://auth0.com/blog/information-warfare-offensive/

Perez, C. (2022, 8). *Information Warfare In Russia's War In Ukraine: The Role of Social Media and Artificial Intelligence in Shaping Global Narratives.* Retrieved from https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

Perez, Christian. (2022). *Information Warfare in Russia's War in Ukraine The Role of Social Media and Artificial Intelligence in Shaping Global Narratives.* Retrieved from https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

PILAR, S. A. (2022). *La narrativa rusa en el laberinto de Ucrania: "Putin ha caído en la trampa de su propio discurso".* Retrieved from https://www.rtve.es/noticias/20220305/

kremlin-defiende-ley-reprime-noticias-falsas-sobre-ejercito/2302962.shtml

Platón. (1872). *Obras Completas, La Repúbliva LIBRO IV* (Vol. TOMO 7). Madrid: Patricio de Azcárate.

Polansky, M. (1965, nov 11). *https://proyectoidis.org.* Retrieved from Singularidad Tecnológica: https://proyectoidis.org/singularidad-tecnologica/

Popescu, M. M. (2020, 8 5). *STRATEGIC COMMUNICATION, NARRATIVE STRUCTURES AND THEIR IMPACT ON HUMAN BEHAVIOUR.* Retrieved from https://www.researchgate.net/publication/343448288_STRATEGIC_COMMUNICATION_NARRATIVE_STRUCTURES_AND_THEIR_IMPACT_ON_HUMAN_BEHAVIOUR/link/5f2aae8f92851cd302dce052/download

Port G1. (2022, 03 17). *Facebook remove vídeo falso de rendição do presidente da Ucrânia.* Retrieved from G1: https://g1.globo.com/tecnologia/noticia/2022/03/17/facebook-remove-video-falso-de-rendicao-do-presidente-da-ucrania.ghtml

Putnam, R. (1996). Diplomacia y política nacional: la lógica de los juegos de doble nivel. (F. P. Iglesias, Ed.) *Zona Abierta* (74), 69-120.

Qiao Liang , & Xiangsui, W. (2021). *Guerra sin Restricciones.* (A. Urricariet, Ed.) CABA, Argentina: Círculo Militar.

Qiao, L., & W. X. (1999). *La Guerra más allá de los límites.* BSAs: Traducción para enseñanza de a ESGC.

Radabaugh, G. C. (2018). The Practical Implications of Information as a Joint Function. *JFQ 89, 2nd Quarter,* 15. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89_15-17_Radabaugh.pdf?ver=2018-04-11-125441-307

RAND. (2009). *Foundations of Effective Influence Operations.* Retrieved from https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf

Rapp, William. (2015, September 1). Civil-Military Relations: The Role of MIlitary Leaders in Strategy Making. (U. A. College, Ed.) 45(3). Retrieved mayo 29, 2021, from https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2739&context=parameters

Real Academia Española. (2022). DLE. Retrieved from Real Academia Española: https://dle.rae.es/conflicto

Reggini, H. C. (2010). La comunicación sin hilos. *Coordenadas, 87.*

República Argentina Ejército Argentino, MFP 51-13. (1968). *Manual del Ejercicio del Mando: MFP 51-13.* (J. I.-O. Doctr), Ed.) Buenos Aires: Ejército Argentino, Departamento Doctrina.

República Argentina Ejército Argentino, ROB 00-01. (2015). Reglamento Básico (ROB - 00 - 01). *Conducción para las Fuerzas Terrestres,* 399. CABA, Argentina.

República Argentina EMCO, PC 00-02. (2015). *Glosario de términos de empleo militar para la Acción Militar Conjunta: PC 00-02.* República Argentina: Estado Mayor Conjunto de las FFAA.

República Argentina EMCO, PC 00-02. (2019). *Glosario de Términos de Empleo Militar para la Acción Militar Conjunta: PC 00-02.*

República Argentina EMCO, PC 20-09. (2008). Planeamiento para la Acción Militar Conjunta – Nivel Estratégico Militar.

República Argentina Ministerio de Defensa. (2014, diciembre 30). *DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL* . Retrieved from Decreto 2645/2021 ANEXO : http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/240966/norma.htm

República Argentina Ministerio de la Defensa. (2021, julio 06). DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL . *Decreto 457/2021.* CABA, Argentina: Poder Ejecutivo Nacional - MInisterio de Defensa.

Richarson, C. J. (2012). *Bridging the air Gap: an information Assurance Perspective.* Retrieved from https://www.academia.edu: https://www.academia.edu/42857545/Richardson_Thesis_Bridging_the_Air_Gap

Rosenberg, B. (2007, julio 1). Technology and leadership. (A. F. (AFJ), Ed.) *Armed Forces Journal.* Retrieved mayo 2012, from http://armedforcesjournal.com/technology-and-leadership/

Rosenberg, Confessore, & Cadwalladr. (2018, Marzo 20). La empresa que explotó millones de datos de usuarios de Facebook. New York, EEUU.

RT. (2022). Retrieved from https://actualidad.rt.com/actualidad/440884-putin-occidente-engano-naciones-pobres

Sanchez de Gallardo, M., & Nava Romero, M. (2007, septiembre - diciembre). Sistemas y barreras de la comunicación en institutos universitarios tecnológicos del municipio Cabimas. (U. d. Zulia, Ed.) *Revista venezolana de Información, Tecnología y Conocimiento,* 4(3), 71-90. Retrieved julio 1, 2020, from https://www.redalyc.org/pdf/823/82340306.pdf

Sapmaz, A. (2022, julio 27). *The Russian Federation's National Security Strategy of 2021: THE INCREASING IMPORTANCE OF INTERNAL SECURITY.* (TASAM, Editor) Retrieved agosto 15, 2022, from Turkish Asian Center for Strategic Studies: https://tasam.org/en/Icerik/70118/the_russian_federations_national_security_strategy_of_2021_the_increasing_importance_of_internal_security)

Saressalo, T. (2018). *The Evolution of the Israel Defence Forces' Information Operations: A Case Study of the Israel Defence Forces' Activities in the Information Domain 2006–2014;.* Retrieved from https://publications.waset.org/abstracts/96767/pdf

Satariano, A. (2022). *How Russia Took Over Ukraine's Internet in Occupied Territories.* Retrieved from https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html

Schmitt, C. (1984). *El concepto de lo politico.* Buenos Aires, Argentina: Folios.

Seck, H. H. (2022, julio). *Ukraine lessons take center stage in Marines' new information warfare plan.* Retrieved julio 6, 2022, from Marines Times: https://www.marinecorpstimes.com/news/your-marine-corps/2022/06/29/ukraine-lessons-take-center-stage-in-marines-corps-new-information-warfare-plan/?utm_source=sailthru&utm_medium=email&utm_campaign=marine-dnr

Shanahan, M. (2020). *The Technological Singularity.* Boston: MIT Press Essential Knowledge series.

Sheiffer, M. J. (2018, 3). U.S. Army Information Operations and Cyber - Electromagnetic Activities LESSONS FROM ATLANTIC RESOLVE. *MILITARY REVIEW ONLINE EXCLUSIVE.* Retrieved from https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Sheiffer-Atlantic-Resolve-v2.pdf

Singularity Group. (2022). *Leadership programs enterprise solutions global community.* Retrieved from CAPÍTULO III - LA GUERRA CIBERNÉTICA

Smith, R. (2007). *The Utility of Force.* New York: Alfred Knoff.

Soriano, M. R. (2022, 6 28). *Operaciones de influencia vs. desinformación: diferencias y puntos de conexión.* Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operacio

Soriano, M. R. (2022, 6 28). *Operaciones de influencia vs. desinformación: diferencias y puntos de conexión.* Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operaciones.pdf

Sosa, B. d. (2019). Reconversión de las Fuerzas Armadas. *Innovar para Defender.* Buenos Aires: Escula Superior de Guerra Conjunta.

Staff, T. J. (2009, 10 7). *Strategic Communication Joint Integrating Concept.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jic_strategiccommunications.pdf?ver=2017-12-28-162005-353#:~:text=Strategic%20communication%20is%20a%20continuous%20function%20that%20occurs,with%20general%20populaces%2C%20%20governments%2C%20and

Steiger, P. (2011). *Virtuous Influence: an imperative do solve U.S. Strategic Communicaton Quandary.* Carlisle Barracks, PA: U.S. Army War College.

Stelzenmüller, C. (2017). *The impact of Russian interference on Germany's 2017 elections.* Retrieved from https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

Steven Lee Myers y Sheera Frenkel. (2022, Agosto 13). *La propaganda rusa prospera en español, árabe y otras lenguas.* Retrieved from https://edicionimpresa.lanacion.com.ar/la-nacion/20220813/page/109/textview

Stockton, P. (2021). *DEFEATING COERCIVE INFORMATION OPERATIONS IN FUTURE CRISES.* Retrieved from https://apps.dtic.mil/sti/pdfs/AD1145324.pdf

StratCom NATO. (2019). *About Strategic Communication.* Retrieved from https://stratcomcoe.org/about_us/about-strategic-communications/1

Stupples, D. (2015, dic 3). *¿Qué es la guerra de información?* Retrieved from https://www.weforum.org: https://www.weforum.org/agenda/2015/12/what-is-information-warfare/

Sugiura, Y. (2022). *Japan National Institute for Denfense Studies.* Retrieved from China Security Report 2022: The PLA's Pursuit of Enhanced Joint Operations Capabilities: http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2022_A01.pdf

Sun, T. (2015). *El arte d ela Guerra.* (R. D. Sawyer, Ed.) BsAs: Distal.

Tatham, L. R. (2010, 8 3). *Strategic Communication & Influence Operations: Do We Really Get 'It'?* Retrieved from https://smallwarsjournal.com/blog/journal/docs-tem-

p/483-tatham-rowland.pdf

Tenenbaum, L. D. (2021). *Centre des études de sécurité.* Retrieved from Cyber influence Les nouveaux enjeux de la lutte informationnelle: https://www.ifri.org/sites/default/files/atoms/files/derochegonde_tenenbaum_cyberinfluence_2021.pdf

Tettamanti, P. A. (1995). *Uso de la Fuerza en los Conflictos Internacionales - Un análisis al final del bipolarismo.* Buenos Aires: Editorial Universidad.

Theohary, C. A. (2018). *Information Warfare: Issues for Congress, CRS Report No. R45142.* Retrieved from Washington, DC: Congressional Research Service: https://sgp.fas.org/crs/natsec/R45142.pdf

Thomas, L. (2004). *"Russia's Reflexive Control Theory and the Military". Journal of Slavic Military Studies, 17;* . Retrieved from https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

Tiirmaa-Klaar, H. (2019). diario de España. *El País.*

Timur Chabuk y Adam Jonas. (2018). *Understanding Russian Information Operations.* Retrieved from https://www.afcea.org/content/understanding-russian-information-operations

Toffler, A. &. (1994). *Las guerras del futuro.* Barcelona: Plaza Janes.

Toffler, A. (1980). *La trecera ola.* Barcelona: Plaza & Janes.

Torres Buelvas, J. (2019, Jun 27). *https://www.redalyc.org.* Retrieved from Zonas grises y delincuencia organizada transnacional: desafíos para la soberanía del Estado en América Latina: https://www.redalyc.org/journal/2739/273963960009/html/

Trama, G. A., & de Vergara, E. (2017). *Operaciones Militares Cibernéticas* (Vol. Contribución Académica). CABA: Escuela Superior Conjunta de las Fuerzas Armadas.

Tzu, S. (2015). *El Arte de la Guerra. Completo* (4ta ed.). (R. D. Sawyer, Ed.) CABA: Distal. Retrieved from https://books.google.com.ar/books?id=O1mYCgAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Tzu-ti, H. (2019, 9 28). *Taiwan most vulnerable to disinformation attacks: Swedish survey.* Retrieved from Taiwan News: https://www.taiwannews.com.tw/en/news/3786185

United Kingdom Army. (2022). *77th Brigade Influence and Outreach.* Retrieved from https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/

United Kingdom Joint Forces, JWP 3-80. (2002). *Joint Warfare Publication. Information Operations: JWP 3-80.* (J. D. Concepts, Ed.) Shirevram: Ministry of Defense.

United Kingdom MoD. (2015, agosto). *Strategic Trends Programme - Future Character of Conflict.* (M. d. Unido, Ed.) Retrieved noviembre 2021, from Development, Concepts and Doctrine Centre (DCDC): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/486301/20151210-Archived_DCDC_FCOC.pdf

United Kingdom MoD. (2019). *Joint Doctrine Note (JDN) 2/19, Strategic Communication: the Defence Contribution.* Retrieved from https://assets.publishing.

service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communic

United Kingdom MoD. (2021, marzo). *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy.* (P. M. británico, Ed.) Retrieved junio 2021, from Government of the United Kingdom: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

United Kingdom MoD. (2022, 6). *Defence Artificial Intelligence Strategy 2022.* Retrieved from https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy

United Kingdon MoD, JDP 0-01 . (2014). *UK Defence Doctrine: JDP 0-01.* Gran Bretaña: Ministerio de Defensa de Gran Bretaña.

United Nations SG. (1995). *Suplemento de Un Programa de paz: Documento de Posición del SG presentado con ocasión del cincuentenario de las Naciones Unidas-A/50/60* S/1995/1*.* Naciones Unidas. New York: Naciones Unidas. Retrieved Octubre 22, 2019, from https://digitallibrary.un.org/record/168325

United States. (2009). *Strategic Communication Joint Integrating Concept.* Department of Defense.

United States Army. (2013). *Inform and influence activities: FM 3-13.* Department of the Army.

United States Army, ATP 7-1003. (2021). *Chinese Tactics: ATP 7-1003.* Washigton D.C., EEUU: United States Army.

United States Army, FM 3-12. (2021). *Ciberspace Operations and Electromagnetic Warfare.* United States Army.

United States Army, TP525-3-1. (2018). *Pamphlets TP525-3-1 (Training and Doctrine Command).* Retrieved from TRADOC: https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

United States DoD. (2009). *Commander's Handbook for Strategic Communication and Communication Strategy.* US Joint Forces Command.

United States DoD. (2016). *Strategy for Operations in the Information Environment.* Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf?msclkid=8b3d7e29c4d811ecb0f5548c8247f365

United States DoD. (2017). *Department of Defense.* Retrieved from Doctrine for the Armed Forces of the United States: JP 1: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

United States DoD. (2020). *Military and Security Developments Involving the People's Republic of China.* Retrieved from https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

United States FBI. (2022). *Most wanted.* Retrieved from https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

United States GAO. (2022, 9). *Information Environment.* Retrieved from United States Government Accountability: https://www.gao.gov/assets/730/722922.pdf

United States Joint Chiefs of Staff, JCOIE. (2018). *Joint Concept for Operating in the Information Environment (JCOIE).* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830

United States Joint Chiefs of Staff, JCOIE JP5-0. (2017). *Joint Planning.*

United States Joint Chiefs of Staff, JP 1. (2017). *Doctrine for the Armed Forces of the United States: JP 1* (Vol. JP 1). Washington D.C., EEUU: Joint Chief of Staff.

United States Joint Chiefs of Staff, JP 2-12. (2018, June 8). *Cyberspace Operations.* (J. C. Staff, Ed.) Retrieved Julio 13, 2020, from Armed Forces of the United States. Joint Chief of Staff.: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

United States Joint Chiefs of Staff, JP 3-04. (2022, 9 14). *Information in Joint Operations: JP 3-04.*

United States Joint Chiefs of Staff, JP 3-13. (2014). *Information Operations: JP 3-13.* Retrieved from Information Operations: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

United States Joint Chiefs of Staff, JP 3-85. (2020). *Joint Electromagnetic Spectrum Operations: JP 3-85.* Joint Chiefs of Staff.

United States Jont Chiefs of Staff, JP 3-12. (2018). Cyberspace Operations.

United States Marine Corps . (2021). *The Marine Corps War College.* Retrieved from Strategy Primer; Marine Corps University; Quantico, Virginia 2021;: https://www.usmcu.edu/Portals/218/MCWAR%20Strategy%20Primer_web.pdf?ver=-h8PSZ2TTQNIwwL7Tp948A%3d%3d

United States Marine Corps, MCDP8. (2022). *U.S. Marine Corps MCDP8.* Retrieved from Information: https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf?ver=6gIvEcD0CUuPAgTSmyDNag%3d%3d

Upton, E. (1878). *The armies of Euprope an Asia.* New York.

Urban, T. (2015). *The AI Revolution: The Road to Superintelligence.* Retrieved from Wait but why : https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html

US army. (2010, Febrero 22). *Cyberspace Operations Concept Capability Plan 2016-2028* . Retrieved from https://irp.fas.org: https://irp.fas.org/doddir/army/pam525-7-8.pdf

USC Center on Public Diplomacy. (2022). *What is soft power?* Retrieved from Soft Power 30 : https://softpower30.com/what-is-soft-power/

USG. (2012). *UPDATE TO CONGRESS ON NATIONAL FRAMEWORK FOR STRATEGIC COMMUNICATION.* Retrieved from The President's National Framework for Strategic Communication (and Public Diplomacy) for 2012: https://mountainrunner.us/2012/03/national-framework-strategic-communication-public-diplomacy/

UZAL, R. (2021, Abril 28). Clase Magistral de la Maestría en Ciberseguridad y

Ciberdefensa de la Uhnivesidad de Buenos Aires . Buenos Aires, CABA, Argentina .

Van Creveld, M. (1991). *La Transformmcaión de la guerra.* Buenos Aires: Uceda.

Vilmer, P. C.-B. (2021). *LES OPÉRATIONS D'INFLUENCE CHINOISES Un moment machiavélien.* Retrieved from Institut de recherche stratégique de l'École militaire (IRSEM): http://www.councilpacificaffairs.org/ressources/les-operations-dinfluence-chinoises-un-moment-machiavelien/

von Clausewitz, C. (2021). *De la Guerra.* Barcelona, España: Obelisco. Retrieved julio 2022

Walton, C. (2022). What's Old Is New Again: Cold War Lessons for Countering Disinformation. pp. https://tnsr.org/2022/09/whats-old-is-new-again-cold-war-lessons-for-countering-disinformation/#_ftnref1.

Weber, M. (2001, agosto). *Max Weber (1919): La política como vocación.* Retrieved abril 4, 2020, from http://www.copmadrid.es/webcopm/recursos/pol1.pdf

Weiburg, A., Watts, C., & Berger, J. (2016, 11 6). *Trolling for Trump: How Russia is trying to Destroy our Democracy.* Retrieved from https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/

Wibawa, T. (2019). *Political Work Guidelines of the People's Liberation Army.* Retrieved from https://www.abc.net.au/news/2019-02-26/chinas-three-warfares-how-does-beijing-decide-who-or-what-to/10825448

Wickramarachchi, P. (n.d.). *U.S. National Strategy for Strategic Communication and Public Diplomacy.* Retrieved from https://www.academia.edu/10468705/U_S_National_Strategy_for_Strategic_Communication_and_Public_Diplomacy

Williams, P., & Bellamy, A. (2021). *Understanding Peacekeeping (Third edition).* Cambridge, Gran Bretaña: Polity Press.

Wynne, M. W. (2007). Volar y Luchar en el Ciberespacio. *Air & Space Power Journal.*

Wyrich, A. (2017, 11 1). Here are the Facebook ads Russia used in its 2016 election influence scheme. pp. https://www.dailydot.com/debug/russia-facebook-ads-2016-election/.

Yeste, M. P. (2020, 6 23). *Implicaciones del ámbito cognitivo en las Operaciones Militares.* Retrieved from Documento de Trabajo 01/2020 CESEDEN: https://emad.defensa.gob.es/unidades/CCDC/ACTIVIDADES/2020_COGNITIVO.html#:~:text=Inevitablemente%2C%20las%20nuevas%20posibilidades%20en%20el%20intercambio%20de,de%20forma%20que%20se%20consiga%20la%20influencia%20deseada.

Zavaleta Mercado, R. (2014, Jun). Los últimos cincuenta años: el tiempo del conocimiento y la violencia. *Revista de Ciencia y Cultura, 18*(32). Retrieved from http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2077-33232014000100005&lng=es&nrm=iso&tlng=es

Esta obra, *Operaciones en el Ambiente de la Información* es una contribución académica acerca del tema, elaborada en la Escuela Superior de Guerra Conjunta de las FFAA de la República Argentina.

A partir de los aportes de varios expertos, se exploran, compendian y discuten las diversas perspectivas y doctrinas de algunos de los países más avanzados, para recalar finalmente en este momento de la historia donde el dominio del campo cognitivo es esencial a cualquier estrategia que se decida implementar, no solo en ese nivel sino también en el nivel operacional y táctico.

La investigación apunta a brindar una visión interdisciplinaria que reúne, en un solo documento, aspectos de la evolución del conflicto actual y futuro en el ambiente de la información, así como sus relacionados, impacto y vínculos con la guerra electromagnética, la guerra ciberespacial y la comunicación estratégica.

Facultad Militar Conjunta
Universidad de la Defensa Nacional