La mente: Nuevo teatro de operaciones; Una mirada global de la guerra cognitiva y sus características.

Mayor (FAC) Andres Fernando Calixto Rodriguez

Artículo para optar al título profesional:

Magister en Derechos Humanos y Derecho Internacional de los Conflictos Armados

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (FAC) Andres Fernando Calixto Rodriguez
Identificación	**:**	74084652
Programa académico	**:**	Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados
Tutor metodológico	**:**	Mauricio Antonio Torres Guarnizo
Tutor temático	**:**	Mayor (R) Diego Fernando Cano Cuevas
Fecha de entrega	**:**	04 de septiembre de 2025
Extensión	**:**	8.000 palabras

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

La mente: Nuevo teatro de operaciones; Una mirada global de la guerra cognitiva y sus características.

The Mind: A New Theater of Operations; A Global Look at Cognitive Warfare and Its Characteristics.

Mayor Andres Fernando Calixto Rodriguez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo explorará la guerra cognitiva como un desafío contemporáneo que redefine la seguridad y defensa nacional más allá de los dominios físicos y de las técnicas, tácticas y procedimientos tradicionales, adentrándose de manera vertiginosa en el espacio de la mente humana y su complejidad.. A través de un análisis estructurado, se abordaran tres objetivos clave que, en conjunto, buscan ofrecer un panorama integral de esta nueva forma de conflicto y de las estrategias necesarias para enfrentarla, con el objetivo de neutralizarla, o cuando menos, mitigarla.

Palabras clave: guerra cognitiva; derechos humanos; conflicto; redes sociales; población objetivo; pensamiento complejo.

[1] Mayor de la Fuerza Aeroespacial Colombiana. Candidato a magíster en Derechos Humanos y Derecho Internacional de los conflictos armados, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Administración Aeronautica, Escuela Militar de Aviación "Marco Fidel Suarez", Colombia. Contacto: Andres.calixto@esdeg.edu.co.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Abstract: This chapter will explore cognitive warfare as a contemporary challenge that redefines national security and defense beyond the physical domains and traditional techniques, tactics, and procedures, rapidly entering the space of the human mind and its complexity. Through a structured analysis, three key objectives will be addressed, which together seek to offer a comprehensive overview of this new form of conflict and the strategies needed to confront it, with the goal of neutralizing it, or at the very least, mitigating it.

Keywords: Cognitive warfare; human rights; conflict; social media; target population; complex thinking..

Introducción

El escenario global contemporáneo se encuentra inmerso en una transformación profunda, marcada por la irrupción de las tecnologías digitales y la proliferación de la información. En este contexto, ha surgido un nuevo campo de batalla, uno donde los proyectiles no son físicos sino cognitivos: la mente humana se ha convertido en el epicentro de una contienda invisible. Como advierte la OTAN, "en la guerra cognitiva, la mente humana se convierte en el campo de batalla; el principal desafío es que es esencialmente invisible; todo lo que se ve es su impacto, y para entonces... a menudo ya es demasiado tarde" (NATO Innovation Hub, 2021). Esta modalidad de conflicto, denominada guerra cognitiva, representa un desafío sin precedentes que trasciende las concepciones tradicionales de seguridad, donde el objetivo no es dominar territorios físicos, sino conquistar percepciones, creencias y comportamientos de poblaciones enteras.

La guerra cognitiva emerge como una evolución natural de las estrategias de manipulación informativa, pero con un alcance y sofisticación sin precedentes gracias al desarrollo tecnológico actual. Universidades como Johns Hopkins y el Imperial College London definen este fenómeno como "el conflicto en el que la mente humana se convierte en el campo de batalla y cuyo objetivo es cambiar no solamente lo que la gente piensa, sino también cómo actúa, moldeando e influyendo en las creencias y los comportamientos individuales y grupales para favorecer los objetivos tácticos o estratégicos de un agresor" (Puyvelde, 2021). Este tipo de conflicto, que en su forma extrema tiene el potencial de fracturar y fragmentar sociedades enteras, se ha intensificado exponencialmente con la

expansión del ciberespacio y las redes sociales, convirtiéndose en una dimensión crítica de la seguridad nacional e internacional en el siglo XXI (Backes & Swab, 2022).

A diferencia de las guerras tradicionales que se libran en dominios físicos como tierra, mar, aire, y posteriormente el ciberespacio, la guerra cognitiva opera en un sexto dominio: el cognitivo, directamente vinculado al cerebro humano, involucrando emociones, motivos, juicios y acciones. Como señala Takagi (2022), "el control de ese espacio será la clave de las guerras futuras".

Actualmente, diversos investigadores han profundizado en la conceptualización y caracterización de la guerra cognitiva. Bernal et al. (2020) la visualizan a través de una matriz que contempla tanto la población objetivo como el propósito, señalando que puede dirigirse desde sociedades enteras hasta individuos específicos, con objetivos de desestabilización o influencia. Por su parte, Ottewell (2021) la define como "maniobras en el ámbito cognitivo para establecer una percepción predeterminada entre una audiencia objetivo con el fin de obtener una ventaja sobre otra parte", mientras que Backes y Swab (2022) la entienden como "una estrategia que se enfoca en alterar, a través de los medios de información, cómo piensa una población objetivo y, a través de eso, moldear sus actuaciones".

Para analizar este fenómeno complejo, la teoría del pensamiento complejo de Edgar Morin ofrece un marco interpretativo particularmente valioso. Como señala el propio Morin, "el pensamiento complejo es, en esencia, una estrategia que tiene intención globalizadora, es decir, que trata de abarcar todos los fenómenos de los que se es presente, pero teniéndose en cuenta sus particularidades como eventos diferentes que son" (Morin, 1990). Este concepto es diametralmente opuesto al pensamiento simplificante, que unifica todo el conocimiento a una sola visión, anulando la diversidad y conduciendo a una "inteligencia ciega", limitación

particularmente peligrosa cuando se trata de comprender fenómenos multidimensionales como la guerra cognitiva (Morin, 2005).

La teoría de la complejidad de Morin se compone como el marco teórico de esta investigación para el análisis de la guerra cognitiva debido a tres principios fundamentales: el principio de recursividad organizacional, el principio dialógico y el principio hologramático. La guerra cognitiva, como fenómeno, ejemplifica perfectamente estos principios: es recursiva porque las percepciones modificadas generan nuevas realidades que a su vez influyen en percepciones subsecuentes; es dialógica porque integra elementos aparentemente contradictorios como la verdad y la falsedad en narrativas híbridas difíciles de desmontar; y es hologramática porque cada operación de manipulación cognitiva contiene en sí mismos los elementos del sistema completo de dominación (Morin, 2005).

Desde la perspectiva de la complejidad, la guerra cognitiva no puede ser entendida como un fenómeno aislado, sino como parte de un entramado de relaciones e interacciones entre múltiples dominios. Morin (2005) propone que "la sociedad es producto de las interacciones entre individuos, pero a su vez retro-actúa sobre los individuos y los productos" (p. 67), lo que nos permite comprender cómo las operaciones de manipulación cognitiva no solo afectan las percepciones individuales, sino que transforman el tejido social completo. En este sentido, la guerra cognitiva representa lo que Morin denominaría un "fenómeno emergente", producto de la interacción entre tecnologías digitales, vulnerabilidades psicológicas, polarización social y objetivos geopolíticos.

En este contexto, surge una interrogante crucial: ¿cómo pueden las sociedades democráticas desarrollar resiliencia frente a las operaciones de guerra cognitiva sin comprometer los valores de pluralismo y libertad de expresión que las definen? Como señala

Puyvelde (2021), "en este contexto, se plantea un interrogante importantísimo: cómo resistir la manipulación cuando nos enfrentamos a una avalancha de información diseñada para provocar respuestas emocionales".

El presente capítulo se estructurará en tres secciones principales para abordar de manera exhaustiva la complejidad de la guerra cognitiva desde una perspectiva global. En primer lugar, se examinara la evolución histórica y conceptual de la guerra cognitiva, estableciendo sus diferencias con formas previas de manipulación informativa y propagandística. Posteriormente, se analizará en detalle las características y mecanismos específicos de la guerra cognitiva contemporánea, con especial atención a las tecnologías y tácticas empleadas para influir en percepciones y comportamientos. En tercer lugar, se exploraran casos concretos de operaciones de guerra cognitiva a nivel global, evaluando su impacto en diferentes contextos sociopolíticos. Todo lo anterior, discutiendo desde la teoría de la complejidad posibles estrategias de resiliencia cognitiva para individuos y sociedades, considerando la tensión fundamental entre la necesidad de protección frente a estas amenazas y el imperativo de preservar los valores democráticos de pluralismo informativo y libertad de expresión que caracterizan a las sociedades abiertas.

Metodología

El presente capítulo se desarrolla bajo un enfoque cualitativo de tipo exploratorio-descriptivo, diseñado para analizar las dimensiones conceptuales, técnicas y estratégicas de la guerra cognitiva. La elección metodológica se fundamenta en la naturaleza compleja y emergente del fenómeno, que exige un análisis interpretativo capaz de integrar perspectivas

multidisciplinares (ciencias políticas, psicología social, cibernética y teoría de la complejidad). Se emplea la **técnica de análisis documental crítico** , mediante la revisión sistemática de literatura académica, informes técnicos de organismos internacionales (OTAN, think tanks) y casos emblemáticos registrados entre 2015 y 2025. Esta triangulación de fuentes permite contrastar visiones teóricas con manifestaciones prácticas del fenómeno, asegurando una comprensión holística y contextualizada.

El **método de análisis** se estructura en tres fases: 1) *Identificación conceptual* , mediante mapeo de definiciones y características clave a partir de autores como Bernal et al. (2020), Backes y Swab (2022) y la OTAN; 2) *Deconstrucción teórica* , aplicando los principios de la teoría de la complejidad de Morin (1990, 2005) para examinar interacciones recursivas entre tecnología, cognición y poder; y 3) *Estudio de casos* , seleccionando operaciones representativas de guerra cognitiva (ej. interferencias en procesos electorales, campañas de desinformación pandémica) para evaluar patrones tácticos e impactos sociopolíticos. Se utiliza software de análisis cualitativo (NVivo) para codificar temáticamente narrativas, identificar relaciones causales y visualizar redes de influencia.

Finalmente, el marco interpretativo se articula desde la **crítica hermenéutica** , integrando el pensamiento complejo de Morin con el análisis de discurso político. Esto implica examinar cómo las operaciones cognitivas explotan antagonismos sociales (principio dialógico), generan realidades recursivas (principio de retroactividad) y fragmentan el tejido colectivo (principio hologramático). La validez se asegura mediante contraste interobservadores y triangulación metodológica, mientras que la ética se garantiza usando únicamente datos de acceso público y citando fuentes primarias sin sesgo ideológico. Este enfoque permite

desentrañar la guerra cognitiva no como un fenómeno aislado, sino como un sistema adaptativo complejo que redefine la naturaleza del poder en el siglo XXI.

La Guerra Cognitiva en el Entorno Digital: Tácticas y Técnicas de Desinformación y Operaciones de Influencia

El Nuevo Campo de Batalla Cognitivo en la Era Digital

La información ha sido históricamente un elemento crucial en los conflictos humanos, influyendo en percepciones y decisiones a lo largo del tiempo. Sin embargo, la irrupción del entorno digital y, en particular, la expansión de las redes sociales, ha transformado radicalmente la naturaleza de esta confrontación (CISA, 2023). Lo que antes se conocía como "guerra de información" o "guerra psicológica" ha evolucionado hacia un concepto más sofisticado y profundo: la **guerra cognitiva** (IT Connect, 2024).

Esta nueva dimensión del conflicto no solo busca influir en el comportamiento a través de la información, sino que tiene como objetivo último modificar la forma en que los individuos piensan, perciben la realidad y procesan la información. Ya no se trata solo de qué se piensa, sino de cómo se piensa, apuntando directamente a las estructuras cognitivas, los procesos de razonamiento y los sistemas de creencias (Pujol, 2024). Según Cano Cuevas (2024), la guerra cognitiva representa uno de los nuevos dominios de la guerra, junto con el ciberespacio y la militarización del espacio exterior, ampliando el campo de batalla más allá de los límites físicos tradicionales y situando a la mente humana en el centro del conflicto contemporáneo.

La facilidad con la que la información, tanto veraz como falsa, puede ser generada, distribuida y consumida a escala masiva ha convertido la mente humana en el campo de batalla más crítico de la era contemporánea (Cluzel, 2020). La convergencia de internet, la informática, la telefonía móvil y las redes sociales ha perfeccionado una maquinaria de comunicación de universalidad y agilidad sin precedentes, permitiendo manipular el discurso público y moldear narrativas estratégicas a gran velocidad (CISA, 2023).

En este contexto, comprender las tácticas y técnicas empleadas en la guerra cognitiva se ha vuelto imperativo para la seguridad nacional, la estabilidad social y la preservación de la democracia (Cano, 2024). Las principales tácticas y técnicas empleadas en la guerra cognitiva en el entorno digital incluyen operaciones psicológicas, operaciones de información, operaciones cibernéticas, propaganda y desinformación, abuso de plataformas alternas y manipulación de actores desprevenidos (IT Connect, 2024; EMAD, 2023; CISA, 2023). Estas estrategias buscan aumentar la polarización, promover movimientos y problemas, deslegitimar gobiernos e instituciones, aislar individuos o grupos, interrumpir actividades económicas clave y distorsionar la información (Cluzel, 2020).

La guerra cognitiva, en palabras de Cano (2024), exige el desarrollo de estrategias y capacidades específicas para enfrentar amenazas que trascienden lo físico y se insertan en el ámbito de la percepción, la información y la cognición. El ciberespacio y las operaciones de información han adquirido un papel central en los conflictos contemporáneos, permitiendo a actores estatales y no estatales manipular la opinión pública, desestabilizar adversarios y socavar la confianza en las instituciones democráticas (Cano, 2024). Además, el desarrollo de tecnologías emergentes, como la inteligencia artificial, incrementa la capacidad de los

actores para manipular la información y personalizar campañas de desinformación, aumentando el alcance y la eficacia de la guerra cognitiva (IT Connect, 2024).

Teniendo en cuenta lo anterior, la teoría de la complejidad aporta un marco de análisis para el estudio de la guerra cognitiva permitiendo abordar este fenómeno como un sistema complejo y dinámico, compuesto por múltiples elementos heterogéneos e interrelacionados que interactúan de manera no lineal y adaptativa. Desde esta perspectiva, la guerra cognitiva no puede entenderse únicamente como la suma de operaciones psicológicas, informativas o cibernéticas aisladas, sino como un entramado sistémico donde las acciones en un dominio afectan y retroalimentan otros, generando resultados impredecibles y emergentes (Morin, 1990). La complejidad organizada, entendida como un sistema con elementos articulados orgánicamente, facilita analizar cómo las estrategias de manipulación cognitiva impactan simultáneamente en individuos, grupos sociales, instituciones y estructuras políticas, configurando un escenario donde la percepción, la información y la acción se entrelazan en un continuo de influencia y resistencia (Bernal et al., 2020). Además, la teoría de la complejidad invita a integrar enfoques transdisciplinarios que incluyen la psicología, sociología, ciencia política y tecnología, reconociendo la importancia de la subjetividad y la interacción social en la construcción del conocimiento y la resistencia frente a la guerra cognitiva (Axelrod, 1997).

En cuanto a su incidencia en el Derecho Internacional de los Derechos Humanos (DIDH) y el Derecho Internacional Humanitario (DIH), la guerra cognitiva plantea desafíos inéditos que requieren una comprensión compleja y holística que se puede lograr desde los axiomas epistemológicos de la teoría de la complejidad. La manipulación sistemática de la percepción

y la información puede vulnerar derechos fundamentales como la libertad de pensamiento, expresión y acceso a la información veraz, afectando la dignidad y la autonomía de las personas (ICRC, s.f.). Al tratarse de un conflicto que no siempre se manifiesta en violencia física directa, el DIH enfrenta limitaciones para regular y proteger a las víctimas en escenarios donde la agresión se ejerce a través de la desinformación y la alteración cognitiva masiva (Randa et al., 2023). Por ello, la teoría de la complejidad contribuye a ampliar el marco conceptual jurídico, promoviendo un enfoque integral que considere la interdependencia entre los actores, las tecnologías y los contextos sociales, y que permita diseñar mecanismos normativos y operativos más efectivos para salvaguardar los derechos humanos y minimizar el daño estructural derivado de estas nuevas formas de guerra (Chávez, 2019). En suma, la complejidad epistemológica y metodológica que aporta esta teoría es clave para entender y enfrentar la guerra cognitiva en sus múltiples dimensiones, garantizando la protección integral del individuo y la estabilidad social en un mundo cada vez más interconectado y vulnerable a la manipulación cognitiva.

La Guerra Cognitiva: Más Allá de la Información y la Percepción

La guerra cognitiva constituye un nuevo paradigma para la estrategia militar y de seguridad, diferenciándose por su énfasis en el control cognitivo del adversario, a diferencia de la guerra de información, que se ocupa del flujo de datos y de la guerra psicológica, que manipula las emociones para influir en el comportamiento, en sí, la guerra cognitiva busca la "colonización" de la mente. Esta estrategia involucra la capacidad de influir directamente en cómo los individuos y las poblaciones procesan la información, toman decisiones, y construyen su percepción de la realidad (Savin, 2021). El objetivo final no es solo modificar

opiniones, sino también subvertir la capacidad de una sociedad para discernir la verdad, debilitar la confianza en las instituciones y fragmentar la cohesión social. Los ataques cognitivos, aunque no explícitamente destructivos en un sentido físico, pueden tener consecuencias devastadoras a largo plazo, erosionando la resiliencia social y la voluntad de un pueblo. Como señalan algunos expertos, la meta es "quebrar la voluntad del adversario para luchar", no mediante la fuerza bruta, sino a través de la desorganización mental y la erosión de la coherencia social (Gil de San Vicente, 2023).

A continuación, se presenta una tabla que sintetiza junto con evidencia empírica sobre ataques cognitivos en escenarios de conflicto armado y sus afectaciones a derechos fundamentales:

Autor(es) / Fuente	**Año**	**Evidencia Empírica y Contexto**	**Afectaciones a Derechos Fundamentales**
Piñeros-Ortiz, S.	2021	En conflictos armados se evidencian síntomas cognitivos y conductuales en víctimas, como miedo, agresión, hiperactividad e inatención.	Impacto en salud mental y bienestar psicológico, afectando el derecho a la salud y a la integridad personal.
Diario Las Américas (sobre Hamás)	2024	Uso de la guerra cognitiva por Hamás en Gaza mediante manipulación emocional con rehenes y videos, buscando doblegar la voluntad del adversario.	Vulneración del derecho a la dignidad, seguridad personal y protección contra tratos inhumanos o degradantes.
Cluzel, E. (OTAN)	2020	La guerra cognitiva afecta la capacidad de toma de decisiones en organizaciones militares, con ataques dirigidos a la mente humana.	Riesgo a la autonomía cognitiva y a la capacidad de decisión libre, vinculados con derechos a la libertad de pensamiento y expresión.
Comité Internacional de la Cruz Roja (CICR)	2024	Propagación de información dañina en conflictos que exacerba odio, violencia y socava el respeto al Derecho Internacional Humanitario (DIH).	Afectación a la protección jurídica en conflictos, derecho a la vida, dignidad y acceso a la información veraz.
Loaiza Agudelo, K.	2023	Perfil cognitivo alterado en víctimas del conflicto armado en Medellín, Colombia, evidenciando secuelas cognitivas y emocionales.	Afectación a derechos a la salud mental, integridad personal y protección contra daños psicológicos derivados del conflicto.
Collado, B.	2025	La guerra cognitiva de precisión emplea IA para identificar y atacar vulnerabilidades cognitivas específicas en conflictos modernos (Israel, Ucrania).	Riesgos éticos y jurídicos por ataques selectivos que pueden violar derechos a la privacidad mental, integridad psicológica y dignidad.

Ienca, M.	2021	Avances en neurotecnología plantean desafíos para derechos humanos, proponiendo nuevos derechos como libertad cognitiva y privacidad mental.	Necesidad de protección legal frente a manipulación cognitiva y vulneración de derechos emergentes relacionados con la mente humana.
Fonnegra, V. J.	2021	Violaciones a derechos humanos en conflicto armado en Colombia, incluyendo desplazamiento, saqueo y violación de derechos a la propiedad y familia por parte de grupos armados organizados.	Afectación directa a derechos civiles, políticos y sociales en contextos de violencia armada.

Fuente: Elaboración de los autores a partir de evidencia empírica recolectada.

Esta tabla refleja cómo la guerra cognitiva, a través de la manipulación informativa, emocional y tecnológica, impacta directamente en derechos fundamentales como la libertad de pensamiento, la integridad mental, la dignidad humana y la protección jurídica en escenarios de conflicto armado. La evidencia empírica recogida en diferentes contextos demuestra la necesidad urgente de fortalecer marcos legales y estrategias multidisciplinarias para mitigar estas afectaciones y proteger a las poblaciones vulnerables.

Las Redes Sociales como Vectores Principales de la Guerra Cognitiva

Las redes sociales han surgido como un espacio importante para la realización de operaciones de influencia cognitiva debido a su diseño y su impacto en la sociedad, su estructura facilita la rápida difusión de contenidos, la segmentación de audiencias y la creación de cámaras de eco y burbujas de filtro, factores relevantes para la influencia cognitiva. Los algoritmos de las plataformas, diseñados para maximizar la interacción, tienden a priorizar contenido que genera reacciones emocionales significativas, lo que puede aumentar la difusión de información errónea y narrativas polarizantes (Salas, 2021). A continuación se presenta una tabla que evidencia el uso de redes sociales en el dominio cognitivo.

Ejemplo / Caso	Evidencia de guerra cognitiva a través de redes sociales	Cita en APA 7
Manipulación de narrativas y percepciones mediante algoritmos y viralización de contenidos	Las redes sociales se han convertido en un campo de batalla donde la desinformación y la manipulación de narrativas se propagan de manera masiva, utilizando algoritmos para amplificar mensajes, polarizar sociedades y distorsionar la realidad percibida por los usuarios.	"Las redes sociales, que alguna vez fueron un faro de conexión, se convierten en el caldo de cultivo perfecto para fermentar estas prácticas de subterfugio... la desinformación se filtra como un veneno invisible, socavando los cimientos de la confianza" (IT Connect, 2024).
Campañas de desinformación y fake news en procesos electorales y conflictos	En elecciones y referendos recientes, bots y cuentas automatizadas han difundido noticias falsas y teorías conspirativas, influyendo en la opinión pública y en la toma de decisiones colectivas, como ocurrió en el Brexit, las elecciones de EE.UU. en 2016 y el plebiscito por la paz en Colombia.	"Las redes sociales se están convirtiendo en el espacio preferido de la propaganda digital o computacional y, por ende, de la desinformación y las fake news... proliferan cuentas automatizadas (bots) y noticias falsas promovidas en Internet por corporaciones y gobiernos" (Kollanyi et al., 2016; Woolley & Howard, 2017, citado en Palacio, 2018).
Polarización social y emocionalidad extrema	El diseño adictivo de las plataformas y el efecto de cámara de eco intensifican las reacciones emocionales, fomentando la polarización política y social y facilitando la propagación de rumores e imágenes violentas.	"Las redes sociales son particularmente adecuadas para empeorar la polarización política y social debido a su capacidad para difundir imágenes violentas y rumores aterradores de manera muy rápida e intensa" (Cluzel, 2020).
Ejércitos virtuales, trolls y bots en conflictos geopolíticos	Se emplean ejércitos virtuales, trolls y bots para manipular la opinión pública, crear odio, propiciar xenofobia, hundir reputaciones y desencadenar conflictos reales a partir de campañas digitales coordinadas.	"Ejércitos virtuales, trolls, campañas de desinformación, difusión de teorías conspirativas y extremistas, intervenciones ilegales en elecciones y conflictos armados… Vivimos en guerra sin saberlo" (Iriarte, 2025).
Aculturación digital y hegemonía cultural a través de redes	Las redes sociales facilitan procesos de aculturación digital, desplazando valores y estructuras identitarias nacionales por los de culturas hegemónicas, afectando la identidad colectiva.	"La guerra cognitiva tiene incidencia en el cambio de estructuras cognitivo-afectivas profundas, como los valores personales y sociales que integran el autoconcepto y la identidad en el ser humano, suplantando en la población objetivo su propia cultura por la cultura hegemónica" (Scribd, 2025).
Control de la narrativa y manipulación predictiva	El uso de algoritmos predictivos y la recolección masiva de datos permiten moldear tendencias y comportamientos sociales desde edades tempranas, facilitando el control de la narrativa y la percepción social.	"La expansión del uso de 'smartphones'... ha abierto una nueva frontera en el control de la información y la manipulación social. Mediante el uso de 'algoritmos predictivos', las grandes corporaciones tecnológicas... pueden moldear las percepciones y las decisiones de las generaciones futuras" (Portal Alba, 2024).

Fuente: Elaboración de los autores a partir de evidencias recolectadas.

Como se puede observar en la tabla. Una de las estrategias principales es la amplificación y difusión de narrativas específicas, esto se lleva a cabo mediante una combinación de cuentas automatizadas (bots), cuentas falsas (sockpuppets) y la coordinación de usuarios reales. Los bots pueden aumentar artificialmente la visibilidad de determinadas publicaciones o hashtags, mientras que las cuentas falsas se infiltran en comunidades en línea para generar discordia o promover agendas ocultas, el objetivo es crear una "ilusión de consenso" o una percepción de indignación generalizada, influenciando la percepción del público (Salazar, 2022). Estas tácticas aprovechan la tendencia humana a conformarse con la mayoría o a reaccionar ante estímulos emocionales intensos.

Las RRSS permiten el micro-targeting de individuos y grupos específicos, los operadores usan datos de usuarios (intereses, historial de navegación, conexiones sociales) para crear mensajes personalizados que explotan vulnerabilidades cognitivas o sesgos preexistentes, esta personalización extrema dificulta detectar las operaciones de influencia, ya que los mensajes están diseñados para resonar con el receptor y evadir la detección general (Giorgi & Walker, 2022). La segmentación de audiencia permite enviar mensajes contradictorios a diferentes grupos sin que sean conscientes de la incoherencia general.

Desinformación y Malinformación: Armas Fundamentales del Arsenal Cognitivo

La desinformación y la malinformación son componentes fundamentales de numerosas estrategias de la guerra cognitiva, la desinformación se define como información falsa que es creada y distribuida deliberadamente con el propósito de engañar, mientras que la malinformación se refiere a información veraz que se difunde con la intención de causar daño, generalmente alterando su contexto o distorsionando su objetivo original (Elizalde &

Polanco Fuentes, 2024). Ambas sirven como herramientas eficaces para manipular la percepción pública y provocar confusión entre la misma.

Las tácticas de desinformación son variadas y en ocasiones muy sofisticadas, por eso es imperativo empezar a entender sus dinámicas y caractizar las mismas, entre ellas se destacan:

Noticias Falsas: Inventar o distorsionar historias que imitan los medios legítimos, estas narrativas explotan sesgos y emociones como el miedo o la indignación para propagarse rápidamente.

Deepfakes y Contenido Sintético: El desarrollo de la inteligencia artificial ha facilitado la creación de videos, audios e imágenes de gran realismo que pueden ser empleados para fabricar eventos o declaraciones falsas de figuras públicas, esta tecnología constituye un reto considerable para la verificación de la verdad, dado que el contenido visual y auditivo, tradicionalmente considerado como evidencia, puede ser manipulado con facilidad (Hernández Vargas & Freitas de Souza Lima, 2023).

Manipulación del contexto: la presentación de información veraz fuera de su entorno original con el fin de provocar una interpretación incorrecta, esto puede incluir el uso de videos o imágenes antiguas para representar eventos actuales, así como la citación selectiva de algunas declaraciones.

Narrativas Divisivas y Polarizantes: Son la creación y amplificación de historias que exacerban las divisiones sociales existentes (políticas, raciales, religiosas, económicas etc.) y que demonizan a grupos con distintas porsturas, el objetivo es la fragmentación social y la imposibilidad de un diálogo constructivo.

Inoculación inversa: Se trata de difundir versiones débiles o poco creíbles de una futura narración veraz, de modo que cuando la verdad salga a la luz, el público ya esté de una u otra forma inmunizado o escéptico con el tema en particular.

Los métodos de producción y difusión de la desinformación son cada vez más sofisticados, estos incluyen redes operadas por personas, ejércitos de bots coordinados y técnicas de SEO (Search Engine Optimization) para asegurar que el contenido aparezca en los resultados de búsqueda. La rapidez con la que se propaga la desinformación a menudo supera la capacidad de los verificadores de hechos para corregirla, lo que le otorga una ventaja en el ciclo de la información.

Operaciones de Influencia y Manipulación Psicológica

Más allá de la desinformación explícita, las operaciones de influencia buscan moldear sutilmente las actitudes y comportamientos a través de la manipulación psicológica, estas operaciones se dirigen a las vulnerabilidades cognitivas inherentes a la mente humana, explotando sesgos para inducir respuestas deseadas, una técnica clave es la ingeniería social, esta se basa en la manipulación psicológica de personas para que realicen acciones o divulguen información confidencial. En el contexto de la guerra cognitiva, esto se puede manifestar a través de la creación de perfiles falsos que establecen relaciones de confianza con individuos clave para extraer información o influir en sus redes (Gavazut Bianco, 2024). Otro método es el targeting psicológico o psicográfico, alli las plataformas digitales permiten perfilar a los usuarios no solo por datos demográficos, sino también por sus rasgos de personalidad, valores, intereses y miedos. Con base en esta información, los operadores pueden diseñar mensajes que impacten profundamente en el estado psicológico de un individuo o grupo, logrando una persuasión más efectiva y subliminal. El uso de "narrativas

maestras" o "marcos cognitivos" es fundamental, en lugar de presentar hechos aislados, se construyen relatos coherentes que organizan la información de una manera particular para guiar la interpretación de la audiencia (García Servert, 2023). Estas narrativas buscan influir en el sistema de creencias subyacente, haciendo que los individuos lleguen a ciertas conclusiones por sí mismos, aunque estas conclusiones hayan sido hábilmente inducidas.

Las operaciones de influencia también se enfocan en socavar la confianza, esto implica atacar la credibilidad de las instituciones (gobiernos, medios de comunicación tradicionales, ciencia), promover la polarización extrema y fomentar el cinismo generalizado hacia cualquier fuente de autoridad o verdad. Al erosionar la confianza, se debilita la capacidad de una sociedad para responder colectivamente a las amenazas y para discernir la información fiable, dejándola más vulnerable a futuras manipulaciones, la constante exposición a la desinformación y las narrativas conflictivas puede llevar a la "fatiga de la verdad", donde los individuos se rinden ante la complejidad de discernir y optan por el relativismo o la negación.

Implicaciones y Desafíos en la Era de la Guerra Cognitiva

La omnipresencia de estas tácticas y técnicas plantea desafíos significativos, por ejemplo, la detección se hace compleja, ya que las operaciones a menudo se disfrazan de movimientos de base o de noticias legítimas, además, la velocidad de propagación de la información digital supera la capacidad de respuesta, permitiendo que la desinformación se asiente antes de ser refutada.

Para contrarrestar esta amenaza, se requiere un enfoque multifacético, la alfabetización mediática y digital es fundamental, empoderando a los ciudadanos para evaluar críticamente la información y reconocer las tácticas de manipulación; las plataformas tecnológicas tienen

la responsabilidad de desarrollar y aplicar algoritmos y herramientas más efectivas para detectar y mitigar la difusión de contenido dañino, aunque esto plantea dilemas sobre la libertad de expresión. Finalmente, los gobiernos y las organizaciones de la sociedad civil deben colaborar en la creación de resiliencia social y la promoción de la cohesión para resistir los intentos de fragmentación.

A manera de síntesis: La Resiliencia Cognitiva como Imperativo Estratégico

La guerra cognitiva en el entorno digital ha redefinido el campo de batalla, trasladándolo a la mente humana, por otra parte, las redes sociales, la desinformación y las sofisticadas operaciones de influencia son las armas principales en este nuevo tipo de conflicto, buscando no solo modificar opiniones, sino alterar los procesos cognitivos y la cohesión social. La identificación y el análisis de estas tácticas son esenciales para comprender la profundidad de la amenaza, la capacidad de una sociedad para discernir la verdad, mantener la confianza en sus instituciones y preservar la unidad ante la polarización inducida se ha convertido en un imperativo estratégico. Desarrollar la resiliencia cognitiva, tanto a nivel individual como colectivo, es la clave para navegar en este complejo paisaje de información y salvaguardar la integridad de nuestras sociedades en la era digital.

Guerra cognitiva: El asalto invisible a la opinión pública y la toma de decisiones en la era de la polarización y la desconfianza.

La proliferación de las tácticas de guerra cognitiva en el espacio digital trasciende la mera manipulación informativa; sus efectos penetran profundamente en la psique individual y en el entramado social, alterando de manera significativa la formación de la opinión pública

y los procesos de toma de decisiones tanto a nivel individual como colectivo (Álvarez, 2023). Este fenómeno se manifiesta en la intensificación de la polarización, la radicalización ideológica y la erosión de la confianza en los pilares fundamentales de la sociedad, como las instituciones democráticas, los medios de comunicación y el contrato social mismo (Bernal et al., 2020; Cluzel, 2020; Nuestro Sur, 2024). La guerra cognitiva, al explotar las vulnerabilidades inherentes de la cognición humana y las características de las plataformas digitales, se convierte en una fuerza disruptiva que afecta la cohesión social y la gobernabilidad democrática (Colom & Chaves, 2023; IT Connect, 2024).

Desde la perspectiva de la teoría de la complejidad de Edgar Morin, resulta insuficiente abordar la guerra cognitiva desde un paradigma simplificador o reduccionista, Morin advierte que los fenómenos sociales y humanos, como la manipulación de la opinión pública, requieren un enfoque multidimensional, capaz de integrar la diversidad de factores, actores y niveles de interacción implicados (Urteaga, 2010; Morin, 1993; Mentes Abiertas Psicología, 2023). La guerra cognitiva debe entenderse como un sistema complejo, donde los antagonismos (polarización, desconfianza, radicalización), no son meros efectos colaterales, sino elementos constitutivos y necesarios del sistema, que interactúan dialógicamente y generan propiedades emergentes imposibles de reducir a causas lineales (Morin, 1993). Así, la desestabilización social y la influencia sobre la opinión pública no pueden analizarse de manera aislada, sino como parte de una red de interacciones recursivas entre individuos, grupos, tecnologías y narrativas, donde el orden y el desorden coexisten y se retroalimentan (Bernal et al., 2020). Este enfoque permite comprender cómo la guerra cognitiva no solo distorsiona la realidad, sino que produce nuevas formas de sentido colectivo, legitimando incluso la violencia política o la desconfianza sistémica, como se evidenció en episodios

como el asalto al Capitolio estadounidense en 2021 (Política Creativa, 2025). En suma, la teoría de la complejidad de Morin invita a superar explicaciones unidimensionales y a reconocer la guerra cognitiva como un fenómeno dinámico, relacional y multidimensional, cuyas consecuencias solo pueden comprenderse plenamente desde una visión integradora y crítica del conocimiento (Morin, 1993; Urteaga, 2010). Partiendo de lo anterior, se presenta un análisis desde los principales ámbitos en los que se ejecuta la guerra cognitiva

Polarización Social y Fragmentación del Discurso

Uno de los efectos más evidentes y perniciosos de la guerra cognitiva es la exacerbación directa de la polarización social. Las narrativas divisivas, estratégicamente amplificadas en redes sociales y ecosistemas de información digital, funcionan como catalizadores que elevan las diferencias preexistentes en una sociedad a niveles insalvables e incluso antagónicos. Los algoritmos utilizados por las plataformas digitales para personalizar la experiencia del usuario y aumentar el *engagement* a través de la exposición a contenido que resuena con sus emociones e intereses, contribuyen involuntariamente a la creación y el fortalecimiento de "burbujas de filtro" y "cámaras de eco" (Gil Martín & Valderrama Zurián, 2022). En estos entornos informativos aislados, las personas están constantemente en contacto con información que solo confirma y refuerza sus propias creencias y sesgos, mientras se ven privadas de la exposición a opiniones y hechos que pueden ser divergentes o que pueden desafiar sus propias preconcepciones.

Esta constante reafirmación de los propios puntos de vista, sin el contrapeso de visiones críticas o alternativas, lleva a una visión del mundo sesgada, simplista y binaria: "nosotros" contra "ellos", los matices, los niveles de complejidad y las posibles áreas de concordia se pierden en un mar sin fin de lucha, parece que cada discusión o desacuerdo, por

trivial que sea, se vuelve una batalla ideológica o hasta moral, donde el "otro" deja de ser alguien con una opinión diferente y pasa al lugar de adversario e, a veces, hasta amenaza.

La capacidad de una sociedad para abordar colectivamente desafíos significativos, innovar y tomar decisiones significativas se atenúa significativamente cuando sus ciudadanos viven en realidades informativas que divergen de manera confusa, sospechan de la otra, y ven a los "otros" como enemigos, esto socava la base misma de la deliberación democrática e impulsa un estado de hostilidad crónica.

Radicalización de Posturas y Comportamientos Extremos

La exacerbación de posturas radicales y comportamientos extremos es una consecuencia directa de la polarización. La polarización extrema, que se ha exacerbado sistemáticamente a través de las operaciones de guerra cognitiva, también crea un caldo de cultivo para la radicalización (Chavarro Sánchez, 2021). Ya sea en forma directa con operaciones activamente incubadas o indirectamente afectando a los miembros pacientes y vulnerables de la población online, se ha forjado una cultura que permite que esto continúe. A medida que las personas se sumergen en cámaras de eco donde sus puntos de vista se validan y amplifican, mientras que las voces opuestas se silencian o se demonizan activamente, los puntos de vista y posiciones ideológicas tienden a radicalizarse (Flores Salgado, 2023). Las narrativas desinformativas y engañosas, a menudo cargadas de un sentido despiadado y emocional, retratan a los "otros", como opositores políticos, minorías, o ideologías rivales, como existencialmente amenazantes "otros" deshumanizados, justificando así acciones cada vez más extremas, incluidos actos de violencia.

La radicalización puede tomar múltiples formas, desde la adopción y difusión activa de ideologías extremistas y la participación y afiliación activa con movimientos marginales

y disruptivos hasta la creencia y justificación de violencia, terrorismo y desobediencia civil radical como los únicos medios para lograr objetivos políticos o sociales. Al explotar adecuadamente las vulnerabilidades psicológicas, como se ha mencionado anteriormente, los sesgos cognitivos, y más importante aún, las necesidades de pertenencia social, la guerra cognitiva aumenta dramáticamente el riesgo de que las personas que padecen otras predisposiciones o que se encuentran en situaciones especialmente vulnerables, ya sea a nivel socioeconómico o emocional, sean arrastradas a la radicalización y actúen como peones involuntarios o patrocinadores activos del desorden social.

Pérdida de Confianza en las Instituciones y la Verdad Objetiva

Efectivamente, el arma engañosa de la tolerancia y la comprensión del lado de esta arista específica de la moderna guerra cognitiva produce sus frutos casi imperceptibles, y es precisamente porque este es un proceso estructural que dura mucho tiempo, si la población no confía en los canales de información tradicionales, se siente desorientada y, por lo tanto, ultrajada por las fuentes de información sin verificar, altamente discernibles o completamente fabricadas. La desconfianza en las instituciones crea un vacío de información que las narrativas de la política alternativa, más a menudo teorías de conspiración, ocupan rápidamente de los actores hostiles (Delgado Arévalo, 2023). La continua proliferación de desinformación y contradicciones crea un ambiente de "fatiga de la verdad", donde el público, abrumado por la cantidad y cronicidad de tinta, la información conflictiva y la complejidad de determinar lo que es verdadero, relativiza, se desinteresa, el cinismo general o la creencia en cualquier cosa hecha de discursos polarizadores, la realidad carece de una base empírica en un sistema lógico en viva ebullición con malas actuaciones (Gil-Rodríguez & García-Peñalvo, 2023). Esta pérdida de confianza no solo priva a los ciudadanos de la

oportunidad de tomar decisiones informadas en su vida diaria, en los procesos electorales o en sus actividades cívicas, sino que también gradualmente socava las bases de la gobernabilidad y la cohesión social democráticas. Una sociedad donde la desconfianza se convierte en el *modus operandi* entre sus propias instituciones y ciudadanos es una sociedad más polarizada, más manejable y menos unible, eso la hace inherentemente más vulnerable a la inestabilidad política, al extremismo inherente y a la desintegración de sus normas y valores fundamentales compartidos. La disolución de un consenso sobre la realidad compartida es en muchos sentidos la ambición final y más desafiante de la guerra cognitiva, ya que crea un vacío moral e intelectual que puede llenarse con ideologías autoritarias o con una peligrosa falta de atención que erosiona las libertades y derechos performativos (Berzins, 2020).

Impacto en la Toma de Decisiones Individual y Colectiva

La combinación interdependiente y sinérgica de polarización, radicalización y desconfianza tiene un impacto directo, severo y creciente en los procesos de toma de decisiones, tanto individuales como colectivos (Echeverría & Gómez, 2024). En cuanto a las dimensiones a nivel individual, las personas, operando dentro de sus respectivas burbujas de filtro, bajo la influencia de información sistemáticamente sesgada o manifiestamente falsa y con una creciente desconfianza en las fuentes tradicionales, se encuentran en riesgo de tomar decisiones personales sobre premisas falsas o una percepción pervertida de la realidad. Esto puede oscurecer un vasto espectro de sus vidas, desde decisiones en tareas cotidianas sobre qué productos consumir y qué mensajes creer en los medios sociales, hasta decisiones cruciales de salud, inversiones financieras, elecciones laborales o, más esencialmente, cívicas, por ejemplo, votar en procesos democráticos (Franco, 2022).

En cuanto al nivel colectivo, la capacidad de una nación, comunidad u organización para simplemente tomar decisiones coherentes y efectivas en tiempos de paz o, más aun, en tiempos de crisis, se ve severamente disminuida. La incapacidad de la opinión pública para discernir la verdad o llegar a un consenso mínimo sobre los hechos hace que sea extremadamente desafiante la necesidad de políticas públicas basadas en evidencia (Acosta-Alvarez, 2024). La polarización lleva a un punto muerto en los debates políticos y sociales, en los que no se puede hacer un compromiso, una negociación y una colaboración mínimamente necesarios para abordar los desafíos unificados que toda la humanidad enfrenta, como el cambio climático, la preparación ante pandemias y la seguridad nacional (Cuervo, 2022). En escenarios de defensa y seguridad, esto se traduce en una población profundamente dividida y desconfiada sin los recursos para implementar acciones significativas en su protección o para unirse ante una amenaza externa o interna, la falta de confianza en las instituciones gubernamentales socava la legitimidad y lleva a la resistencia civil, la desobediencia y, en los peores casos, la inestabilidad política. La toma de decisiones democrática es estructuralmente frágil cuando la información basada en la que se supone que se hacen las personas y sus representantes se ha distorsionado, fragmentado y desconectado sistemáticamente de la realidad compartida, lo que lleva a un punto muerto o al surgimiento de soluciones autoritarias simples (Herrero, 2024).

Propuestas de Recomendaciones para la Detección, Análisis y Mitigación de las Amenazas a la Seguridad Nacional Derivadas de la Guerra Cognitiva

Resulta relevante analizar cada una de las variables hasta ahora mencionadas, con el fin de trazar una ruta que permita comprender de manera mas concréta las implicaciones del manejo de la información y sus derivaciones, positivas y negativas para la Seguridad

Nacional. La omnipresencia y la sofisticación creciente de la guerra cognitiva representan un desafío sin precedentes para la seguridad nacional de cualquier Estado (Puyvelde, 2021). Habiendo identificado las tácticas empleadas y analizado sus profundos efectos en la opinión pública y la toma de decisiones, se hace imperativo proponer estrategias robustas y multifacéticas para su detección, análisis y mitigación (Backes & Swab, 2022). Es asi como la naturaleza persuasiva de estas amenazas exige un enfoque que trascienda las capacidades tradicionales de defensa y seguridad, involucrando a diversos actores estatales, la sociedad civil, el sector privado y la cooperación internacional entendiendo que la resiliencia cognitiva de una nación se convierte así en un pilar fundamental de su seguridad en el siglo XXI.

Marco Estratégico General: Un Enfoque Holístico de Resiliencia Cognitiva

Para contrarrestar eficazmente la guerra cognitiva, es fundamental adoptar un marco estratégico que vaya más allá de la mera reacción y se centre en la construcción de una resiliencia cognitiva proactiva, este enfoque holístico debe reconocer que el dominio cognitivo es un campo de batalla intrínsecamente civil y que la defensa no puede ser exclusivamente militar (Centro de Innovación de la OTAN, 2021). Requiere una estrategia interinstitucional, intersectorial y colaborativa que coordine esfuerzos a nivel gubernamental, educativo, social y tecnológico.

La resiliencia cognitiva implica la capacidad de una sociedad para resistir la manipulación, discernir la verdad de la desinformación y mantener la cohesión social frente a narrativas divisivas teniendo presente que esto no se logra con censura, que socava la democracia, sino fortaleciendo las capacidades críticas de los ciudadanos y las estructuras que sostienen la información fiable. Una política de seguridad nacional adaptada a la guerra cognitiva debe entender que la mente del ciudadano es la infraestructura crítica a proteger y

que la "defensa" implica fortalecer la capacidad individual y colectiva para pensar críticamente, verificar la información y participar de manera constructiva en el debate público (Morín, 1990). Este marco debe operar bajo los principios de transparencia, libertad de expresión y protección de los derechos civiles, evitando que las medidas de mitigación se conviertan en herramientas de opresión interna, toda vez que se trata de construir una sociedad que sea epistemológicamente robusta, capaz de integrar la complejidad y resistir la simplificación binaria impuesta por las operaciones cognitivas (Morín, 2005).

Detección y Monitoreo de Amenazas Cognitivas: Inteligencia de Fuentes Abiertas y Tecnologías Avanzadas

La detección temprana es el primer eslabón en la cadena de respuesta a la guerra cognitiva, esto requiere una capacidad sofisticada de monitoreo y análisis que trascienda las metodologías tradicionales de inteligencia, las recomendaciones clave en este ámbito incluyen:

Fortalecimiento de las Capacidades de OSINT (Open Source Intelligence): Establecer unidades o centros de excelencia dedicados al monitoreo sistemático de redes sociales, foros online, medios de comunicación extranjeros y plataformas de contenidos que son generados por los usuarios. Estas unidades deben emplear analistas con habilidades lingüísticas y culturales diversas, que sean capaces de identificar patrones, narrativas emergentes, campañas coordinadas de inautenticidad y la propagación de desinformación en tiempo real. La gran cantidad de datos en fuentes abiertas es un tesoro para la detección, lo cual, exige herramientas y metodologías avanzadas para ser eficazmente procesada (Bernal, Gutiérrez & Rodríguez, 2020).

Desarrollo y Empleo de Herramientas de IA y Big Data: Invertir en tecnologías de inteligencia artificial y análisis de *big data* para automatizar la identificación de anomalías, como la actividad coordinada de bots y trolls, la detección de *deepfakes* y *cheapfakes*, la identificación de narrativas virales dañinas y el análisis del sentimiento en grandes volúmenes de texto y datos (Jaramillo Vélez, 2022). Estas herramientas actúan como una primera línea de defensa, alertando sobre actividades sospechosas que luego requieren un análisis humano más profundo partiendo de la premisa que la IA no solo es un vector de ataque, sino también una poderosa herramienta de defensa en el dominio cognitivo (Luna, 2023). Es decir que estas herramientas ayudan a alertar sobre distintas amenazas de una manera mas eficiente y clara para el ser humano. De modo, que estas tecnologías pueden ser utilizadas de manera integral tanto en defensa como en seguridad.

Creación de Redes de Alerta Temprana: Establecer mecanismos de colaboración entre agencias gubernamentales (defensa, inteligencia, seguridad cibernética, asuntos exteriores entre otros), el sector privado (empresas de tecnología y redes sociales) y organizaciones de la sociedad civil (verificadores de hechos, investigadores académicos). Esto permite compartir información de manera ágil sobre amenazas previamente detectadas y coordinar respuestas acorde a las mismas, para tal efecto un sistema de semáforo o indicadores de riesgo compartidos puede resultar beneficioso, todo esto, en atención a que la velocidad de propagación de la guerra cognitiva exige una respuesta coordinada y casi instantánea que solo puede lograrse con redes de este tipo.

Vigilancia de Infraestructuras Críticas y Procesos Democráticos: Monitoreo específico de conversaciones y actividades online que puedan amenazar la integridad de infraestructuras críticas (energía, salud, comunicaciones, defensa) o de procesos democráticos (elecciones,

consultas populares), buscando intentos de manipulación de la percepción pública sobre su seguridad o legitimidad, lo cual pone en evidencia que la protección de estos elementos es esencial para la estabilidad del Estado.

Análisis de Campañas de Guerra Cognitiva: Forense Digital y Comprensión del Comportamiento Humano

Una vez detectada una posible amenaza, es crucial realizar un análisis mas profundo para comprender su origen, sus objetivos, sus métodos y su impacto potencial, por ello las recomendaciones para el análisis incluyen:

Análisis Forense Digital y Atribución: Desarrollar capacidades para rastrear el origen de las campañas de desinformación y las operaciones de influencia, identificando a los actores detrás de ellas (Estados, grupos no estatales, sociedad civil, individuos). Esto implica el análisis de metadatos, patrones de actividad de cuentas, redes de difusión y la infraestructura técnica utilizada. La atribución, aunque difícil, es clave para la disuasión y la respuesta diplomática o legal (Ottewell, 2021). Comprender los *modus operandi* de los actores adversarios es tan importante como detectar la propia actividad.

Análisis Psicológico y Sociológico de Narrativas: Es necesario ir más allá de la detección técnica para entender cómo las narrativas de la guerra cognitiva explotan los sesgos cognitivos, las emociones humanas, las divisiones sociales y las vulnerabilidades psicológicas de la población (Takagi, 2022). Esto requiere equipos multidisciplinares con expertos en psicología, sociología, antropología y ciencias políticas, capaces de desentrañar el impacto emocional y cultural de estas campañas, toda vez que las decisiones humanas están profundamente influenciadas por la cognición, y comprender cómo esta es manipulada es fundamental (Herrero, 2024).

Modelado Predictivo: La utilización de modelos predictivos basados en datos históricos y análisis de tendencias para anticipar la evolución de las campañas de guerra cognitiva, identificar a las poblaciones o grupos más vulnerables y prever los posibles escenarios de impacto en la seguridad nacional, permite una planificación de respuesta más eficaz y proactiva.

Evaluación del Impacto Real: Desarrollar metodologías para medir el impacto real de las operaciones de guerra cognitiva en la opinión pública y en los procesos de toma de decisiones, esto va más allá de mediciones o conteos superficiales (*likes, shares*) y busca entender cambios en actitudes, comportamientos, confianza institucional y cohesión social. Por eso resulta vital cuantificar la magnitud del daño para priorizar las respuestas y asignar recursos.

Estrategias de Mitigación y Construcción de Resiliencia Nacional

La mitigación de las amenazas cognitivas no se limita a la eliminación de contenido, sino que se debe centrar en construir una sociedad más robusta y menos susceptible a la manipulación, por cuanto las recomendaciones en este ámbito son variadas y abarcan múltiples dominios así:

Alfabetización Mediática y Digital (AMD) Robusta: La educación sin lugar a dudas es la defensa escénica, implementar programas de AMD a nivel nacional, desde la educación primaria hasta la superior y en la formación continua de adultos priorizando que estos programas enseñen a los ciudadanos a evaluar críticamente las fuentes de información, reconocer sesgos cognitivos y trampas emocionales, así como a identificar diferentes tipos de desinformación (noticias falsas, *deepfakes*, manipulación de contexto), comprender el funcionamiento de los algoritmos de las redes sociales, fomentar el pensamiento crítico, la

capacidad de discernimiento y la resiliencia psicológica ante la información polarizante. Promover el uso responsable y ético de las plataformas digitales (Jaramillo Vélez, 2022). Todos estos aspectos, ayudan en si mismos a crear conciencia sobre el manejo de la información de la mano con las nuevas tecnologías, por otra parte, ayudan a generar cultura de seguridad y porevencion, una población informada y crítica es la mejor defensa.

Fortalecimiento de la Confianza Institucional y Transparencia: Combatir la desconfianza erosionando la credibilidad de las fuentes maliciosas, implica que las instituciones gubernamentales, los medios de comunicación legítimos y los expertos científicos actúen con la máxima transparencia, integridad y rigor a través de una comunicación proactiva, veraz y oportuna por parte de las autoridades, convirtiéndose en un eje crucial para construir y mantener la confianza del público. Las campañas de comunicación estratégica que expliquen procesos complejos o refuten desinformación de manera clara y sencilla, resultan también esenciales. La legitimidad percibida de las instituciones es una fortaleza cognitiva que debe ser cultivada (Franco, 2022).

Regulación Inteligente y Colaboración con Plataformas Digitales: Explorar nuevos marcos regulatorios que incentiven la responsabilidad de las empresas de redes sociales en la moderación de contenido dañino, la transparencia de los algoritmos y la identificación de cuentas inauténticas, sin caer en la censura (Gil-Rodríguez & García-Peñalvo, 2023). Es importante establecer canales de comunicación y colaboración fluidos con las plataformas para el intercambio de información sobre cualquier tipo de amenazas y la implementación de acciones correctivas ágiles, esto podría incluir la definición de estándares para la atribución de contenido sintético. Por el contrario, la autorregulación de las plataformas ha demostrado

ser insuficiente; se requiere de manera urgente un marco normativo más robusto y con un enfoque definido.

Desarrollo de Capacidades de Contrainformación y Narrativa Estratégica: La experiencia ha demostrado que no es suficiente con refutar la desinformación; es imperativo construir y promover narrativas positivas y cohesionadoras que reflejen los valores democráticos y la realidad nacional, lo cual está directamente relacionado con la capacitación y generación de cultura. Esto implica el desarrollo de capacidades de comunicación estratégica que permitan a los Estados y a la sociedad civil contar su propia historia, contrarrestar narrativas extranjeras hostiles y fortalecer la identidad nacional y la cohesión (Cuervo, 2022). La "inoculación" (exponer a las personas a versiones debilitadas de argumentos desinformativos para que desarrollen resistencia) es una técnica prometedora para fortalecer la resiliencia del público a futuras exposiciones de desinformación.

Protección de Infraestructura Cognitiva y Procesos Democráticos: Con respecto a la implementación de medidas específicas para proteger la integridad de los sistemas de información relacionados con elecciones, infraestructuras críticas y servicios públicos esenciales, se debe incluir la ciberseguridad, pero también la protección contra operaciones de influencia que buscan sembrar el caos o la desconfianza en la legitimidad de estos procesos. La defensa de la democracia pasa por la defensa de la información que la sustenta (Chavarro Sánchez, 2021).

Cooperación Internacional y Multilateral: Un Frente Unificado

La guerra cognitiva es un fenómeno transnacional que no respeta fronteras físicas, ningún país o Estado puede enfrentarla eficazmente de forma aislada, por lo tanto, la cooperación internacional y multilateral es indispensable para construir una defensa colectiva (Echeverría

& Gómez, 2024). Es así como al emplear cada medida activa o pasiva que busque mitigar los efectos de la guerra cognitiva y que, por otro lado, propenda por la coordinación entre Estados, grupos u organizaciones como mecanismo para identificar y contrarrestar diferentes amenazas, en consecuencia se deban materializar y consolidar los siguiente aspectos:

- Intercambio de Inteligencia y Mejores Prácticas: Establecer canales y mecanismos para el intercambio regular de inteligencia y contrainteligencia acerca de amenazas cognitivas entre países aliados, así como el intercambio de buenas prácticas en detección, análisis y mitigación, esto permite aprender de las experiencias de otros y fortalecer las capacidades mutuas.
- Desarrollo de Normas Internacionales: Trabajar en la creación de normas y códigos de conducta internacionales para el uso responsable del ciberespacio y el dominio cognitivo y para la administración de justicia sobre las operaciones de influencia maliciosas por parte de actores estatales o no estatales. La ausencia de un marco legal claro dificulta la disuasión y la rendición de cuentas (Flores Salgado, 2023).
- Colaboración en Investigación y Desarrollo: Fomentar la investigación coordinada en nuevas tecnologías de detección y contramedidas, así como en la comprensión de la psicología y la sociología de la guerra cognitiva, toda vez que la naturaleza evolutiva de estas amenazas exige una innovación constante.
- Apoyo a la Sociedad Civil Global: Financiar y apoyar a organizaciones de la sociedad civil, periodistas de investigación y verificadores de hechos que trabajan en la primera línea de la lucha contra la desinformación a nivel global, no hay que desconocer que

estos actores son cruciales para la resiliencia democrática y con frecuencia tienen una agilidad que las estructuras estatales no poseen.

La puesta en práctica de estas recomendaciones implica una considerable inversión en recursos, tecnología y talento humano especializado, al mismo tiempo, requiere un cambio cultural y conceptual, al reconocer que la seguridad y defensa nacional contemporánea se desarrolla tanto en el ámbito informativo y cognitivo como en los dominios tradicionales. El futuro de la democracia y la estabilidad global dependerá en gran medida de nuestra capacidad colectiva para construir sociedades cognitiva y socialmente resilientes (Delgado Arévalo, 2023).

Conclusiones

En primer lugar, hemos analizado las tácticas y técnicas que impulsan la guerra cognitiva, destacando cómo se despliega a través de las operaciones de influencia y la desinformación en el entorno digital, se evidencia que estas tácticas no son accidentales; se trata de campañas psicológicas y sociales diseñadas para explotar los sesgos cognitivos y las vulnerabilidades de la sociedad, utilizando plataformas como las redes sociales para amplificar narrativas que polarizan, radicalizan y erosionan la cohesión, la distinción entre bots, trolls, deepfakes y la manipulación de la narrativa son fundamentales para comprender el arsenal utilizado en este nuevo campo de batalla.

En segundo lugar, el análisis se centró en establecer los efectos de estas operaciones, revelando el profundo impacto que tienen en la formación de la opinión pública y en los procesos de toma de decisiones, se observa cómo la desinformación masiva y coordinada no

solo distorsiona la percepción de la realidad, sino que también genera una profunda desconfianza en las instituciones gubernamentales y en los medios de comunicación legítimos. Esta pérdida de confianza es el efecto mas insidioso de la guerra cognitiva, ya que deslegitima los pilares del Estado y de la democracia, dejando a la población vulnerable a futuras campañas de influencia.

Finalmente, el capítulo explora un conjunto de **recomendaciones estratégicas** para la detección, análisis y mitigación de estas amenazas. Se expone un enfoque holístico que combina la inversión en capacidades de inteligencia de fuentes abiertas (OSINT) y el uso de tecnologías de inteligencia artificial para la detección temprana. Sin embargo, la defensa más fundamental radica en la construcción de la resiliencia cognitiva a nivel social, esto implica una apuesta firme por la alfabetización mediática y digital, el fortalecimiento de la confianza institucional a través de la transparencia y la colaboración con el sector privado, así como la promoción de narrativas estratégicas que contrarresten la desinformación.

En definitiva, la guerra cognitiva representa una amenaza multidimensional que no puede ser abordada únicamente con soluciones unilaterales, se requiere una respuesta integral y coordinada que involucre tanto a los organismos de defensa y seguridad como a la sociedad civil. La capacidad de un Estado para proteger su soberanía en la era digital dependerá, en gran medida, de su capacidad para educar a sus ciudadanos, fortalecer sus instituciones y defender la integridad de la mente humana frente a las operaciones de influencia hostiles.

Referencias

Acosta-Alvarez, J. (2024). *Más allá de la IA: el lado oscuro de la mente detrás de la guerra cognitiva.*

Álvarez, D. D. (2023). *La guerra cognitiva y la manipulación de la mente en la era digital.* Editorial GEU.

Álvarez, J., Bernal, F., & Cano, D. F. (2017). La guerra cognitiva y nuevas formas de amenazas a la paz y a la seguridad y la defensa nacionales. *KAS - ESDEG*.

Backes, M., & Swab, R. (2022). Guerra cognitiva: el futuro del conflicto. *Revista de Guerra de la Información, 21*(1), 45-60.

Bernal, J., Gutiérrez, L., & Rodríguez, P. (2020). Guerra cognitiva: Caracterización y retos para la seguridad nacional. *Revista de Estudios en Seguridad y Defensa, 12*(2), 67-89.

Berzins, J. (2020). *Russian New Generation Warfare: Theory, practice, and lessons for EU defence.*

Cano Cuevas, D. F. (2024). Desafíos de la seguridad humana en los nuevos dominios de la guerra. *Novum Jus, 18*(3), 41-68.

Centro de Innovación de la OTAN. (2021). *Guerra cognitiva.* https://www.innovationhub-act.org/sites/default/files/2021-08/cognitive-warfare.pdf

Chavarro Sánchez, N. (2021). *Amenaza híbrida y guerra cognitiva: El desafío de proteger la soberanía y la democracia en Colombia.* Universidad Militar Nueva Granada.

CISA. (2023). *Tácticas de desinformación.*

Cluzel, E. (2020). *Guerra cognitiva*. Centro de Innovación.

Collado, B. (2025). *Guerra cognitiva de precisión: El nuevo frente invisible en los conflictos modernos.* CEPI - UBA.

Colom, G., & Chaves, A. (2023). *Nuevos espacios estratégicos y cognitivos: de la guerra de la información a la guerra cognitiva.*

Comité Internacional de la Cruz Roja (CICR). (2024). *¿Por qué al CICR le preocupa la difusión de "información dañina" en la guerra?* Recuperado de https://blogs.icrc.org/law-and-policy/es/2024/09/26/por-que-al-cicr-le-preocupa-la-difusion-de-informacion-danina-en-la-guerra/

Cuervo, J. (2022). Una aproximación a la guerra cognitiva y las operaciones de información. *Cuadernos de Estrategia*, (210), 133-154.

Delgado Arévalo, E. M. (2023). *Guerra cognitiva y el escenario híbrido: Desafío para la seguridad y defensa del Estado.*Universidad Militar Nueva Granada.

Diario Las Américas. (2024). El terror de Hamás y la guerra cognitiva. *Diario Las Américas*. Recuperado de https://www.diariolasamericas.com/opinion/el-terror-hamas-y-la-guerra-cognitiva-n5363585

Echeverría, D., & Gómez, I. (2024). La guerra híbrida y su evolución hacia la guerra cognitiva. *Estudios Estratégicos*, (54), 1-15.

Elizalde, R. M., & Polanco Fuentes, R. (2024). De la guerra fría a la guerra cognitiva, el caso de Cuba. *Revista de Cooperación*, (25).

EMAD. (2023). *Implicaciones del ámbito cognitivo en las Operaciones Militares.*

Flores Salgado, E. P. (2023). La guerra cognitiva y la desinformación como elementos clave en la geopolítica actual. *Revista Iberoamericana de Estudios de Desarrollo, 12*(1), 1-20.

Fonnegra, V. J. (2021). Violaciones a los derechos humanos en el conflicto armado. *Corte Interamericana de Derechos Humanos*. Recuperado de https://www.corteidh.or.cr/tablas/r34451.pdf

Franco, R. (2022). *La guerra de cuarta generación y la guerra cognitiva: Un análisis comparativo.*

García Servert, R. (2023). *La guerra de la información, el dominio cognitivo: Apuntes para una reflexión pendiente*[PDF]. Academia de las Ciencias y las Artes Militares.

Gavazut Bianco, L. E. (2024). Guerra Cognitiva, Aculturación Hegemónica y Espacios de Comunicación No Digitales. *Kaikará – Revista de Comunicación para la Liberación, 1*(1).

Gil de San Vicente, I. (2023). *Vencer en la guerra cognitiva*. [Conferencia]. Universidad Internacional de las Comunicaciones, Caracas.

Gil Martín, G. A., & Valderrama Zurián, J. (2022). *El impacto de las redes sociales en la guerra cognitiva: Un estudio de caso.*

Gil-Rodríguez, I., & García-Peñalvo, F. J. (2023). *Desinformación y contrainformación en la era digital: Retos y oportunidades.*

Giorgi, L. M., & Walker, M. S. (2022). Guerra Cognitiva. *Año 14, Número 27*, 9-17.

Hernández Vargas, J. R., & Freitas de Souza Lima, L. (2023). *Transición del orden mundial: impactos en las estrategias de seguridad y defensa en Colombia y la región.* KAS - ESDEG.

Herrero, M. (2024). *Guerra cognitiva: Anatomía de la persuasión y el control mental.*

Ienca, M. (2021). Hacia nuevos derechos humanos en la era de la neurotecnología. *Redalyc*. Recuperado de https://www.redalyc.org/journal/3400/340067606006/html/

Iriarte, D. (2025). *Guerras cognitivas.* Arpa Editores.

IT Connect. (2024). *Guerra Cognitiva: Narrativas y Desinformación en el siglo 21.*

Jaramillo Vélez, L. M. (2022). *Comunicación estratégica y guerra cognitiva: Herramientas para la defensa nacional.*

Kollanyi, B., Howard, P. N., & Woolley, S. C. (2016). Bots and automation over Twitter during the US election.

Loaiza Agudelo, K. (2023). *Perfil cognitivo en personas víctimas del conflicto armado.* [Tesis de pregrado]. Repositorio TDEA. https://dspace.tdea.edu.co/bitstream/handle/tdea/3198/HOLGU%C3%8DN%20DIOSSA.docx.pdf

Luna, A. (2023). *La inteligencia artificial en la guerra cognitiva: Amenazas y defensas.*

Morín, E. (1990). *Introducción al pensamiento complejo.* Gedisa.

Morín, E. (2005). *El método 1: La naturaleza de la naturaleza.* Cátedra.

Ottewell, P. (2021). Guerra cognitiva: el nuevo campo de batalla. *Estudios de Defensa, 21*(3), 234-249.

Palacio, M. (2018). *Informe Anual de la Profesión Periodística.*

Piñeros-Ortiz, S. (2021). Consecuencias de los conflictos armados en la salud mental. *Revista Colombiana de Psiquiatría, 50*(3), 424-432. https://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-41572021000300424

Política Creativa. (2025). *Conceptos sobre las guerras cognitivas.*

Portal Alba. (2024). *Guerra cognitiva y control de la información.*

Pujol, I. (2024). Guerra cognitiva: Un nuevo campo de batalla. *Revista Española de Defensa.*

Puyvelde, D. V. (2021). Guerra cognitiva y el futuro del conflicto. *Security Studies Review, 29*(1), 12-21.

Ruiz, J. L. S. (2019). *El pensamiento complejo de Edgar Morin en acción.*

Salas, A. (2021). *Contrarrestar la guerra cognitiva: conciencia y resiliencia.* Johns Hopkins University & Imperial College London.

Salazar Pérez, R. (2022). *En la era de Guerra Cognitiva: Cómo construir socialmente al enemigo.* Universidad Autónoma de Sinaloa.

Savin, L. (2021). La OTAN desarrolla nuevos métodos de guerra cognitiva. *Rebelión.*

Scribd. (2025). *Guerra Cognitiva como Proceso de Aculturación Hegemónica.*

Takagi, K. (2022). El dominio cognitivo: clave para la guerra futura. *Asia-Pacific Review, 29*(2), 89-104.

Urteaga, E. (2010). La teoría de la complejidad de Edgar Morin: contribuciones y límites. *Diálogo Filosófico, 78*, 477-490.