

La guerra cognitiva y nuevas formas de amenazas a la paz y a la seguridad y la defensa nacionales

DOI: <https://doi.org/10.25062/9786287602489.14>

Jorge Ricardo Hernández Vargas*

Leonardo Freitas de Souza Lima†

Introducción

*La victoria sonríe a quienes anticipan el cambio
en el carácter de la guerra, no a quienes esperan para adaptarse
después de que ocurren los cambios.*

Giulio Douhet

La cuarta revolución industrial, o revolución informática y digital, y las nuevas tecnologías derivadas de la misma están cambiando significativamente la forma en que se relacionan, interactúan, comunican, perciben y sienten las personas, lo que permite un cambio en el

* Brigadier general del Ejército de Colombia, del arma de ingenieros. Ingeniero civil, profesional en Ciencias Militares, magíster en Ciencias Militares de la Escuela de Estudios Avanzados del Ejército de los Estados Unidos (SAMS, por sus siglas en inglés), en Fort Leavenworth (Kansas); magíster en Seguridad de la Universidad Webster, en San Luis (Misuri); y magíster en Estrategia de Seguridad Nacional de la Universidad de Defensa de los Estados Unidos, en Washington D.C. Contacto: ricardohervar70@hotmail.com.

† Coronel de la Fuerza Aérea Brasileña, de la especialidad de intendencia. Profesional en Ciencias de Logística con habilitación en Intendencia de la Aeronáutica, especialista MBA en Gestión Pública y en Planeamiento y Gestión Estratégicos, curso de Comando y Estado Mayor de la Fuerza Aérea Brasileña, especialista en Geopolítica y Relaciones Internacionales y magíster en Seguridad y Defensa de la Escuela Superior de Guerra de Colombia. Contacto: leogeopolbra@gmail.com.

carácter de la guerra y, por ende, la aparición de un nuevo tipo de guerra: la guerra cognitiva. Aunque las estrategias de propaganda e influencia siempre han existido, la sofisticación de las nuevas tecnologías digitales y el uso cada vez más generalizado de las redes sociales han hecho posible que actores estatales, no estatales e independientes, lleguen a audiencias más amplias con contenido personalizado y en tiempo real. La guerra cognitiva lleva enfoques conocidos y novedosos dentro de la información, la cibernética y la guerra psicológica a un nuevo nivel, al intentar no solo alterar la forma en que piensan las personas, sino también cómo reaccionan ante la información. Además, los métodos de guerra cognitiva desdibujan las líneas entre objetivos civiles y militares y podría decirse que cambian la aplicación de la fuerza de los dominios físicos a los virtuales.

Así las cosas, las líneas de la guerra en el siglo XXI se están volviendo cada vez más delgadas. Los desafíos a la seguridad y a la defensa de los Estados no solamente incluyen guerras entre ellos, conflictos de contrainsurgencia, terrorismo y combinaciones de estos, sino también guerras en el dominio cognitivo. La superioridad militar convencional de un país, al menos en el futuro inmediato, no garantizará vencer en este nuevo tipo de guerra y estos desafíos no se pueden enfrentar únicamente a través del uso del instrumento de poder militar de una nación. Lo ideal sería lograr anticipar el cambio del carácter de la guerra y diseñar la estrategia adecuada por medio de la articulación tanto de los instrumentos (diplomático, informacional, militar y económico) y elementos de poder nacional (capital humano, industria, economía, tecnología, investigación y desarrollo, infraestructura, cultura, gobernanza, deseo nacional y reputación internacional) para mantener a salvo los intereses nacionales.

Puesto que el contexto estratégico nos muestra que la guerra cognitiva ya está siendo empleada por diferentes actores, se hace imperativo que los estrategas en defensa y seguridad entiendan que la guerra se puede librar en un nuevo dominio, el cognitivo, y que esto los obliga a identificar los nuevos roles y desafíos que este tipo de guerra representa para las naciones. Por lo anterior, deben establecer las medidas necesarias para hacerle frente, de manera tal que, en un conflicto enmarcado dentro del dominio cognitivo, los Estados y sus fuerzas militares desempeñen un papel esencial en la defensa de los intereses de una nación frente a este tipo de guerra.

En este orden de ideas, el presente capítulo se desarrollará en cuatro grandes segmentos. El primero aborda los marcos conceptuales y teóricos relacionados con la descripción de las guerras de quinta generación, la guerra cognitiva y sus diferentes componentes. En el segundo, se analiza la guerra cognitiva y las nuevas amenazas para la seguridad y la defensa nacionales. El tercero aborda el impacto de la guerra cognitiva en Colombia, una posible estrategia para combatirla y la descripción de las capacidades con que cuentan las Fuerzas Militares para combatir este tipo de guerra. Y el cuarto y quinto corresponden a las conclusiones y recomendaciones, respectivamente.

El nuevo carácter de la guerra: la guerra cognitiva, determinando el problema

La primera y más importante evaluación y precisión que tiene que hacer un comandante es determinar qué tipo de guerra está emprendiendo.

Carl von Clausewitz

En su magistral obra sobre la guerra, el teórico militar prusiano Carl von Clausewitz (1989) escribió: “la guerra es más que un verdadero camaleón que adapta ligeramente sus características según sea el caso” (p. 89). Y continuó afirmando que las características de la guerra están directamente relacionadas con las condiciones políticas, económicas, sociales y militares, las cuales le imprimen un carácter único a cada conflicto. Mas recientemente, los estudiosos de los conflictos modernos como Álvarez, Santafé y Urbano (2017) coinciden con Clausewitz, pero proponen que el nuevo cambio en el carácter de la guerra obedece al impacto de las nuevas tecnologías y cómo estas influyen en las ideas de las personas.

Teniendo en cuenta lo anterior, para que los líderes civiles y militares puedan determinar el carácter o tipo de guerra que representa la guerra cognitiva, se hace necesario, en primer lugar, definir qué son las guerras de quinta generación.

Las guerras de quinta generación, G5G

El concepto de las generaciones de la guerra fue creado por un equipo de analistas de los Estados Unidos, que incluyó a William S. Lind, y tuvo como propósito argumentar que el carácter de la guerra es cambiante y se deriva de factores como los dominios¹, las tácticas, las técnicas, el armamento y los objetivos a alcanzar (Lind, Nightengale, Schmitt y Sutton, 1989).

En 1999, los coroneles Qiao y Wang, del Ejército Popular de Liberación Chino, pronosticaron en su obra *Guerra sin restricciones*, el advenimiento de un nuevo tipo de guerra, caracterizada por el aumento de violencia política, violencia económica y tecnológica que, según los autores, podría ser más devastadora que una guerra convencional (Qiao y Wang 1999). Es decir, los coroneles ya dilucidaban el surgimiento de la guerra de quinta generación (G5G).

Después, Abbott (2010) ratificó el pronóstico de los coroneles chinos y estableció una primera aproximación al concepto de G5G al definirla como aquella que se ejecuta principalmente a través de acciones militares no cinéticas, como la ingeniería social, la desinformación y los

1 Se conoce comúnmente como dominio de la guerra al espacio en el cual esta se desarrolla. Los dominios pueden ser terrestres, marítimos y aeroespaciales, pero recientemente se han incorporado el dominio ciberespacial y el cognitivo.

ataques cibernéticos, apalancada por tecnologías emergentes como la inteligencia artificial y los sistemas totalmente autónomos, es decir, una guerra de información y percepción.

Más adelante, Schmid (2013) amplió este concepto y estableció que la G5G se caracteriza por su omnipresencia y el hecho de que las personas que participan en ella no necesariamente usan la fuerza militar, sino que emplean una combinación de fuerza cinética y no cinética.

Por su parte, Álvarez *et al.* (2017) afirmaron que las nuevas guerras han dejado su estilo tradicional para transformarse en un estado de conflicto colectivo y organizado, que puede desarrollarse a través de hostilidades violentas y no violentas, es decir, guerras de quinta generación.

Del mismo modo que las diferentes definiciones acerca de la G5G, la tipología de la guerra también nos ayuda a definir este concepto, por medio de la clasificación de los diferentes tipos de guerras y con base en factores tales como las tácticas, las técnicas, la doctrina, el equipo, los recursos humanos y técnicos, el mecanismo de derrota, el objetivo que persiguen y el dominio en que se desarrollan las guerras. Una mejor clasificación de los tipos de guerras fue la planteada por Álvarez *et al.* (2017), quienes establecieron cuatro ejes sobre los cuales se categorizan las guerras.

La figura 1 describe, en primer lugar, el eje A, correspondiente a los escenarios en donde se desarrollan las G5G, los cuales son del orden físico, de información y cognitivo. El escenario físico incluye los dominios terrestres (con énfasis en las ciudades), marítimo y aeroespacial; el escenario de la información que incorpora el dominio cibernético; y el escenario cognitivo y social que abarca también el dominio político. En segundo lugar, el eje B describe la naturaleza del adversario consistente en supracombinaciones de actores estatales, no estatales e independientes², quienes desarrollan acciones de fuerza (cinéticas) y de no fuerza (no cinéticas) en los ya mencionados escenarios físico, de información y cognitivo, buscando una ventaja táctica o estratégica. En tercer lugar, el eje C, correspondiente a los objetivos que persiguen las G5G que pretenden hacer que el adversario colapse internamente por la inercia de sus organizaciones, a través de la implosión como mecanismo de derrota³. Finalmente,

2 El Departamento del Ejército de Estados Unidos (2010) clasifica los actores en estatales y no estatales y, dentro de estos últimos, incluye a los actores independientes. Los actores estatales están conformados por los Estados plenamente reconocidos por la comunidad internacional, mientras que los actores no estatales son aquellos que no representan a una nación en particular tales como grupos guerrilleros, terroristas y crimen organizado, entre otros. Los actores no estatales incluyen un subgrupo denominado actores independientes, que incluye a las ONG, las compañías transnacionales y los medios de comunicación, entre otros.

3 De Cheg (citado en Álvarez, 2017) plantea analizar las redes y supracombinaciones como procesos, en lugar de instituciones o estructuras, y de esta manera atacar sus subprocesos, incluyendo el desarrollo del liderazgo; la construcción de alianzas; el alcance público e ideológico; la adquisición de fondos, material y apoyo; el reclutamiento; el adoctrinamiento y la capacitación del personal; la planificación y focalización; la movilización y las operaciones; las comunicaciones; y la explotación de los resultados. Por lo tanto, el ataque contra los subprocesos de un ejecutor de G5G podría llevarse a cabo por cualquier medio, sea este militar o no militar, letal o no letal, cinético o no cinético, lo cual conlleva a que los esfuerzos del oponente sean irrelevantes, hasta el punto de que se vuelva vulnerable a la implosión por inercia o parálisis.

el eje D establece el carácter de la guerra de las G5G, que se caracteriza por ser una guerra irrestricta, que emplea fuerza cinética (violencia) y no cinética (no violencia).

Figura 1. Ejes de categorización de las guerras



Fuente: adaptado de Álvarez *et al.* (2017).

Una vez definidas las G5G y su componente cognitivo, podemos continuar con el marco conceptual y teórico de la guerra cognitiva, sus componentes, su relación con el ambiente urbano y los objetivos que esta persigue.

Entendiendo la guerra cognitiva

Las razones que favorecieron la aparición de la guerra cognitiva están estrechamente relacionadas con la convergencia de internet, la informática, la telefonía móvil y las redes sociales, las cuales representan la perfección de una maquinaria de comunicación de tal universalidad, omnipresencia y agilidad, que brinda la posibilidad de manipular el discurso público a la velocidad de un jet. Esto aumenta las apuestas en la batalla de las narrativas estratégicas que se libran entre actores estatales, no estatales e independientes, de modo que proporcionan las condiciones necesarias para el surgimiento de este tipo de guerra.

Aunque no existe un consenso para la definición de la guerra cognitiva, a continuación, abordaremos algunas definiciones tanto de estudiosos de los conflictos modernos, como de algunas organizaciones e instituciones.

Para Ottewell (7 de diciembre de 2020), la guerra cognitiva intenta alterar las percepciones de las personas, las cuales se manifiestan ya sea en acciones o reacciones. Las percepciones son un producto de la cognición, las cuales se convierten en el objetivo que la guerra cognitiva pretende manipular. Así mismo, el autor define la cognición como:

El proceso mental de adquirir y comprender conocimiento, que implica el consumo, la interpretación y la percepción de información. En consecuencia, el dominio cognitivo consiste en la percepción y el posterior razonamiento, los cuales pueden ser modelados, mediante la manipulación de la información, para influir en la interacción entre las creencias, los valores y la cultura de los individuos, grupos y sociedades (párr. 1, traducción propia).

En este mismo sentido, para Álvarez *et al.* (2017), el escenario cognitivo es:

Donde residen la intención, la doctrina, las tácticas, las técnicas y los procedimientos; es el dominio donde surgen los conceptos decisivos. Por su parte, el escenario social comprende los elementos necesarios de cualquier empresa humana; es donde los seres humanos interactúan, intercambian información, forman conocimiento compartido y entendimientos, y toman decisiones colaborativas. A su vez, es el ámbito de la cultura, la religión, los valores, las actitudes y las creencias, y donde se toman decisiones políticas relacionadas con la voluntad de la comunidad (p. 192).

De igual manera, como lo mostró Álvarez (2022), en las diapositivas, en la guerra cognitiva el campo de batalla es la mente de las personas y su objetivo principal es modificar no solo lo que la gente piensa, sino la forma en cómo piensan y cómo actúan. Este tipo de guerra desarrolla operaciones de información (diplomacia pública, propaganda, operaciones psicológicas, subversión política y cultural, engaño o interferencia), a través de redes informáticas, para interrumpir, dañar o modificar lo que una audiencia objetivo “sabe” o “piensa que sabe” sobre sí misma y el mundo que la rodea, promoviendo movimientos de disidencia u oposición (p. 22).

Para Hung y Hung (2022), el concepto de guerra cognitiva se refiere a:

Las actividades realizadas para manipular los estímulos ambientales y de esta manera controlar los estados mentales y los comportamientos tanto de los aliados como de los adversarios, en cualquier tipo de conflicto, enfocándose en la entrada (flujo de información), al igual que en el sistema cognitivo y su salida (comportamientos) (p. 2, traducción propia).

Otros estudiosos como Rosner y Siman-Tov (8 de marzo de 2018) afirman que la guerra cognitiva es la manipulación del discurso público por parte de elementos externos que buscan socavar la unidad social o dañar la confianza pública en un sistema político. Bernal, Carter, Singh, Cao y Madreperla (2020) sostienen que la guerra cognitiva es la militarización de la opinión pública, por parte de una entidad externa, con el propósito de influir en la política pública y gubernamental y desestabilizar a las instituciones públicas de una nación. Backes

y Swab (2019) entienden la guerra cognitiva 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.

Según lo expresa la OTAN en su revista *online*, la guerra cognitiva es:

El conflicto en el que la mente humana se convierte en el campo de batalla y cuyo objetivo es el de cambiar no solamente lo que la gente piensa, sino también cómo actúa, que, llevada a cabo con éxito, moldea e influye en las creencias y los comportamientos individuales y grupales para favorecer los objetivos tácticos o estratégicos de un agresor. En su forma extrema, la guerra cognitiva tiene el potencial de fracturar y fragmentar a toda una sociedad, de modo que ya no tenga la voluntad colectiva de resistir las intenciones de un adversario, de manera tal que un oponente puede llegar a someter a una sociedad sin recurrir a la fuerza o la coerción directas (Johns Hopkins University e Imperial College London, 20 de mayo de 2021, párr. 1, traducción propia).

Por su parte, un trabajo colaborativo entre la Universidad John Hopkins, la Universidad Técnica Checa de Praga, el Colegio Imperial de Londres y el Instituto de Tecnología de Georgia, define la guerra cognitiva como un nuevo tipo de conflicto consistente en la militarización de la opinión pública por parte de entidades externas, cuyo propósito es influir y/o desestabilizar una nación.

Acorde con las anteriores definiciones, se podría decir que la guerra cognitiva es aquella que se libra en la mente y busca no solamente influir en lo que piensan, sino también en cómo actúan las personas, y cuyos propósitos principales son la influencia en las políticas públicas y la desestabilización de las instituciones de una nación. De modo que, para cumplir con sus propósitos de influenciar y desestabilizar, la guerra cognitiva tiene una serie de componentes de tipo no cinético, tales como operaciones psicológicas, operaciones de información y operaciones cibernéticas, que se ejecutan en un ambiente cada vez más urbano.

Componentes de la guerra cognitiva

Para Claverie, Prébot, Buchler y Du Cluzel (2022), en la guerra cognitiva todos los elementos de la guerra de información, incluidas las operaciones psicológicas, se combinan para la acción militar. Así mismo, estos académicos afirman que en la guerra cognitiva convergen dos campos operativos que hasta ahora se gestionaban por separado: operaciones psicológicas y operaciones de influencia (poder blando), por un lado; y operaciones cibernéticas destinadas a degradar o destruir activos de información física, por el otro lado.

Operaciones psicológicas y guerra cognitiva

Las operaciones psicológicas han existido desde tiempos ancestrales y buscan efectos tales como imponer la voluntad política, mitigar intelectual y moralmente, local y universalmente

al adversario, mediante la acción psicológica (Costa, 2018). En este sentido, el Ejército de los Estados Unidos (2005) persigue, a través de este tipo de operaciones, influir en el comportamiento de las audiencias objetivo para apoyar los objetivos nacionales, lo que hace por medio de la transmisión de información seleccionada para injerir en las emociones, los razonamientos y, en última instancia, en el comportamiento de la población objetivo. Así mismo, relaciona las operaciones psicológicas con el uso de productos o propaganda blanca, gris y negra, ejecutada por los diferentes servicios de las Fuerzas Armadas.

En cuanto a los productos blancos, los define como aquellos que son oficiales, abiertos y se identifica fácilmente que provienen de los EE. UU., mientras que los productos grises tienen un elemento de origen ambiguo, encubierto y su origen es difícil de identificar, y los productos negros deben parecer como si se originaran en una fuente hostil (Headquarters, Department of the Army, 2005).

Por medio de la ejecución de operaciones psicológicas, la guerra cognitiva persigue el control de la mente y de las emociones, apalancándose en la cuarta revolución industrial, y emplea principalmente productos o propaganda gris, que son más fáciles de difundir a grandes audiencias y cuya autoría queda en el anonimato.

En este contexto, las operaciones psicológicas combinan acciones que involucran información y emociones colectivas que pueden dirigir el comportamiento de una población o, al menos, de una parte de ella. La misma lógica se puede aplicar a un grupo específico de personas tales como estudiantes, profesores, trabajadores, incluso y más peligroso aún, a las fuerzas militares de una nación.

Operaciones de información y guerra cognitiva

Las operaciones de información se emplean para controlar el flujo de información y la información pura en todas sus formas. Están encaminadas a influir, interrumpir, corromper o usurpar la toma de decisiones humana y automatizada del adversario, mientras se defienden la información y los sistemas de información propios (Headquarters, Department of the Army, 2016). Así mismo, las operaciones de información incluyen la recopilación de información táctica sobre un adversario, como también la difusión de propaganda en busca de una ventaja competitiva sobre este (Rand Corporation, 2022).

Operaciones cibernéticas y guerra cognitiva

Las operaciones cibernéticas se incluyen como componente de la guerra cognitiva, en razón a que comparten el mismo *modus operandi* o, peor aún, pueden emplear los mismos canales para la ejecución de sus acciones. En este sentido, las operaciones cibernéticas pueden emplear virus informáticos, los cuales se propagan a través de las redes sociales y están dirigidos a los contactos de la víctima, de manera tal que los agentes de guerra cognitiva utilizan la

información de los contactos de la persona afectada para difundir una cantidad abrumadora de información falsa o engañosa, a través de cuentas que se ven e interactúan de forma humana (Bernal *et al.*, 2020).

La guerra cognitiva y la prevalencia del ambiente urbano

La guerra cognitiva tiene una relación muy estrecha con el fenómeno de la urbanización de las naciones, que permite a las grandes urbes conectarse con las ciudades medianas y pequeñas, en lo que algunos autores clasifican como megaciudades. De esta manera, millones de personas se concentran en espacios reducidos y así se convierten en blancos potenciales de la guerra cognitiva. Si en el pasado los objetivos militares implicaban la conquista de vastos territorios, hoy las grandes ciudades y sus poblaciones, especialmente en los países en desarrollo, son el foco de atención de todo tipo de actores (Hoffman, 2007). Por consiguiente, tal concentración de población favorece un mayor alcance de las operaciones psicológicas y, por ende, de la guerra cognitiva.

En resumen, en un ambiente cada vez más urbano, las operaciones psicológicas persiguen controlar lo que sienten las personas, las operaciones de información intentan controlar lo que ve la población objetivo y las operaciones cibernéticas pretenden interrumpir las capacidades tecnológicas de la mencionada población. Es decir, todas en conjunto aportan a la guerra cognitiva, la cual se enfoca en influir sobre cómo piensa y actúa la población objetivo, para finalmente desestabilizarla. Para un mejor entendimiento, la tabla 1 muestra las características de los componentes de la guerra cognitiva y su convergencia en esta.

Tabla 1. Componentes de la guerra cognitiva

Características	Operaciones psicológicas	Operaciones cibernéticas	Operaciones de información	Guerra cognitiva
Usos masivos de datos y tendencias		X	X	X
Dirigida a influir en el pensamiento y modificar la conducta	X			X
Capacidad para alcanzar grandes audiencias		X		X
Enfocada en la circulación de la información	X		X	X
Empleo de propaganda gris	X			X

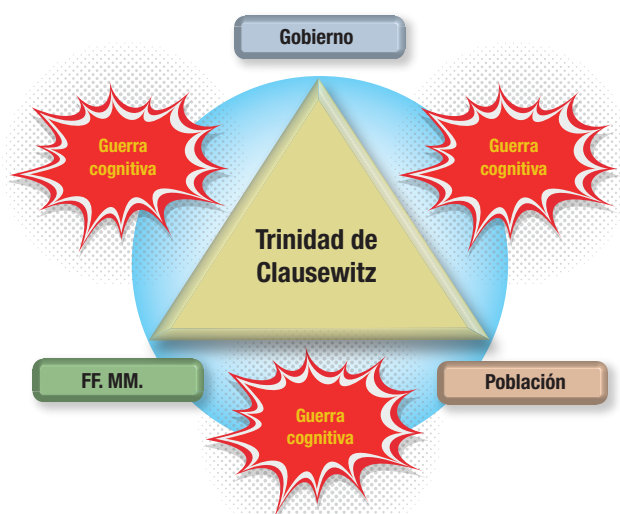
Fuente: adaptado de Bernal *et al.* (2020).

Objetivos de la guerra cognitiva

Para Clausewitz (1989), la naturaleza de la guerra es siempre la misma y consiste en imponerle la voluntad a un adversario. Así mismo, el teórico militar sostiene que la guerra es una trinidad compuesta por la violencia y el odio, el azar y la probabilidad, y las consideraciones políticas, elementos que se desarrollan a través de la interacción de las personas, las fuerzas militares y los gobiernos. Siendo consecuentes con lo anterior, podríamos afirmar que la naturaleza de la guerra cognitiva es diferente a cualquier otro tipo de guerra, ya que, en lugar de obligar a nuestro adversario a hacer nuestra voluntad, el objetivo es lograr que el enemigo se destruya a sí mismo desde adentro, dejándolo incapaz de resistir, disuadir o desviar nuestros objetivos (Bernal *et al.*, 2020).

De igual manera, podríamos afirmar que la trinidad de Clausewitz sigue cobrando vigencia en el contexto estratégico actual, que nos muestra cómo las dinámicas políticas, económicas, sociales y militares, son altamente vulnerables a cualquier ataque en el dominio cognitivo. Ello podría llegar a alterar la dinámica y la forma en que interactúan las personas, las fuerzas militares y el gobierno, y así se causaría una ruptura en la trinidad al generar antagonismos y animosidades entre estos grupos de interés, de modo que una sociedad o nación pueden llegar a implosionar. En este sentido, Bernal *et al.* (2020) manifiestan que la guerra cognitiva pretende que los adversarios se destruyan a sí mismos de adentro hacia afuera y esto se hace por medio de la influencia en la política pública y gubernamental y la desestabilización de las instituciones. La figura 2 muestra la trinidad de Clausewitz, la interacción entre los grupos que la conforman y la ruptura que puede generar la guerra cognitiva.

Figura 2. El impacto de la guerra cognitiva en la trinidad de Clausewitz (1989)



Fuente: elaboración propia.

De otra parte, para Bernal *et al.* (2020), la guerra cognitiva se puede visualizar en una matriz en la que se contemplan la población objetivo y el propósito. En cuanto a la población, esta puede variar desde sociedades enteras, hasta elementos individuales tales como líderes en los campos político, económico, social, militar, religioso y académico, entre otros. En términos de propósito, la guerra cognitiva tiene dos objetivos principales: la desestabilización y la influencia. La figura 3 ilustra los objetivos y la población a quien va dirigida la guerra cognitiva.

Figura 3. Matriz población y objetivos de la guerra cognitiva



Fuente: adaptado de Bernal *et al.* (2020).

Desestabilizar

El primer objetivo fundamental de la guerra cognitiva es desestabilizar a las poblaciones objetivo. Según Bernal *et al.* (2020), la desestabilización se realiza al interrumpir la organización y la unidad de los sistemas y personas de una población (trinidad de Clausewitz).

Esto da como resultado una caída drástica de la productividad y una pérdida de cooperación, ya que esa población ahora está abrumada por problemas internos y menos enfocada en alcanzar objetivos comunes (intereses nacionales). Los perpetradores interrumpen la organización y la unidad de sus poblaciones objetivo, acelerando las divisiones preexistentes o introduciendo nuevas ideas, pretendiendo el enfrentamiento entre los diferentes grupos que conforman una sociedad y el aumento de la polarización (p.12).

En el nivel individual, los líderes pueden ser considerados objetivos de desestabilización cuando son la fuente de ideas polarizadoras. En el ámbito grupal, los atacantes también

pueden apuntar a la población en general para introducir ideas divisivas, las cuales chocan con sus creencias, sus principios y sus valores (cultura de una sociedad o nación) (Bernal *et al.*, 2020). Así mismo, los atacantes pueden impulsar narrativas falsas contra la cultura o contra grupos específicos de personas. Para los mencionados autores, algunas estrategias de guerra cognitiva que se alinean con los objetivos de desestabilización incluyen (p. 13):

- Aumentar la polarización
- Promover movimientos y problemas
- Deslegitimar el gobierno y su liderazgo
- Deslegitimar las instituciones
- Aislar a individuos o grupos
- Interrumpir actividades económicas claves
- Distorsionar la información

Como ejemplo de que la guerra cognitiva a menudo busca dividir a una población, aumentar la polarización y aprovechar las divisiones existentes en su interior, podemos examinar el caso de las filtraciones de los correos electrónicos de la Convención Nacional Demócrata de los Estados Unidos (DNC, por sus siglas en inglés) ocurridas en 2016. Según Yuhás (citado en Bernal *et al.*, 2020, p. 16):

En abril de 2016, las unidades cibernéticas rusas obtuvieron acceso a los servidores internos del DNC, lo que les permitió robar correos electrónicos y documentos confidenciales, los cuales varios meses después, se filtraron en WikiLeaks. Fue en este punto cuando los eventos pasaron de una operación cibernética, a un ataque de guerra cognitiva, en razón a que las campañas desviaron su atención y la división comenzó a crecer dentro del partido demócrata. Producto del ataque, se reveló que el DNC estaba favoreciendo a Hillary Clinton en el tiempo previo a la selección de un candidato presidencial de ese partido. Esto puso a los demócratas progresistas y los demócratas moderados unos contra otros. La ruptura dentro del partido demócrata resultó en un cambio en el apoyo de los candidatos. En lugar de centrarse en el ataque ruso en sí, las figuras políticas estaban mucho más preocupadas por el contenido y lo que podría significar para sus carreras. Los votantes comenzaron a cambiar debido a los problemas planteados por estos nuevos documentos y publicaron declaraciones de descontento. La campaña de Hillary Clinton admitió que este ataque tuvo un efecto significativo en el resultado de la elección general. Y esto no quiere decir que no hubo un mayor impacto polarizador a lo largo de las líneas partidarias. La campaña del presidente Trump también se centró en el contenido de los ataques, en lugar del ataque ruso en sí. En un momento en que el país no podía darse el lujo de reaccionar de manera partidista, los dos partidos principales se enfrentaron entre sí, lo que resultó en una de las etapas más polarizadas de la política estadounidense (traducción propia).

Influenciar

El segundo objetivo fundamental de la guerra cognitiva es influir en las poblaciones objetivo. Para Bernal *et al.* (2020), este objetivo se logra:

Manipulando la interpretación y comprensión del mundo o el entorno que tiene la población objetivo sobre estos y la intención final es que un grupo determinado tenga ideas afines sobre un tema propuesto por los atacantes. En su mayor potencial, los perpetradores tienen como objetivo generar consenso entre una población con suficiente poder para efectuar un cambio de paradigma. Para influir en cómo piensan poblaciones enteras o segmentos de poblaciones, los perpetradores pueden apuntar a líderes políticos, económicos, académicos, sociales, religiosos y militares como vectores para llegar a una audiencia más amplia. Alternativamente, los perpetradores pueden simplemente divulgar información falsa, lanzando una amplia red con la esperanza de llegar a suficientes personas para provocar el cambio. De otra parte, la influencia puede utilizarse como medio de desestabilización, cuando se alienta o coacciona a ciertos sectores de la población, para que adopten y promuevan puntos de vista específicos, dirigidos contra los de otros grupos de la población (p. 19).

Según estos autores (Bernal *et al.*, 2020, p. 20), la influencia se puede llevar a cabo por medio de:

- Promover ideologías extremistas
- Manipular las creencias de una sociedad
- Controlar actividades económicas claves
- Deslegitimar las acciones gubernamentales
- Influir o deslegitimar las elecciones
- Deslegitimar a los grupos de oposición
- Reclutar adeptos a una causa

Continuando con el ejemplo de las elecciones presidenciales de los Estados Unidos en 2016, se evidencia que la interferencia del Kremlin fue compleja e insidiosa y apuntó a múltiples aspectos de la política estadounidense. En este sentido, las agencias de inteligencia estadounidenses determinaron que el Gobierno ruso había ordenado que se filtraran los correos electrónicos de la campaña de la candidata Hillary Clinton y que se crearan bots de redes sociales para propagar puntos de vista extremistas y noticias divisivas. Después de casi tres años, el 18 de agosto de 2020, el Senado de los EE. UU. publicó un informe en el que se afirmaba que el Comité descubrió que el Gobierno ruso participó en un esfuerzo agresivo y multifacético para influir o intentar influir en el resultado de las elecciones presidenciales de 2016 (The Senate, 2020). Así las cosas, Rusia, con su experiencia en guerra cognitiva y por medio de la

influencia, logró explotar las divisiones de los estadounidenses para influir en su pensamiento y en su voluntad de voto. Del mismo modo, Rosner y Siman-Tov (2018) afirmaron que Rusia:

Por medio de la influencia trató de convencer a los estadounidenses de que los conciudadanos de un partido político contrario son peligrosos y la integridad de las elecciones no se podía garantizar. Tal ha sido el impacto del ataque ruso, que los sentimientos de división se han mantenido hasta el presente. Los votantes de ambos lados del espectro político se han polarizado cada vez más, perpetuando una mentalidad de nosotros contra ellos. Ya existen tanto demócratas como republicanos que creen que el otro partido traiciona los ideales de la nación y esta situación ha sido exacerbada por el uso de trolls y bots rusos (párr. 3, traducción propia).

En suma, podríamos decir que, a diferencia de los otros tipos de guerras cuyo objetivo es imponerle nuestra voluntad a un adversario, la guerra cognitiva pretende que el enemigo se destruya a sí mismo desde adentro, lo que podría interrumpir la dinámica de la trinidad de Clausewitz y, de esa manera, hacer implosionar a una sociedad entera. En este sentido, la guerra cognitiva persigue dos objetivos principales: primero, influir en la manera como piensan las personas individual o colectivamente y así manipular sus actuaciones; segundo, desestabilizar a un grupo o a toda una sociedad al punto de quebrantar su voluntad de lucha, de modo que el agresor pueda someterles sin recurrir al uso de fuerza cinética o a la coerción directa.

La guerra cognitiva y las nuevas amenazas para la seguridad y la defensa nacionales

*Cuanto más se desvíe una sociedad de la verdad,
más odiará a aquellos que la proclaman.*

George Orwell

Como se describió antes, las nuevas tecnologías combinadas con las redes sociales y los medios de comunicación permiten que la revolución tecnológica y digital se dé a gran escala, sea simultánea y tenga un alcance global y omnipresente. Por esta razón, el alcance de dicha revolución facilita que millones de personas se conecten a través de sus dispositivos móviles o de sus computadores, con un poder de procesamiento, una capacidad de almacenamiento y un acceso a la información sin precedentes.

Si bien es cierto que las características de las nuevas tecnologías enunciadas ofrecen la posibilidad a la sociedad en general de conectarse y compartir información, estas condiciones

también pueden ser utilizadas por actores estatales, no estatales e independientes para ejecutar guerra cognitiva y de ese modo es posible que se conviertan en una amenaza para las personas, los grupos sociales, las naciones e incluso los sistemas democráticos; es decir, una amenaza para la seguridad y la defensa nacionales. Así entonces, las principales herramientas por medio de las cuales se materializan las amenazas dentro de la guerra cognitiva son la desinformación, las noticias falsas y la posverdad.

Desinformación. Hasta hace poco, el término más utilizado en el discurso político para identificar cuestiones relacionadas con la manipulación de la información era desinformación, de la palabra rusa *dezinformatsiya*, que deriva del título de un departamento de propaganda negra de la KGB responsable de producir información falsa con la intención de engañar a la opinión pública (Jackson, 17 de octubre de 2017). La desinformación es una práctica relativamente reciente en comparación con la propaganda, que se originó en el siglo XVII y generalmente connota el uso selectivo de información destinada a producir algunos efectos políticos deseados (Jackson, 17 de octubre de 2017).

Si bien la desinformación debe interpretarse como el producto de la construcción de una falsedad intencional, este fenómeno conlleva a la propagación de información incompleta, vaga, engañosa o ambigua. La desinformación puede estar compuesta en su mayoría de hechos verdaderos, pero desviados del contexto real o mezclados con falsedades para respaldar un mensaje deliberado, que generalmente hace parte de un plan o una agenda más amplia (Jackson, 17 de octubre de 2017).

Es decir, la desinformación busca manipular o influir en la opinión de grupos para apoyar una causa o creencia en particular, a menudo promoviendo los beneficios y las virtudes de una idea o un grupo, al mismo tiempo que distorsiona la verdad o suprime el contrargumento. Por ejemplo, desde su agresión militar contra Ucrania, Rusia ha emprendido una campaña de desinformación sostenida y coordinada, controlada por el Estado y dirigida a la población rusa, sus países vecinos y el resto del mundo, con el objetivo particular de influir en la opinión pública. De esta manera, los medios de información pro-Kremlin se han encargado de insistir en que había pruebas de que Ucrania estaba cometiendo atrocidades contra su población de habla rusa en el este del país, lo que justifica que Rusia tenía la obligación de intervenir en esta situación, sobre todo porque Ucrania y Rusia son una sola nación. Este mensaje repetitivo ilustra el intento del Kremlin de difundir desinformación y manipular información para justificar su agresión militar contra Ucrania.

Noticias falsas. De otra parte, según Giusti y Piras (2021), las noticias falsas son una versión avanzada y tecnológica de la desinformación, ya que con este término se hace referencia a piezas de información manipuladas intencionalmente, las cuales se propagan a través de las redes sociales. De acuerdo con estos autores, en un principio la difusión de noticias

falsas estuvo ligada a la vida política en sus momentos más sensibles, como las elecciones y las crisis internacionales. Actualmente, el uso de noticias falsas se ha expandido rápidamente y hoy día hacen parte de la mayoría de los aspectos de la política y de la vida común (Giusti y Piras, 2021).

De otra parte, la construcción de una realidad falsa, alternativa o alterada y su difusión a través de los medios y/o el boca a boca no es un fenómeno nuevo en la política, como sí lo son el uso masivo a nivel mundial de las nuevas tecnologías de la cuarta revolución industrial y el extenso alcance de las redes sociales (Fuller, 2018), que pueden difundir noticias o mensajes falsos a un ritmo tan vertiginoso que los pueden convertir en tendencia hasta llegar a ser virales.

De igual manera, las redes sociales y las aplicaciones de mensajería instantánea han demostrado ser extraordinarios amplificadores de noticias falsas y, por lo tanto, han adquirido un papel político estratégico mucho más allá de su función inicial como plataformas de recreación y socialización. De hecho, se están convirtiendo en poderosas herramientas políticas.

Por tanto, la combinación de noticias falsas y redes sociales es especialmente adecuada para producir efectos subliminales que pueden llegar a los estratos más profundos y emocionales de la mente de las personas, con mayores posibilidades de persistencia y persuasión en comparación con la desinformación difundida por otros medios. Un ejemplo evidente de noticias falsas se dio durante la pandemia de COVID-19. Al inicio de esta, las redes sociales y de mensajería se vieron saturadas de mensajes que afirmaban que tomar abundante agua, hacer gárgaras con sal y agua caliente o aplicar ungüentos en la nariz, eran métodos efectivos para eliminar la enfermedad. Una vez inventadas las vacunas, las redes se volvieron a saturar de información que afirmaba que estas hacían parte de una conspiración para reducir la población de la Tierra. Otros mensajes afirmaban que a través de la vacuna se implantaban chips, mientras que otros aseguraban que la vacuna podría causar efectos secundarios graves para la salud o incluso la muerte.

Posverdad. Hannan *et al.* (citado en Giusti y Piras, 2021) emplean la expresión posverdad para describir la compleja relación contemporánea en la que realidad, falsedad y poder interactúan y se mezclan en el mundo de los medios y las redes sociales. Para los mencionados autores, la posverdad:

Revela una fase política en la que las personas se inclinan a aceptar argumentos basados en sus propias emociones y creencias más que en hechos y realidades. En consecuencia, decisiones políticas tan importantes como votar para elegir a sus gobernantes o la toma de decisiones colectivas como un referéndum, están más relacionadas con impulsos emocionales, ideológicos e impresiones superficiales más que a la selección racional basada en evaluaciones de políticas. El debilitamiento de la relevancia del razonamiento racional se

abre a la fácil instalación de información falsificada. En esta perspectiva, una mentira no es necesariamente algo que se opone a la verdad; es más bien un derivado de una versión distorsionada de la misma, de modo que los límites entre la verdad y la mentira se difuminan (Giusti y Piras, 2021, p. 6, traducción propia).

Como lo explica Bufacchi (24 de enero de 2020), mientras que una mentira subvierte una verdad específica, la posverdad intenta subvertir la verdad misma y el prefijo *pos* se refiere a la afirmación de que una idea específica se ha vuelto redundante y, por lo tanto, puede desecharse de forma segura. La posverdad es la creencia de que la verdad ya no es esencial, que la verdad se ha vuelto obsoleta. En este mismo sentido, Keller, Schoch, Stier y Yang (2020) añaden que las noticias falsas son una excelente herramienta para allanar el camino hacia la posverdad, ya que estas no necesariamente niegan los hechos o lo que se puede definir como verdad, sino que sugieren interpretaciones engañosas o inventan hechos que no existen pero que, sin embargo, son plausibles o cercanos a lo que el público podría esperar.

De otra parte, Polyakova y Meserole (2019) afirman:

Los Estados se han convertido en cuna de políticas divisorias a través de sus discursos y políticas populistas, la deslegitimación de la competencia, las políticas de odio y resentimiento, la demonización, la enemistad de sus adversarios políticos, y todos estos elementos se han vuelto rasgos comunes tanto en regímenes democráticos como autocráticos (p. 4, traducción propia).

En este sentido, un dirigente político podría usar la posverdad para dominar el escenario político o para deslegitimar a un oponente, sus ideas, la historia e incluso toda una ideología o cultura. Estas acciones las llevaría a cabo por medio de técnicas de política divisiva, empleando la combinación de tecnologías de la información, las redes sociales, las noticias falsas y la desinformación, de tal suerte que intoxicaría no solamente el ambiente político, sino también el social, para que los ciudadanos se vuelvan partidistas de un grupo en específico y se enfrenten al contrario (Polyakova y Meserole, 2019). Un ejemplo de cómo se ha aplicado la posverdad lo podemos tomar del mandato del expresidente Donald Trump y su política “América grande otra vez”. A través de esta política, el exmandatario daba a entender a sus seguidores que Estados Unidos estaba en decadencia y él sería su salvador. Así mismo, esta política polarizó al país y exacerbó los sentimientos hacia los inmigrantes y las tensiones raciales en los Estados Unidos.

Con todo lo anteriormente expuesto, se podría decir que las nuevas tecnologías sumadas a las redes sociales han permitido la aparición y propagación de fenómenos como las noticias falsas, la desinformación y la posverdad, las cuales se convierten en nuevas amenazas para la seguridad y defensa nacionales, de las que Colombia no ha estado exenta.

La guerra cognitiva y su impacto en Colombia

Colombia no ha estado exenta de las nuevas amenazas de la guerra cognitiva, ya que desde la implementación de los acuerdos de paz entre las Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC-EP) y el Estado colombiano, a partir de 2017, diferentes actores (estatales, no estatales e independientes) han venido ejecutando diversas acciones de este tipo de guerra en contra del país.

Como señala Stent (27 de enero de 2022), en los últimos años, un actor estatal, Rusia, ha venido adelantando operaciones de información a través de redes sociales y de sus canales de televisión y también estaría interfiriendo en las campañas electorales de algunos países. Es decir, Rusia, a través de acciones no violentas, emplea un modelo de guerra cognitiva con el propósito de desestabilizar la unidad nacional de otros países.

Para Global Americans (18 de noviembre de 2021), China, Rusia y otros actores anti-democráticos son muy activos en la promoción de la desinformación y la propaganda en América Latina. A través de sus medios de comunicación estatales, como *Russia Today (RT)*, *Telesur*, *Sputnik Mundo* y *Xinhua Español*, al igual que por medio de las redes sociales Twitter y Facebook. Así mismo, O'Grady (30 de enero de 2022) indica que los canales de televisión rusos *RT* y *Sputnik* han adelantado campañas de desinformación para favorecer tanto las narrativas del eje Rusia-Cuba-Venezuela-Nicaragua-Bolivia, como las de algunos partidos políticos de la región.

Consecuente con lo anterior, Global Americans (18 de noviembre de 2021) señala que:

Los mensajes chinos en Colombia se centran en su papel como un socio comercial importante y, por lo tanto, la narrativa proyectada es una asociación mutuamente beneficiosa entre los dos países. Por el contrario, los medios estatales rusos en Colombia se han involucrado más activamente durante los momentos de descontento social y esos mensajes se centran, en gran medida, en temas de conversación antigubernamentales (párr. 1, traducción propia).

La investigación de Global Americans también concluye que los actores políticos venezolanos igualmente se han involucrado en esfuerzos agresivos de desinformación contra el gobierno colombiano, debido en parte a la voluntad de Bogotá de albergar a un gran número de refugiados venezolanos y miembros de la oposición venezolana (18 de noviembre de 2021).

Con referencia a actores no estatales, según Davis, Kilcullen, Mills y Spencer (2016), las extintas FARC-EP, después de haber firmado el Acuerdo de Paz en 2017, estarían dedicadas a desarrollar una estrategia de aplicación de todas las formas de lucha, incluyendo guerra cognitiva, cuyo objetivo sería la toma del poder a través del uso de acciones no cinéticas (no

violentas), tales como manipulación de la protesta social, propaganda internacional y esfuerzos por destruir la legitimidad de las Fuerzas Militares colombianas.

Asimismo, Ellis (2021) plantea que el Ejército de Liberación Nacional (ELN) también estaría empeñado en el empleo de la protesta social como medio para apoyar sus objetivos estratégicos de deslegitimar y desestabilizar al Gobierno colombiano. De otra parte, Begue (10 de mayo de 2021) afirma que las noticias falsas provenientes de diferentes actores han contribuido a que las manifestaciones que se han venido presentando en Colombia, durante los últimos años, se tornen más violentas, en especial contra los miembros de la Policía Nacional.

Como ya se mencionó, actores estatales seguirán ejecutando acciones de guerra cognitiva, a través de hostilidades no violentas. Para Humire (2022), los mencionados actores reconocen que el mejor armamento contra Colombia es la desinformación. Por lo tanto, Rusia y otros actores estatales, a través de las redes sociales, seguirán tratando de erosionar la narrativa democrática de Colombia, fomentando la protesta social violenta.

Según se ha visto, la guerra cognitiva ya está presente en Colombia, por lo tanto, el Estado colombiano y las FF. AA. deberán establecer una estrategia para combatir este nuevo tipo de guerra. Dentro de dicha estrategia, un primer paso puede ser identificar las amenazas, las capacidades institucionales y las posibilidades de enfrentamiento; un segundo paso consistiría en establecer las dimensiones en que se podrían generar acciones para enfrentar amenazas y ataques de tipo cognitivo.

Desarrollando una estrategia para combatir la guerra cognitiva

Para desarrollar una estrategia coherente, los estrategas militares y civiles deberán establecer cuáles son las amenazas que pueden poner en peligro los intereses nacionales y, por ende, la estabilidad del país. Así mismo, contrastar las amenazas con las capacidades institucionales y las acciones para combatirlas. La tabla 2 presenta un resumen ejemplificativo de cómo estructuras ya existentes en las instituciones militares de Colombia tienen capacidad de actuar como elementos claves en el enfrentamiento de las amenazas en el campo cognitivo.

La resiliencia de las instituciones militares puede ser evaluada por la confrontación entre acciones u operaciones a nivel cognitivo (características señaladas en la literatura especializada) y las capacidades existentes. Además, es imprescindible generar en los gobernantes y comandantes militares la consciencia acerca de los riesgos silenciosos de las amenazas cognitivas e informacionales, y también del conjunto de las capacidades no cinéticas que tienen a su disposición para hacer la prevención y el enfrentamiento de tales amenazas.

Tabla 2. Confrontación ejemplificadora entre algunas amenazas cognitivas y capacidades institucionales de las Fuerzas Militares

Amenazas cognitivas	Capacidades institucionales	Posibilidades de enfrentamiento (ejemplos)
Fragmentación del tejido social	Sistema de comunicación social y sistemas de gestión y protección del patrimonio cultural e histórico	Campañas de fortalecimiento de la identidad nacional y los valores culturales
Desestabilización de las instituciones	Sistema de educación	Fortalecimiento de la cultura de legalidad y apoyo a las instituciones
Manipulación de las emociones colectivas	Sistema de comunicación social y sistemas de asistencia social	Fortalecimiento de comunicaciones estratégicas, creación de una sección dedicada a contrarrestar noticias falsas, posverdad y desinformación
Miedo de actuar por inseguridad jurídica	Sistemas de doctrina militar y asesoría jurídica	Ampliación y actualización de los manuales de procedimiento
Noticias falsas	Comunicaciones estratégicas	Creación de un noticiero institucional

Fuente: elaboración propia.

En caso de que tales capacidades no tengan ningún efecto, o sean por demás débiles, en su esfera de responsabilidad, tal condición necesita ser reportada a niveles adecuados como riesgo o fragilidad interna a ser corregida, en el mismo nivel de importancia que las demás condiciones críticas operacionales, logísticas, financieras, entre otras.

Estas y otras capacidades críticas pueden ser replicadas o inducidas en otras instituciones (públicas y privadas) consideradas esenciales para mantener la institucionalidad y la estabilidad política de la sociedad en su conjunto. Sin embargo, para que las FF. MM., tengan las capacidades necesarias para hacer el enfrentamiento y logren la resiliencia deseada para proteger una nación tan compleja como Colombia, es necesaria una concientización mayor y una articulación interinstitucional.

Logrado el nivel de percepción de riesgos y capacidades de enfrentamiento, es posible empezar la formulación de una estrategia institucional para detección y enfrentamiento de las amenazas cognitivas.

Los ejemplos citados arriba representarían una cuarta dimensión, de prevención y contención de daños, que complementarían la estrategia propuesta por Álvarez *et al.* (2017, p. 257-258): “por ende, una estrategia de “astucia” se podría caracterizar por tres dimensiones: 1) concientización; 2) detección y exposición; y 3) descubrimiento y penetración”.

Si desarrollamos un conocimiento profundo de la guerra cognitiva, podremos establecer componentes fundamentales del adversario como su estrategia y su centro de gravedad. Así mismo, será posible aprovechar sus debilidades y atacarlas a través de operaciones de información, estableciendo narrativas propias o contranarrativas para contribuir a la construcción

de la verdad institucional. En otras palabras, se podría emplear el modelo presentado por Sharp (2010) que consiste en identificar la estrategia del adversario, no trabajar dispersamente, atacar los pilares de apoyo, emplear la lucha no violenta, y aprovechar los errores del contrario y explotarlos.

En este sentido, la tabla 3 establece una concepción un poco más ampliada de una posible estrategia de preparación y enfrentamiento de las amenazas de los campos de información y cognitivos.

Las acciones de protección de la fuerza, como parte de funciones básicas de conducción de la guerra, en los planeamientos conjuntos de paz y de guerra, necesitan también considerar las amenazas cognitivas que pueden afectar significativamente las capacidades operacionales, logísticas y administrativas. El ambiente de fragmentación política y social que caracteriza a las sociedades hoy día lleva a un contexto operacional altamente complejo, de modo que genera incertidumbre en todos los niveles de mando de las fuerzas militares y de seguridad.

Tabla 3. Concepción de estrategia de enfrentamiento institucional en ambiente de guerra cognitiva

Dimensión	Características
Concientización o monitoreo	El Estado colombiano debería animar a sus ciudadanos para que desarrollen su propia resiliencia personal frente a los ataques cognitivos. Lo ideal sería que los ciudadanos tomaran medidas para protegerse de los ataques que provienen de la conectividad provocada por nuestra dependencia de la tecnología.
Marco y criterios de reconocimiento de amenazas	Primero, se debe considerar agregar la guerra cognitiva al marco de las amenazas, y segundo, desarrollar un conjunto de criterios para determinar cuándo se está produciendo un ataque cognitivo. Por esta razón, el Estado colombiano y sus FF. AA. deben trabajar para desarrollar un conjunto de reglas o un marco que permita definir los actos de guerra cognitiva y responder adecuadamente a ellos.
Enfoque proactivo	Antes de que el Estado y sus FF. MM. puedan tomar medidas para combatir los efectos de la guerra cognitiva, deben adoptar un enfoque proactivo para descubrir los ataques en tiempo real y así poder contrarrestarlos.
Prevención	Identificación y fortalecimiento de las capacidades institucionales adecuadas para hacer el enfrentamiento de las amenazas cognitivas antes de cualquier operación o campaña detectada.
Análisis de vulnerabilidades	Descubrir las vulnerabilidades propias, por medio de la detección de cualquier división o fracción que un enemigo pueda explotar para debilitar o desestabilizar. Esto podría contribuir al diseño de planes de mitigación y a la elaboración de contranarrativas que prevengan un caos a gran escala antes de que comience.
Detección y exposición	Implicaría actividades de recopilación y análisis de inteligencia que tendrían como objetivo determinar lo que el adversario estaría tratando de hacer creer y, como resultado, lo que quisiera que el otro hiciera. En esencia, el objetivo sería reconstruir con precisión la historia de engaño del engañador a partir de los datos y la información disponibles.

Dimensión	Características
Análisis de riesgos	Se enfocaría en revelar lo que sería real. En este caso, los activos de recopilación y análisis de inteligencia se utilizarían para separar lo relevante de lo irrelevante y lo real de lo falso, con el propósito de determinar cuáles serían las verdaderas capacidades y la intención del adversario.
Ajustes organizacionales e institucionales	Se deben establecer unidades de tipo cognitivo dentro de las FF. AA., que tengan canales de comunicación con otras instituciones. Las responsabilidades de estas unidades se deben enfocar, en primer lugar, en establecer las capacidades actuales que se tienen para enfrentar la guerra cognitiva, desarrollar marcos de acción y realizar una evaluación de vulnerabilidad del Estado y sus FF. MM. Segundo, prepararse para ataques cognitivos antes de eventos importantes, como elecciones y protestas, en todo el país. Tercero, investigar los ataques cognitivos para determinar quién es el perpetrador y así poder elaborar una respuesta adecuada. Cuarto, se deben establecer enlaces o canales de comunicación eficientes con los conglomerados de medios como Meta, Google y Microsoft, para definir reglas y jurisdicciones sobre casos de ataques cognitivos, especialmente cuando la difusión de información errónea en las plataformas de redes sociales puede amenazar potencialmente la seguridad y la defensa nacionales. Por último, se debe generar un marco normativo que procure contener la desinformación en línea y la difusión de contenido falso.
Acciones de respuesta ofensivas	Hay ciertos factores que se pueden utilizar para crear un marco que guíe el desarrollo de estrategias ofensivas. El primero de ellos es establecer si la guerra que se está librando es principalmente de cognición y cuáles son sus objetivos. El segundo es entender el estado geopolítico del adversario para encontrar puntos de presión, tales como sus centros de riqueza y poder, su infraestructura, el diseño de su industria, sus líderes y medios de comunicación, entre otros.

Fuente: elaboración propia a partir de Álvarez, Barón y Monroy (2019).

De otra parte, dada la prevalencia del ambiente urbano, en donde la tropa está en mayor exposición a múltiples influencias, los comandantes necesitan estar atentos para establecer que están siendo víctimas de un ataque en el campo cognitivo. Por tal razón, se hace necesario evaluar la pertinencia o viabilidad de incluir aspectos de nivel cognitivo e informacional entre los protocolos de protección de las Fuerzas.

Formulado el desarrollo de una posible estrategia para enfrentar la guerra cognitiva, continuaremos con una reflexión del papel de las fuerzas militares en este entorno.

Las Fuerzas Militares y la guerra cognitiva

El mapeo o monitoreo del clima organizacional dentro de las instituciones militares no es aún un acto de gestión, pero sí de verdadera seguridad interna. La correcta identificación de las emociones prevalentes en los varios estamentos que constituyen las fuerzas militares y de policía no es tarea fácil, pero puede permitir la percepción de movimientos de influencia externa directa o indirecta.

Extrapolando el entorno interno puramente organizacional, también es necesario prestar atención a las indicaciones emocionales de la sociedad en su conjunto. En tal sentido, Moisi

(2009) toma esta preocupación como una responsabilidad de la dirección máxima en el campo político de las naciones:

Es deber de los gobiernos examinar las emociones de sus respectivas poblaciones, sacar provecho de ellas si son positivas o intentar modificarlas o subyugarlas si son negativas (“sabiduría oriental”). Este deber no puede ser realizado si no se intenta diagnosticar antes el estado emocional de la población (p. 53).

En este contexto, el primer desafío de las Fuerzas Militares es protegerse de cualquier campaña psicológica o cognitiva que pueda afectar negativamente al propio efectivo, con el fin de generar resiliencia y, en consecuencia, mantener sus capacidades.

Las tropas, acostumbradas a actuar y luchar en las selvas, sabanas y montañas, lejos de los núcleos de población, estaban relativamente protegidas de las acciones cognitivas debido a la dificultad de acceso a los medios de comunicación. Con el aumento de la incidencia mediante una prevalencia potencial, en algunos años, de las operaciones militares en las zonas urbanas, todo el personal estará más expuesto a diversos tipos de influencias sociales, por medios presenciales o tecnológicos. Esto genera la necesidad de hacer un seguimiento más constante de las condiciones psicológicas e identificar posibles campañas organizadas de operaciones psicológicas contra los militares.

Si los objetivos de las campañas cognitivas incluyen la influencia y la desestabilización de la población objetivo, las fuerzas militares deben representar la imagen de unión, legitimidad e institucionalidad de un país. El fenómeno de la fragmentación de la identidad nacional en identidades sectoriales, de género, étnicas, locales y de otro tipo, en el cual cada grupo busca satisfacer sus intereses específicos o incluso sus emociones colectivas, representa un riesgo real para la sociedad en su conjunto.

En este sentido, Moisi (2009) advierte claramente de la importancia que ha adquirido el tema de la identidad en la sociedad actual afirmando que “en la atmósfera ideológica del siglo XX, el mundo fue definido por modelos políticos conflictivos tales como el socialismo, el fascismo y el capitalismo. En el mundo actual, la ideología ha sido reemplazada por la lucha por la identidad” (p. 34).

Desde la implementación del Acuerdo de Paz en 2017, el Gobierno colombiano junto con sus Fuerzas Militares y de Policía o Fuerzas Armadas, han venido enfrentando, de parte de actores estatales y no estatales, una serie de desafíos que reflejan el nuevo carácter de la guerra o guerra cognitiva.

Incluso la existencia y el alcance de las actividades de las fuerzas militares se cuestionan a medida que cambia el escenario nacional e internacional. En el caso específico de las Fuerzas colombianas, en el período llamado posacuerdo, este importante debate puede ser

fácilmente el foco de las operaciones cognitivas, de modo que afecte significativamente las capacidades y los recursos asignados a las instituciones, desde la influencia en la población o los grupos de toma de decisiones en una campaña de mediano y largo plazo.

Los desafíos que representa la guerra cognitiva obligan a que las FF. AA. asuman nuevos papeles para la defensa y la seguridad nacionales. Uno de estos papeles está directamente relacionado con el restablecimiento de una sociedad cada día más resquebrajada (Universidad a Distancia de Madrid, 2015).

Para conseguir este propósito, se deberían fortalecer las relaciones civiles-militares, en el entendido de las relaciones entre el estamento militar con el poder político y la ciudadanía. En esta relación, factores como la confianza y el respeto del uno por el otro son fundamentales. El estamento civil debe poseer la confianza suficiente y estar convencido de la importancia que juegan sus FF. AA. para combatir una guerra cognitiva. En términos de respeto, tanto FF. AA. como estamento civil deberán propender por un profundo respeto mutuo en el entendido que, según Rousseau y su contrato social (Ratto, 2015), deben existir deberes y derechos tanto para el Estado como para sus ciudadanos. Así las cosas, les corresponde al Estado y a sus FF. AA. reconstruir las narrativas que sus adversarios han tratado de edificar, alrededor de la institucionalidad y la legitimidad colombianas.

Según Moisi (2009):

Dado que el mundo en que vivimos solo puede volverse más complejo, las culturas y naciones, tanto como los individuos, se obsesionan cada vez más con sus propias identidades. Esta obsesión solo puede afianzar el peso de las emociones en la política internacional (p. 229).

Las Fuerzas Militares pueden ser el punto de concentración de la confianza de la población en las instituciones, incluso en tiempos de duda y desorden. Representan un depósito de valores, tradiciones y memoria histórica de la Nación y así contribuyen decisivamente al mantenimiento de la identidad nacional, factor de gran importancia para el mantenimiento del tejido social. En las filas de las Fuerzas Militares, se encuentran representantes de todos los grupos sociales, de modo que también son un camino de movilidad social en Colombia.

En complemento de su composición social diversa, está su distribución geográfica en todo el territorio colombiano, lo que configura a la Fuerza Pública como el mayor conjunto institucional de carácter nacional. En varios rincones del país, especialmente los fronterizos, las unidades militares o policiales son la única presencia física del Estado y, por tanto, representan a la institucionalidad en esos lugares.

La capacidad de agregar diferentes grupos sociales, con sus respectivas identidades colectivas, permitió la construcción de confianza entre las instituciones militares y la población en general, a lo largo de la historia. Dichos vínculos de confianza entre los diversos grupos

sociales y las instituciones públicas son esenciales para la formación de una identidad nacional, la cual permite la gobernabilidad en las áreas donde hacen presencia las FF. AA.

Pastrana, Reith y Cabrera (2020) explican la correlación directa entre la identidad y los intereses nacionales. Estos académicos identifican en la Fuerza Pública colombiana, formada por las Fuerzas Militares más la Policía Nacional, uno de los factores formativos de la identidad nacional.

Figura 4. Relación entre FF. MM., intereses nacionales y acciones cognitivas



Fuente: elaboración propia.

La figura 4 muestra la importancia de las FF. MM. como factores de formación de la identidad nacional, que por su turno sustentan la gobernabilidad del Estado colombiano (conjunto de toda la institucionalidad pública) y son un importante referente para el establecimiento de los intereses nacionales. Tales intereses naturalmente pueden confrontar intereses de fuerzas políticas y económicas adversas (nacionales o extranjeras). Dentro del marco conceptual de las guerras cognitivas, las fuerzas adversas pueden generar acciones cognitivas para influir o debilitar las bases de sustentación de los intereses nacionales.

Bilal hace un aporte importante al afirmar que la confianza entre la población en el Estado es un blanco constantemente amenazado en el ámbito de las guerras cognitivas y tales ataques pueden ocurrir bajo el desconocimiento o percepción del país atacado. También la confianza interna dentro de sociedad puede ser erosionada o destruida. Este autor presenta como remedio para combatir tales acciones, el mantenimiento de redes de confianza mutua entre todos los actores de la sociedad (Bilal, 30 de noviembre de 2021) y sostiene que:

Construir, reconstruir y fortalecer la confianza sigue siendo fundamental para crear una resiliencia duradera frente a las amenazas cognitivas que ponen en grave peligro la seguridad a nivel estatal y social. La construcción de confianza dentro y entre las comunidades debe ser

el eje de los esfuerzos para neutralizar la guerra cognitiva y las amenazas que esta presenta (párr. 1, traducción propia).

Para recomponer la sociedad desquebrajada que nos presenta el contexto actual, las FF. AA. deberán desempeñar un papel más preponderante en la forma como el Estado se comunica con la opinión pública. Para este propósito, es necesario crear equipos de comunicaciones estratégicas capaces de entregar un mensaje directo y efectivo, que influya en la voluntad y en el pensamiento de los colombianos.

Un último papel y no menos importante para las FF. AA. es el de servir como articuladores de toda la institucionalidad, dentro de un contexto de seguridad multidimensional. Trabajando de una forma articulada FF. AA. e instituciones lograrían alterar las condiciones de todo orden que afectan al individuo y que, a la postre, sostienen las narrativas de los grupos armados ilegales y los populistas.

Pero antes de ser un referente de identidad y estabilidad nacional, las Fuerzas Militares deben crear o identificar mecanismos (capacidades) diseñados para asegurar su propia cohesión y resiliencia en un escenario de creciente complejidad.

Las capacidades inherentes de las Fuerzas Militares

Las Fuerzas Militares constituyen el único conjunto de instituciones que cuentan internamente (y articuladamente) con todas las capacidades materializadas en diferentes servicios y sistemas para realizar la detección y el afrontamiento de múltiples amenazas en el campo cognitivo. Otras instituciones en la sociedad, a nivel público y privado, tienen estructuras similares por separado, pero no el conjunto completo y articulado. Entre las capacidades con las que cuentan las FF. MM. se encuentran las siguientes.

Los servicios de inteligencia

Los servicios de inteligencia y contrainteligencia realizan un monitoreo constante del flujo de información, incluso parcialmente, por lo que permiten identificar posibles interferencias en la institución y sus áreas de responsabilidad. El establecimiento de doctrinas y procedimientos de información sensible reduce la exposición externa de la institución. En este sentido, Álvarez *et. al* (2017) proponen:

Para enfrentar este desafío, la contrainteligencia colombiana necesitará de una estrategia integral que identifique las amenazas emergentes en los dominios cognitivo e informativo que integre conocimientos y actividades de las diversas entidades de inteligencia, como el Departamento Nacional de Inteligencia, la Inteligencia Militar, la Dirección de Inteligencia de la Policía Nacional y el Ministerio de Defensa Nacional (p. 257).

Los sistemas de educación

Un sistema adecuado de educación y formación permite alinear y nivelar las visiones del mundo, reforzar valores culturales, establecer un lenguaje común, imprimir un fuerte sentido de legalidad e institucionalidad y, en definitiva, estructurar a cada individuo integralmente dentro de su colectivo.

Al considerar todos los cambios sociales, políticos y del escenario operacional, tenemos como consecuencia la evolución en los aspectos doctrinarios en relación con el manejo de informaciones en todas las fases de las operaciones militares, lo cual exige adaptaciones en las escuelas de formación y entrenamiento en todos los niveles.

Por tal razón es necesario desarrollar la doctrina y la formación de todo el personal para actuar en un entorno volátil, incierto, complejo y ambiguo, como el desarrollado en la década pasada durante los tiempos más difíciles del conflicto armado. También es primordial que el mando estratégico reconozca las operaciones psicológicas o campañas en el campo cognitivo en su contra. Las nuevas amenazas pueden provenir de las interacciones entre las Fuerzas Militares con las instituciones públicas y privadas de la sociedad civil, o incluso de grupos poco conocidos de diferentes partes del mundo. Así mismo, percibir la amplitud de todas estas posibles interacciones y relaciones es una habilidad personal importante por desarrollar en los líderes de hoy y mañana.

En este orden de ideas, Malamud (2014) explica la necesidad de entrenamiento y formación de personal militar con características de rendimiento flexible y adaptable a un entorno externo cada vez más complejo, donde los enemigos no siempre son visibles o fácilmente identificables. A esto se suma la realidad del aumento en la variedad de misiones realizadas y los roles desempeñados por las FF. AA. con la sociedad, donde las crecientes interacciones sociales y políticas requieren nuevas habilidades por parte de estas.

Barrera, Hernández y Ramírez (2021) hacen significativas contribuciones al debate sobre la importancia de la educación en las instituciones militares en el entorno de las guerras cognitivas, incluyendo propuestas teóricas de reestructuración con un enfoque en la ética militar. Los autores aportan a la discusión, conceptos relevantes como la formación intelectual en el cuerpo de instituciones militares y policiales, con el consiguiente mantenimiento de la capacidad de ejercer el liderazgo cultural en la sociedad. En este sentido, los autores sostienen que:

Reformar el primer momento educativo en torno a la reestructura de los intelectuales orgánicos ya tiene consigo una ventaja, y es que las Fuerzas Armadas no tienen que deliberar el liderazgo cultural, dado que ya forman parte de él (Barrera *et al.*, 2021, p. 198).

Tener su propio grupo de intelectuales dentro de la organización, capaces de interpretar el ambiente social y político volátil, y después generar conocimiento y doctrina de actuación

para las FF. AA., abre la posibilidad de adaptación rápida de la institucionalidad para enfrentar las diversas amenazas. Es posible generar, entonces, un discurso único y coherente para las fuerzas, lo que permitirá la cohesión de ideas y de percepciones del ambiente social, político y económico. Tales percepciones bien alineadas y actualizadas son condición esencial para la elaboración de estrategias para enfrentar los retos que presenta la guerra cognitiva.

De otra parte, en las guerras cognitivas es esencial identificar, desde muy temprano, las primeras acciones del adversario, aprender rápido, difundir el nuevo conocimiento, adaptarse y hacer el enfrentamiento de amenazas en el ambiente complejo de nuestros días. En este sentido, las Fuerzas tienen un sistema de educación propio, que puede realizar estas tareas y mejorar sus respuestas cinéticas y no cinéticas, incorporando nuevos conocimientos que las hacen capaces de fortalecerse ante cada ataque.

Los sistemas de comunicación social

El sistema de comunicación interna puede actuar rápidamente y alcanzar ampliamente lo efectivo, de modo que se pueda refutar información falsa con el potencial de influir negativamente en la moral de la tropa. Los mismos canales comunicativos pueden ser utilizados para difundir y mantener actualizada la narrativa establecida por la institución en alineación con las políticas estatales para el sector (Giraldo y Cabrera, 2020).

Las campañas internas para fortalecer el liderazgo en sus diversos niveles y la confianza mutua entre los funcionarios ayudan a prevenir (o al menos reducir) los efectos de las acciones externas destinadas a desestabilizar las instituciones.

Los sistemas de apoyo y asistencia social

Los servicios de apoyo y asistencia social, destinados a asistir a los militares y sus familias, ayudan a reducir los niveles de insatisfacción en el personal, y así facilitan que estos sean menos vulnerables a las acciones de guerra cognitiva que persigan crear división interna. De igual manera, permiten acciones en el campo psicosocial del personal, con las cuales se logra el fortalecimiento de los vínculos entre los individuos y sus instituciones para así reducir las influencias externas que pueden amenazar la cohesión interna o hasta la misma voluntad de luchar de los hombres y mujeres que componen las FF. AA.

En este sentido, para Fukuyama (2019), la concepción de lo que es la dignidad humana ha ido cambiando a lo largo de los años en la cultura occidental, adoptando enfoques religiosos, filosóficos o psicológicos, según el grupo social al que pertenezca o se sienta vinculado el individuo. Fue utilizada como soporte de argumentación o justificación de diferentes corrientes políticas e ideológicas en diferentes países. Está directamente relacionada con conceptos importantes como el reconocimiento (personal y colectivo), la identidad y el resentimiento.

El mantenimiento de la percepción de los individuos cerca de su condición de dignidad, de ser apoyado y acogido por las instituciones, es un factor preventivo muy fuerte ante las tentativas externas de crear fracturas y divisiones que puedan quebrantar la unidad y cohesión de las Fuerzas.

En este orden de ideas, los servicios organizados de asistencia social, a través de organizaciones públicas o privadas, pueden representar la materialización de la legítima intención de los comandantes de generar acciones de apoyo efectivo a los integrantes de las FF. AA. o a sus familiares. Este reconocimiento del valor y la importancia del individuo, especialmente en los momentos de mayor necesidad o fragilidad social, puede representar el fortalecimiento de los vínculos personales (emocionales) entre la institución y sus integrantes.

Las oficinas y asesorías jurídicas institucionales

El fenómeno del activismo jurídico, una realidad demostrada por Mejía y Pérez (2015), juntamente con el litigio estratégico, constituyen amenazas u obstáculos a la normal actuación de los agentes públicos. Los dos fenómenos, sumados a la excesiva judicialización de litigios de cualquier naturaleza, generan una verdadera guerra jurídica en contra de las FF. AA. en Colombia.

Todo este conjunto crea un ambiente de disuasión parcial contra las acciones estatales destinadas a mantener el orden público, en la medida que tanto militares como policiales, podrían reducir sus iniciativas debido a la sensación de inseguridad jurídica o no protección frente a constantes cuestionamientos legales. Padilla (2012), al hacer un análisis de la realidad colombiana, declara que:

La guerra jurídica se está convirtiendo rápidamente en un factor clave en un intento de destruir la voluntad de lucha del Estado al socavar la legitimidad de las autoridades y el apoyo popular requerido para mantener un gobierno efectivo y emplear el poder militar (p. 136).

Un punto importante del enfrentamiento de esta amenaza es el mantenimiento de una cultura institucional de regulación constante de las acciones operativas y administrativas, con el fin de crear referencias más seguras para las diversas actividades de los miembros de las FM. MM. Como buenas prácticas ya existentes, podemos mencionar los sectores de doctrina y lecciones aprendidas en funcionamiento, que transforman experiencias vividas y observadas en estandarización. Tales normas o reglamentos, debidamente ajustados al marco jurídico vigente, contribuyen directamente a aumentar la sensación de seguridad de los funcionarios públicos (militares y civiles).

Las autoridades civiles y militares necesitan hacer la correcta preparación legal del campo de combate. Los conflictos se están volviendo muy legalistas y complejos, con grande exposición en diversos canales de comunicación, por lo que los comandantes deben tener en cuenta que el concepto de la operación planificada se limita dentro del marco legal. La

disponibilidad de asesoramiento legal en tiempos oportunos es extremadamente necesaria para mejorar la adherencia de los procedimientos a las normas vigentes (Padilla, 2012).

Los sistemas de gestión y protección del patrimonio cultural e histórico

Moisi (2009) nos habla de la importancia de la llamada localización emocional como factor de gran influencia en las actitudes colectivas, con efectos directos en el posicionamiento político de países y grupos de influencia. Regiones, monumentos, templos y espacios físicos con imagen conocida y posición geográfica de influencia innegable y valor en el imaginario colectivo, tienen potencial para uso político. Vandalizar un templo de cierta religión, destruir la estatua de un personaje ícono de la historia, ocupar una plaza que es un punto de encuentro de los ciudadanos de una ciudad, entre otras acciones, tienen el potencial de lograr influir o incluso provocar los valores colectivos de la sociedad. El simple abandono de sitios con valor histórico y cultural puede representar, a mediano y largo plazo, una forma de reducir la percepción del sentido colectivo de identidad común.

Por lo tanto, identificar y preservar las ubicaciones emocionales puede ser un paso importante hacia el fortalecimiento de las identificaciones culturales y los sentidos de pertenencia y, por lo tanto, reducir los riesgos de fragmentación social. Puesto que las Fuerzas Militares tienen una rica colección histórica de monumentos performáticos y arquitectónicos, resultado de su estabilidad y continuidad a través de los siglos como instituciones permanentes del Estado, el mantenimiento y la difusión interna y externa de dicha colección puede ser un factor crítico para el fortalecimiento de su identidad como instituciones, con un efecto en la identidad de la Nación en su conjunto.

Del mismo modo, el registro histórico de los hechos, circunstancias, acciones y demás información relevante relacionada con las Fuerzas Militares y policiales necesita una atención especial. Actualmente hay buenas iniciativas en marcha, como los museos militares y policiales, al igual que los centros de memoria histórica. Estos programas sistémicos de tala histórica deben incorporarse definitivamente en las políticas de alto nivel de las FF. AA. como una forma de protección contra la creación y manipulación de narrativas por parte de grupos de interés que tienen cualquier objetivo de atacar la legitimidad y la imagen institucional. Según Garzón (2022):

Ciertamente, no existe un modo correcto que permita distinguir de antemano los buenos y los malos usos del pasado, lo cual nos previene contra dos formas de instrumentalización de la memoria: primero, que “el culto a la memoria no siempre sirve para las buenas causas”; y segundo, que “el culto a la memoria no siempre sirve a la justicia”. Las políticas de la memoria, como cualquier política, pueden estar al servicio de fines mezquinos como la posverdad, el partidatismo electoral o el odio tribal (p. 26).

Tener la estructura para crear y mantener su propia política de memoria a nivel institucional es una gran ventaja estratégica de las FF. AA., en la medida que permite acciones planeadas y coordinadas en términos de largo plazo, evitando las oscilaciones de visión y los partidismos y teniendo disponibilidad de recursos, entre otros factores inherentes a los cambios naturales de gobiernos dentro de la realidad política colombiana.

Hecha una revisión propositiva acerca de las capacidades no cinéticas inherentes a las fuerzas de seguridad de Colombia, se puede aterrizar en las siguientes conclusiones que nos permiten comprender el posible papel de las FF. AA., considerando el análisis basado en factores observables y literatura disponible.

Conclusiones

El presente trabajo establece que la guerra cognitiva es aquella que se libra en la mente y busca no solamente influir en lo que piensan, sino también en cómo actúan las personas, y cuyos propósitos principales son la influencia en las políticas públicas y la desestabilización de las instituciones de una nación. De modo que, para cumplir con sus propósitos de influenciar y desestabilizar, la guerra cognitiva tiene una serie de componentes de tipo no cinético tales como operaciones psicológicas, operaciones de información y operaciones cibernéticas, que se ejecutan en un ambiente cada vez más urbano.

En ese ambiente crecientemente urbano, las operaciones psicológicas persiguen controlar lo que sienten las personas, las operaciones de información buscan controlar lo que ve la población objetivo y las operaciones cibernéticas intentan interrumpir sus capacidades tecnológicas. Es decir, todas en conjunto aportan a la guerra cognitiva, la cual se enfoca en influir cómo piensa y como actúa la población objetivo, para finalmente desestabilizarla.

A diferencia de los otros tipos de guerras cuyo objetivo es imponerle nuestra voluntad a un adversario, la guerra cognitiva pretende que el enemigo se destruya a sí mismo desde adentro, lo que podría interrumpir la dinámica de la trinidad de Clausewitz y haría implosionar a una sociedad entera. En este sentido, la guerra cognitiva persigue dos objetivos principales: primero, influir en la manera como piensan las personas individual o colectivamente y así manipular sus actuaciones; segundo, desestabilizar a un grupo o a toda una sociedad, al punto de quebrantar su voluntad de lucha, para así permitir que el agresor los someta sin recurrir al uso de fuerza cinética o a la coerción directa.

En el campo individual, la guerra cognitiva busca: a) alterar las percepciones de las personas y así modificar cómo piensan, sienten y actúan; b) controlar sus estados mentales; c) modificar lo que estas saben o piensan que saben; d) moldear o cambiar sus creencias.

A nivel grupal o de la sociedad, la guerra cognitiva persigue: a) manipular el discurso público; b) socavar la unidad social; c) dañar la confianza en un sistema político o una ideología; d) desestabilizar instituciones o, incluso, una nación entera.

De otra parte, las nuevas tecnologías sumadas a las redes sociales han permitido la aparición y propagación de fenómenos como las noticias falsas, la desinformación y la posverdad, las cuales se convierten en nuevas amenazas para la seguridad y defensa nacionales, en razón a que contribuyen a la consecución de los objetivos que la guerra cognitiva persigue: influir en las personas y desestabilizar a las sociedades.

Con la implementación del acuerdo de paz con las FARC-EP en 2017, actores estatales y no estatales le han declarado una guerra cognitiva a Colombia, con la cual, a través de acciones no violentas, buscan influenciar en el pensamiento de las personas y la desestabilización de la Nación y sus instituciones. Finalmente, las FF. AA. colombianas y sus diferentes capacidades deberán asumir los desafíos de la guerra cognitiva por medio de una estrategia para combatir este nuevo tipo de guerra. Dentro de dicha estrategia, un primer paso puede ser identificar las amenazas, las capacidades institucionales y las posibilidades de enfrentamiento. Un segundo paso consiste en establecer las dimensiones en que se podrían generar acciones para enfrentar amenazas y ataques de tipo cognitivo.

El conjunto de capacidades y estructuras existentes en la composición de las instituciones militares del país les permite tener la resiliencia suficiente para enfrentar las nuevas amenazas que supone la guerra cognitiva. Sin embargo, se debe realizar un amplio estudio para detallar posibles nuevas amenazas y establecer una correlación acertada con las capacidades existentes.

Las inversiones en las capacidades no cinéticas que consoliden la identidad institucional son hoy un factor crítico para posibilitar la resiliencia en un entorno de guerra cognitiva. La suma que implica la importancia institucional de las Fuerzas Militares para el mantenimiento de la estabilidad nacional, con su resiliencia frente a los ataques en los campos de la información y cognitivos, hace de las FF. AA. un pilar esencial en el apoyo al país en un ambiente de guerra cognitiva.

Las observaciones y reflexiones contenidas en este trabajo deben ayudar a los responsables de la preparación y el empleo de las FF. MM. y de otras fuerzas de seguridad del Estado, respecto a la necesidad de adaptarlas a los nuevos roles que estas desempeñarán, ante el nuevo tipo de amenazas que plantea la guerra cognitiva.

La confianza mutua entre los elementos esenciales de la trinidad de Clausewitz (Estado, pueblo y fuerzas militares) es un blanco en constante riesgo en tiempos de guerra cognitiva, cuando la verdad es atacada y la democracia sigue amenazada. El momento de prepararse es ahora y todo el mundo está observando.

Recomendaciones

Como consecuencia del presente estudio, se podrían presentar las siguientes recomendaciones:

- A la Escuela Superior de Guerra: evaluar la posibilidad de implantar una línea de estudios acerca de la dimensión cognitiva de los conflictos con afectación en la defensa y la seguridad nacionales.
- Al Comando General de las Fuerzas Militares: evaluar la posibilidad de incluir en sus políticas una mayor atención al acompañamiento y monitoreo de las condiciones psicológicas, de opinión y de sentimientos colectivos de los integrantes de las FF. MM., cuando se presenten ataques de tipo cognitivo. Así mismo, incluir en sus políticas una nueva visión más amplia e integrada acerca de las capacidades no cinéticas de las instituciones militares y de policía, considerando las nuevas amenazas del campo cognitivo en los ámbitos externo e interno. El arte y diseño operacional podría brindarles a las FF. MM. la oportunidad para conocer más a fondo este nuevo tipo de guerra y así establecer las medidas para combatirla.

Referencias

- Abbott, D. (2010). *The Handbook of Fifth-Generation Warfare*. Ann Arbor: Nimble Books.
- Álvarez, C. E. (2022). *Estudios de la guerra y los conflictos. Guerras de 5ª generación*. Bogotá: Escuela Superior de Guerra.
- Álvarez, C. E.; Barón, P. y Monroy, V. (2019). *Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa. Vol. 1*. Bogotá: Sello Editorial ESMIC.
- Álvarez Fernández, C. E.; Santafé García, J. F. y Urbano Morales, O. J. (2017). *Escenarios y desafíos de la seguridad multidimensional en Colombia*. Bogotá: Escuela Superior de Guerra.
- Backes, O. y Swab, A. (2019). Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. *Policy Analysis Paper, Belfer Center for Science and International Affairs*. Recuperado de: <https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states>
- Barrera-Herrera, O. F.; Hernández-Cubides, J. A. y Ramírez-Pedraza, Y. E. (2021). Ética militar en el marco de guerras de quinta generación: propuestas teóricas para reestructurar la educación en instituciones militares. En J. Jiménez-Reina, E. C. Figueroa-Pedrerós y M. Bricknell [Eds], *Ética militar y nuevas formas de guerra. Retos para las Fuerzas Armadas colombianas* (pp. 177-207). Bogotá: Escuela Militar de Cadetes José María Córdova.
- Begue, M. (10 de mayo de 2021). How fake news affects protesters in Colombia. *CGTN America*. Recuperado de: <https://america.cgtn.com/2021/05/10/how-fake-news-affects-protesters-in-colombia>
- Bernal, A.; Carter, C.; Singh, I.; Cao, K. y Madreperla, O. (2020). *Cognitive Warfare. An Attack on Truth and Thought*. Johns Hopkins University y North Atlantic Treaty Organization.
- Bilal, A. (30 de noviembre de 2021). Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review*. Recuperado de: <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>
- Bufacchi, V. (24 de enero de 2020). What's the Difference between Lies and Post-Truth in Politics? A Philosopher Explains. *The Conversation*. Recuperado de: <https://>

theconversation.com/whats-the-difference-between-lies-and-post-truth-in-politics-a-philosopher-explains-130442

- Clausewitz, C. (1989). *On War* (first paperback printing). Princeton, N.J.: Princeton University Press.
- Claverie, B; Prébot, B.; Buchler, N. y Du Cluzel, F. (2022). *Cognitive Warfare: The Future of Cognitive Dominance*. Bourdeaux: Science and Technology Organization North Atlantic Treaty Organization.
- Costa, D. (2018). Guerra psicológica nos novos tipos de guerra. *Revista Silva, Humanidades em Ciências Militares*, 2(2), 17-32.
- Davis, D.; Kilcullen, D.; Mills, G. y Spencer, D. (2016). *A Great Perhaps? Colombia: Conflict and Convergence*. Londres: Hurst & Company.
- Dimock, M. y Gramlich, J. (29 de enero de 2021). How America Changed During Trump's Presidency. *Pew Research Center*. Recuperado de: <https://www.pewresearch.org/2021/01/29/how-america-changed-during-donald-trumps-presidency/>
- Ellis, R. E. (2021). El fortalecimiento de las actividades del ELN (Ejército de Liberación Nacional) en Colombia y Venezuela. *Revista Fuerza Aérea EUA*, 2, 24-45.
- Fukuyama, F. (2019). *Identidad. La demanda de dignidad y las políticas de resentimiento*. Bogotá: Ariel.
- Fuller, S. (2018). *Post-truth: knowledge as a power game*. Nueva York: Anthem Press.
- Garzón Vallejo, I. (2022). *El pasado entrometido. La memoria histórica como campo de batalla*. Bogotá: Crítica.
- Giraldo-Bonilla, H. F. y Cabrera-Ortiz, F. [Eds.] (2020). *Estrategia de diplomacia pública y comunicaciones estratégicas para la defensa multidimensional de Colombia 2020-2030*. Bogotá: Sello Editorial ESDEG.
- Giusti, S. y Piras, E. [Eds.] (2021). *Democracy and fake news: information manipulation and post-truth politics*. Abingdon y Nueva York: Routledge.
- Global Americans. (18 de noviembre de 2021). *Measuring the impact of misinformation, disinformation, and propaganda in Latin America*. Recuperado de: <https://theglobalamericans.org/2021/11/disinformation-latin-america/>
- Headquarters, Department of the Army. (2005). *FM 3-05.30. Psychological Operations*.
- Headquarters Department of the Army. (2010). *TC 7-100, Hybrid Threat*.

- Headquarters, Department of the Army. (2016). *FM 3-13. Information Operations*.
- Hoffman, F. G. (2007). *Conflict in the 21st Century*. Arlinton: The Potomac Institute for Policy Studies.
- Humire, J. (2022). *El impacto en América Latina de las acciones rusas*. Presentado en el webinar “Guerra en Ucrania”, marzo 3, Santiago de Chile.
- Hung, T-Ch. y Hung, T-W. (2022). How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars. *Journal of Global Security Studies*, 7(4). <https://doi.org/10.1093/jogss/ogac016>
- Jackson, D. (17 de octubre de 2017). Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News’. *National Endowment for Democracy*. Recuperado de: <https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/>
- Johns Hopkins University e Imperial College London. (20 de mayo de 2021). Countering cognitive warfare: awareness and resilience. *NATO Review*. Recuperado de: <https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html>
- Keller, F. B.; Schoch, D.; Stier, S. y Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, 37(2), 256-80. DOI: 10.1080/10584609.2019.1661888
- Klepper, D. (9 de agosto de 2022). Russian disinformation spreading in new ways despite bans. *AP News*. Recuperado de: <https://apnews.com/article/russia-ukraine-misinformation-european-union-government-and-politics-e5a1330e834fde428aab599b5c423530>
- Lawrence, A.; Crespi, M.; David, A.; Gegov, A.; Giordano, J. y Guillory, S. (2021). *Cognition Workshop. Innovative Solutions to Improve Cognition*. NATO.
- Lind, W. S.; Nightengale, K.; Schmitt, J. F. y Sutton, J. W. (1989). The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*, 22-26. Recuperado de: <https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html>
- Malamud, M. (2014). El nuevo “militar flexible”. *Revista Mexicana de Sociología*, 76(4), 639-663. Recuperado de: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032014000400005&lng=es&tlng=es

- Mejía, J. y Pérez, R. (2015). Activismo judicial y su efecto difuminador en la división y equilibrio de poderes. *Justicia*, 27, 30-41.
- Moisi, D. (2009). *La geopolítica de las emociones. Cómo las culturas del miedo, la humillación y la esperanza están reconfigurando el mundo*. Bogotá: Editorial Norma.
- O'Grady, M. A. (30 de enero de 2022). Putin Is Already in Cuba and Venezuela. *WSJ Opinion*. Recuperado de: <https://www.wsj.com/articles/putin-is-already-in-cuba-and-venezuela-south-america-influence-western-hemisphere-ukraine-11643567547>
- Ottewell, P. (7 de diciembre de 2020). Defining the Cognitive Domain. *Over The Horizon*. Recuperado de: <https://othjournal.com/2020/12/07/defining-the-cognitive-domain/>
- Padilla, J. M. (2012). Guerra jurídica: el caso colombiano. *Revista Científica General José María Córdova*, 10(10), 107-142. Recuperado de: <https://revistacientificaesmic.com/index.php/esmic/article/view/230>
- Pastrana Buelvas, E.; Reith, S. y Cabrera Ortiz, F. [Eds] (2020). *Identidad e intereses nacionales de Colombia*. Bogotá: Fundación Konrad Adenauer, KAS.
- Polyakova, A. y Meserole, C. (2019). Exporting Digital Authoritarianism: The Russian and Chinese Models. *Policy Brief, Foreign Policy at Brookings Institution*. Recuperado de: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf
- Qiao, L. y Wang, X. (1999). *Un-Restricted Warfare*. Beijing: PLA Literature and Arts Publishing House.
- RAND Corporation. (2022). *Information Operations*. Recuperado de: <https://www.rand.org/topics/information-operations.html>
- Ratto, A. (2015). *Rousseau: el hombre es bueno por naturaleza, pero la sociedad lo corrompe*. Barcelona: RBA.
- Rosner, Y. y Siman-Tov, D. (8 de marzo de 2018). Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion. *INSS*. Recuperado de: <https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/>
- Schmid, A. P. [Ed.] (2013). *The Routledge Handbook of Terrorism Research* (first published in paperback). Londres y Nueva York: Routledge, Taylor & Francis Group.

Sharp, G. (2010). *From Dictatorship to Democracy: A Conceptual Framework for Liberation*. Boston: Albert Einstein Institution.

Stent, A. (27 de enero de 2022). The Putin Doctrine. *Foreign Affairs*. Recuperado de: <https://www.foreignaffairs.com/articles/ukraine/2022-01-27/putin-doctrine>

The Senate. (2020). *Report of the select committee on intelligence United States Senate on Russian active measures campaigns and interference in the 2016 U.S. election*.

Universidad a Distancia de Madrid. (2015). *La violencia organizada en el siglo XXI*. Recuperado de: <https://www.youtube.com/watch?v=4xYxZY-lRoU>