

Capítulo 8

Impacto estratégico de las operaciones de desinformación y la respuesta efectiva de las Fuerzas Militares en el siglo XXI*

DOI: <https://doi.org/10.25062/9786287602809.08>

Humberto Andrés Niño Vergara

Miguel Antonio González Martínez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La desinformación es un recurso que se ha utilizado en diferentes momentos para afectar la estabilidad política y administrativa en una sociedad. En los niveles operacional y táctico se produce para entorpecer los procesos de las Fuerzas, específicamente para dificultar la conducción de las operaciones militares y provocar un esfuerzo mayor por parte de la Inteligencia militar en el procesamiento de información para la toma de decisiones del mando. Entre los diferentes medios utilizados en esta área, por ejemplo, se difunde información sacada de contexto, noticias falsas, se afectan los activos informáticos mediante operaciones cibernéticas, entre otros. Dado que sus efectos son disímiles, se debe analizar a partir de su impacto en cada nivel de las Fuerzas Militares para establecer una estrategia. En cualquier caso, las Fuerzas Militares requieren de fundamentos doctrinales soportados por una estructura organizacional capaz de gestionar la desinformación según el impacto en cada nivel.

Palabras clave: desinformación; doctrina; Ejército Nacional de Colombia; Fuerzas Especiales; nuevas guerras.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Humberto Andrés Niño Vergara

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Administrador de Empresas, Universidad Nueva Granada. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Contacto: humberto.nino@buzonejercito.mil.co

Miguel Antonio González Martínez

Doctorando en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Historia, Universidad Nacional de Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Docente e investigador, Departamento Ejército, Escuela Superior de Guerra "General Rafael Reyes Prieto", y docente del Programa de Relaciones Internacionales y Estudios Políticos FAEDIS, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-6034-912X> - Contacto: miguel.gonzalez@esdeg.edu.co

Citación APA: Niño Vergara, H. A., & González Martínez, M. A. (2024). Impacto estratégico de las operaciones de desinformación y la respuesta efectiva de las Fuerzas Militares en el siglo XXI. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 189-208). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.08>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

La desinformación surge como un fenómeno emergente en los conflictos contemporáneos que tiene impacto en la estructura social y política. Por medio de estas acciones se promueve la consecución de fines políticos y se propicia el espacio para que converjan diferentes factores que atentan contra el poder del Estado, el monopolio de la Fuerza, la estabilidad de los gobiernos y el imperio de la ley.

En el presente capítulo se analizan tres aspectos fundamentales que estructuran el hilo conductual del trabajo. Primero, el concepto y la teoría de las operaciones de desinformación y su impacto estratégico a nivel internacional. En segundo lugar, se analiza el papel de las Fuerzas Militares frente a las operaciones de desinformación, bien sea para prevenir su aparición o disipar su impacto estratégico. Finalmente, como tercer punto, se estudian los fundamentos operacionales para las Fuerzas Especiales (FF. EE.) frente a las operaciones de desinformación.

A lo largo de este recorrido se recogen los conceptos doctrinales que permitirán a las FF. EE. en Colombia entender el contexto en cual los actores armados al margen de la ley lanzan operaciones de desinformación para producir una respuesta oficial, legítima, efectiva y oportuna. Por medio de esta, se busca determinar la responsabilidad o el papel que deben desempeñar las FF. EE. en el mantenimiento del orden constitucional y la defensa del Estado, tras la influencia de otros actores que buscan desestabilizarlo.

Metodológicamente, se desarrolló una investigación de carácter cualitativo, en la cual se emplearon fuentes primarias en documentos disponibles. Según Hernández Sampieri et al. (2010), existen diversas realidades subjetivas, las cuales varían en su forma y contenido entre individuos, grupos y culturas. Por ello, el investigador cualitativo parte de la premisa de que el mundo social es “relativo” y solo puede ser

entendido desde el punto de vista de los actores estudiados. Dicho de otra forma, el mundo es construido por el investigador (Hernández et al., 2010, p. 11).

Esta perspectiva metodológica encaja con la teoría en la medida en que el capítulo dialoga con el mundo contemporáneo propio de la era posmoderna, en cuya agenda se propone desmitificar los discursos (científicos, artísticos y culturales) de la modernidad que moldearon y construyeron la realidad presente, a la vez que se asume una postura crítica frente al positivismo científico del siglo XIX. Sin duda, la incursión de la lingüística con la obra de Ferdinand de Saussure, *Curso de lingüística general* (1919), abrió una nueva perspectiva interpretativa en la forma de comprender los eventos culturales y los hechos sociales. De esta manera, muchos investigadores tomaron el estructuralismo como el marco teórico de sus investigaciones influidos por la teoría del *signo lingüístico* que propuso el lingüista francés. Posteriormente, Jacques Derrida integró la noción de la “deconstrucción” de los discursos, con lo cual dio vigencia a la lucha por la verdad: por el discurso legítimo a partir del lugar de enunciación del cual emergen.

Con estas nuevas lecturas intertextuales de la realidad, aunado al fenómeno de la globalización y su profundización con la masificación del internet, se ha allanado el camino hacia una libre interpretación en la comunicación, e incluso la incorporación de neologismos como el de la *posverdad*, el cual trae al debate, finalmente, el afán por la lucha de la verdad en un mundo cada vez más volátil, complejo, incierto y ambiguo.

La desinformación

La desinformación son actividades enfocadas en difundir información falsa, mal informar e incluso desinformar a la audiencia, potencializadas en el mundo contemporáneo por la globalización y la llegada de las tecnologías de la información y comunicaciones (TIC), las cuales facilitan el acceso y la publicación de la información, con el efecto colateral de que dificultan su control. Las redes sociales (Facebook, Twitter –ahora X–, TikTok, WhatsApp, etc.) desempeñan un papel central en este fenómeno gracias a que en los últimos años se ha democratizado el acceso a internet, de manera que la población ha encontrado en estas un vehículo expedito para comunicar ideas, pensamientos, emociones, reacciones, entre otros, a gran escala y en tiempo real, sin que exista un filtro efectivo para establecer la veracidad de la comunicación y evaluar si proviene de una fuente certificada (el caso de los *bots* –programas informáticos–). Se configura así en el marco de la

posmodernidad un fenómeno paradójico: en plena era de la información, crece la desinformación de modo exponencial a partir de la instrumentalización de amplias audiencias que abarcan diferentes sectores de la población, los cuales reciben mensajes con gran rapidez, difunden el material a un costo muy bajo y con una facilidad que burla las condiciones de veracidad.

Sociológicamente, el consumo y la propagación de material de desinformación se explica a partir de la reafirmación de la identidad de la persona, que ve en el contenido la representación de su pensamiento, sin reparar en su procedencia o realismo. Esta conducta se puede reforzar debido a los sesgos cognitivos del receptor del mensaje; por ejemplo, si una persona tiene una preferencia por una determinada corriente política, tendrá una tendencia natural a creer, sin un juicio crítico previo, las noticias que refuercen su pensamiento.

Es así como esta "revolución tecnológica" aplicada al campo de la información ha impactado en diferentes esferas de la vida pública como la cultura, la economía y la política, de manera que la desinformación afecta todo tipo de emociones que se materializan en la acción política y/o en los movimientos sociales. El ámbito militar no es ajeno a este fenómeno, pues al conducir una función primordial del Estado, su defensa y seguridad, está en constante riesgo de verse afectado por operaciones de desinformación que buscan promover la inestabilidad social y afectar al Gobierno. Por esta razón, la fuerza pública debe generar condiciones de seguridad de la información para proteger los sistemas oficiales y contrarrestar los mensajes en contra del orden institucional.

Este escenario ha promovido una transición en la estrategia de despliegue hacia una visión de las instituciones oficiales en la que, justamente, la información es uno de los ejes principales (Sierra, 2003). Al igual que los recursos naturales, el medioambiente y las personas, la información se pueden entender como un activo estratégico de los Estados, pues la mala gestión de la desinformación puede traer como consecuencia altos costos políticos, económicos, sociales, entre otros.

Un antecedente de los efectos que puede tener la desinformación se encuentra en la Guerra Fría, en la cual las dos potencias dominantes del sistema internacional emplearon todos los medios posibles para contener el avance del sistema adversario, en medio de la pugna de las fuerzas ideológicas entre capitalismo y comunismo. A la sazón, ya existía la experiencia de la propaganda que los dos bandos usaron durante la Segunda Guerra Mundial para legitimar y promover, ante la opinión pública, las acciones políticas y bélicas en el marco de la guerra. El auge y la masificación de los medios de comunicación como la prensa, la radio y el cine

tuvieron un papel trascendental en la movilización de las voluntades en contra de los adversarios en contienda.

En los años 50, las tácticas de desinformación se constituyeron en un elemento formal, con agencias especiales cuyo propósito era desprestigiar a los Estados Unidos y sus aliados en beneficio del comunismo a nivel global. Como efecto, los norteamericanos diseñaron estrategias para contrarrestar los ataques de la URSS, modificando la política exterior en torno a la información y su impacto en los países aliados, su capacidad de influir en los adversarios y desplazando el uso de la fuerza. De esta manera se consolidó la Oficina de Defensa Estratégica, cuyo objetivo era desarrollar tácticas de desinformación en las relaciones internacionales del Estado (Rodríguez, 2017).

En síntesis, la desinformación tiene el propósito de afectar la estabilidad de un Estado, para lo cual trata de deteriorar el reconocimiento y la reputación de las instituciones oficiales difundiendo mensajes de odio y/o miedo. En la actualidad, uno de los países que más ha utilizado esta estrategia es Rusia, cuya intervención se ha consolidado sobre la base de los siguientes puntos críticos:

- Realizar operaciones maliciosas en medios sociales.
- Entregar desinformación por medio de métodos tradicionales de divulgación como radio y televisión.
- Influir en la opinión pública para generar aliados que defiendan su posición y compartan sus ideas frente al adversario. Para esto han utilizado sobre todo las conferencias.
- Conducir operaciones cibernéticas para dañar la percepción de los medios de comunicación.
- Hackear y divulgar información (U. S. Department of State, 2022b).

De igual manera, al investigar qué información ha tratado de posicionar, se encontró lo siguiente:

- Rusia, por ejemplo, en el conflicto con Ucrania actúa motivado por la victimización de su adversario.
- Volver a acontecimientos históricos para estigmatizar a sus oponentes o resaltar sus acciones heroicas en el pasado.
- Criticar la cultura occidental para generar incertidumbre.
- Atacar los movimientos populares y demás expresiones de inconformismo como un acto de influencia realizado por sus adversarios militares y políticos.
- Construir realidades que favorezcan su posición, crear confusión y desmoralizar al adversario (U. S. Department of State, 2022b).

De esta manera, no solo se pretende afectar la protección de la información directamente relacionada con datos oficiales, redes financieras, plataformas que permiten el trabajo del sector público y privado, entre otros ciberdelitos, sino que además se busca controlar posibles estrategias de guerra psicológica e influir en la sociedad. El internet es un recurso a disposición tanto de la información como de la desinformación, toda vez que, por un lado, permite filtrar información a velocidades extraordinarias, y por otro, facilita operaciones de desinformación para afectar un objetivo (Sierra, 2003).

Este panorama arroja una *guerra de la información*, la cual consiste en acciones dirigidas a crear y mantener la superioridad de la información, mientras se protegen los sistemas propios. En la actualidad, este tipo de guerra presenta una amplia gama de estrategias debido a que la revolución tecnológica generó nuevas amenazas, ya que diferentes grupos y entidades oficiales pueden adquirir los medios para afectar la reputación y la estabilidad de la información, e incluso robarla, borrarla, modificarla o espiarla (López, 2007).

Entonces, esta guerra de la información alimenta un concepto de guerra que no implica el uso de una boca de fuego y que se convierte en un tipo de amenaza clásico en el campo de la guerra híbrida. En este escenario, se utilizan diferentes elementos de carácter económico, político, diplomático, entre otros, para afectar la confianza del adversario, generar condiciones sociales adversas en procura de promover manifestaciones violentas, obstaculizar la reacción de los gobiernos haciendo que su sistema de gestión sea frágil y legitimar el uso de la fuerza o, incluso, considerarla necesaria (LISA Institute, 2019). Y es de este modo que las operaciones de desinformación se convierten en una modalidad de amenaza híbrida y un potencial detonante de un conflicto convencional. En cualquier caso, su finalidad es afectar a un adversario político.

Esta amenaza híbrida va de la mano con la propaganda de guerra constante en publicaciones que buscan movilizar a las personas y desacreditar al oponente. Claramente, la propaganda de guerra, al igual que la información, ha evolucionado al ritmo de la tecnología de la información (Noguera, 2013), razón por la cual se emplean las mismas prácticas: difundir estrategias falsas y utilizar la credibilidad del público. En resumen, consiste en emplear operaciones maliciosas, utilizar la desinformación y otro tipo de mecanismos para desestabilizar al enemigo (Medina, 2022).

Como se ha visto, la desinformación es el conjunto de estrategias para generar beneficio propio y dañar a un oponente. En este sentido, la información que se entrega ya tiene un objetivo específico, razón por la cual ya está tergiversada (Ustarroz, 2021).

Otros autores definen la desinformación como la información carente de exactitud o manipulada que, en cualquier caso, es difundida con una intención maliciosa; entre esta se encuentran las noticias falsas y las historias imprecisas (Rini, 2017).

La desinformación puede ir acompañada de mensajes sensacionalistas que tienen gran acogida e impacto social; en algunos casos, también de imágenes que generan un gran efecto psicológico para provocar un sentimiento de miedo, odio, rechazo, aprobación o exaltación, según el objetivo de la operación. Este método en particular se usa desde los tiempos de la radio y se ha comprobado su poder, a tal punto que se acuñó el concepto de *infodemia* (Arteaga, 2020). Su objetivo, más allá de la victoria militar, es alcanzar el poder político aprovechando las variadas emociones que fomenta en la población. Esta modalidad ha sido ampliamente utilizada por los rusos, quienes han buscado sacar provecho de la difusión de noticias falsas y de la información manipulada para imponer su visión del mundo, someter al adversario, cumplir sus objetivos y validar su intervención militar (U. S. Department of State, 2021).

En todo caso, la finalidad de la desinformación promueve un grupo de creencias, una posición política, una imagen y el reconocimiento de una figura política o, incluso, en algunos casos, busca afectar la percepción de un adversario mediante la difusión de información. La guerra de la información se consolida sobre la base de los instintos primarios de la humanidad, los cuales desencadenan una estructura de violencia organizada (Contreras, 2001).

El impacto de estas operaciones es estratégico, en la medida en que produce alteraciones sociales porque van dirigidas a los miedos de la humanidad. Una estrategia en este sentido es generar repulsión contra el enemigo por la violación de los Derechos Humanos o afectación de valores sociales según el imaginario de cada cultura. Estas operaciones de desinformación generan incluso contenido cien por ciento falso para generar repulsión (U. S. Department of State, 2022a).

Además, uno de los aspectos que hacen que este tipo de amenazas híbridas sea tan efectivo es que los agresores permanecen en el anonimato, lo cual dificulta identificar de dónde provienen las amenazas (Arteaga, 2020). Este punto es un elemento central de la doctrina rusa, en la cual se considera fundamental el empleo de una guerra psicopolítica denominada *maskirovka*, en ruso *маскировка*, que busca engañar al enemigo con técnicas de ocultamiento, simulación y difusión de noticias falsas. De esta manera, "las prácticas de *maskirovka* a escala militar incluyen [...] manejo del lenguaje [...] así, por ejemplo, la palabra *ofensiva* ha desaparecido totalmente del vocabulario militar soviético y ha sido remplazada por eufemismos tales como *movimiento*, *salida* o *defensa*" (Antoine, 2019, p. 21).

La desinformación no solo genera un impacto en la audiencia, influyendo sus emociones y sentimientos frente a sus valores sociales y miedos, sino que también se caracteriza por su origen incierto, intención e impacto, lo cual la convierte en una herramienta poderosa a nivel internacional. Y es que se desconoce quién entrega la información, si todos los datos son falsos o si, por el contrario, hubo una tergiversación, si se sacó del contexto en el que realmente ocurrieron los hechos o si se están manipulando para favorecer un interés político determinado (Arteaga, 2020).

Normalmente, al comunicar cualquier tipo de información se enfrenta el reto de que el mensaje se reciba de la manera y con el propósito que se definió cuando se decidió hacerlo. En el ambiente militar, esto genera mayor impacto, ya que un escenario contaminado de incertidumbre, discrepancias o errores en la interpretación obstaculiza la toma de decisiones y, por lo tanto, debilita la capacidad de reacción (Guzmán, 2019).

Hay dos conceptos que inicialmente convergen en este punto: las noticias falsas o *fake news* y las operaciones maliciosas. Específicamente, las *fake news* se refieren a aquellas noticias a las que se les puede comprobar la falsedad, pero que no implican necesariamente una intención perversa, pues también pueden ser consecuencia de un mensaje mal comunicado, un error en la fuente de la información, entre otros. A diferencia de las operaciones de desinformación, las *fake news* se presentan de manera aleatoria y casi por casualidad, mientras que la desinformación se calcula en contra de un grupo y reúne esfuerzos conscientes (Paladino et al., 2021).

Además de las *fake news* hay seis tipos adicionales de desinformación: 1) sátira o parodia; 2) falsa conexión con contenido de fácil apertura; 3) contenidos engañosos que son mentiras combinadas en una serie de datos veraces; 4) falso contexto, que involucra una serie de eventos en un contexto ajeno al real; 5) contenido impostor, que es cuando buscan engañar a la audiencia para robar información u obtener un beneficio, y 6) contenido manipulado, que, como lo dice su nombre, tiene una intención clara de influir o dirigir al expectante en favorecimiento del desinformador (Doble Check, 2020).

Una de las medidas que han tomado los Estados Unidos para contener las operaciones de desinformación y protegerse de las noticias falsas ha sido socializarlas en medios oficiales con su correspondiente corrección o verificando los hechos, como se ve en la página web del Departamento de Estado. En Colombia, una iniciativa importante es la campaña VERA, impulsada por Asomédios, en la cual las emisoras radiales más importantes del país transmiten breves mensajes

en procura de desmentir noticias falsas que se han hecho virales a través de diferentes medios.

Pero, ¿qué tan efectiva puede ser esta medida en relación con la velocidad con la que las operaciones de desinformación cumplen sus objetivos? La realidad es que esto aún se desconoce, pero se aprecia la iniciativa de generar respuestas contundentes para contener los efectos adversos de la desinformación. Adicional a estos esfuerzos de personal capacitado para filtrar la información antes de que sea publicada, se requiere fomentar una cultura ciudadana para evitar la propagación de anuncios con desinformación, así como hacer un trabajo coordinado e interagencial para identificar con mayor eficiencia el contenido engañoso, rechazar su divulgación y contrarrestarlo desmintiendo el engaño.

Otro ejemplo reciente fue la situación de salud pública que generó el virus Covid-19. Para contrarrestar sus efectos, diferentes gobiernos, organizaciones internacionales y el sector privado se involucraron en campañas para promover la vacunación y desmentir la desinformación. En este contexto, la Unión Europea sustentó sus importantes esfuerzos en contra de la desinformación argumentando que el manejo correcto de la crisis de salud pública iba a tener una relación directa con el número de fallecimientos por la enfermedad (Comisión Europea, 2021).

La desinformación es un fenómeno organizado que requiere planeamiento, la disposición de una logística para lograr que el mensaje diseñado se propague y la persecución de un objetivo específico, entre otros elementos. Adicionalmente, la desinformación es un arma que se emplea contra un adversario para afectar su credibilidad, legitimidad, estabilidad y movilizar pensamientos, emociones y acciones en contra del enemigo o a favor de quien fragua la estrategia de desinformación (Rodríguez, 2017).

Además del impacto estratégico que se ha analizado hasta ahora, la desinformación es una industria que opera en más de 48 países. Diferentes actores que desconocen el objetivo final de la desinformación engrosan las cadenas de esta amenaza (Levy, 2021).

Por este motivo, la Comisión Europea presentó un plan de acción contra la desinformación que aporta algunas acciones puntuales para controlarla. Primero, mejorar las capacidades para detectar, analizar y exponer una operación de desinformación, para lo cual se requiere fortalecer la tecnología capaz de controlar, evitar e identificar de dónde proviene la noticia falsa o la desinformación en general, así como reaccionar de manera rápida para evitar la propagación de su contenido.

Segundo, es necesario fortalecer las respuestas del sector privado y del sector público en conjunto. Finalmente, y de la mano con lo anterior, se debe movilizar el

sector privado, aumentando la sensibilidad de la ciudadanía frente a los efectos de la desinformación y aumentar la posibilidad de adaptarse, aprender y desechar la información manipulada (Comisión Europea, 2018).

Una vez analizados los conceptos relacionados con la desinformación, a continuación se determina cuáles son los retos que asumen las Fuerzas Militares frente a las operaciones de desinformación en la seguridad y la defensa nacionales. Para esto se investiga la doctrina militar colombiana y se proponen algunos conceptos que den luces sobre cómo se deben orientar las capacidades de las Fuerzas Militares para mantener la ventaja ofensiva y defensiva en el terreno de las operaciones de desinformación.

Estrategia de las Fuerzas Militares ante la desinformación

La guerra de la información ha promovido un valor inmaterial especial en los ejércitos, cuya fuente radica en el poder y el conocimiento. La primera estrategia se ha encaminado a que los ejércitos desarrollen mecanismos de seguridad y defensa de su patrimonio inmaterial con programas de detección, control y prevención en la invasión y robo de su información más sensible (Sierra, 2003).

Con base en lo anterior, se conducen operaciones de información para fortalecer las capacidades de la Fuerza en la protección de sus activos de información, al tiempo que utiliza la desinformación como estrategia para su beneficio. Las acciones giran en torno a destruir los sistemas informáticos y tecnológicos del enemigo para imposibilitar su uso, interrumpir la circulación de la información, degradar su moral combativa y/o sus sistemas de mando y control; negar el acceso a información sensible; generar decepción en una audiencia frente al opuesto; conseguir información del contrario o plantar mensajes con contenido falso en su contra; influir en los expectantes para conseguir un comportamiento favorable para la Fuerza y detectar de manera temprana la intrusión a los sistemas informáticos oficiales (Andrade et al., 2011).

Las operaciones de información, que pueden ayudar a disuadir al adversario a cero costos en términos bélicos, se consolidan en el ataque, la defensa y el apoyo electrónico (Clark, 2010). De esta manera se entrega valor público a diferentes sectores de la sociedad y se ayuda a proteger diferentes aspectos de la vida pública y privada, como la información financiera, entre otras.

Después de analizar la desinformación como una estrategia en contra de los Estados, ahora es importante analizar la hoja de ruta de las Fuerzas Militares frente a esta creciente amenaza. Por un lado, la Fuerza debe hacer un esfuerzo para protegerse de estas operaciones y, por otro, debe definir estrategias militares para controlar la difusión de desinformación que pueda afectar su legitimidad, la del Estado en general y la del orden institucional. Para cumplir este objetivo, se requiere la intervención de todos los niveles operacionales que componen la fuerza pública.

Cuando se habla del nivel estratégico se hace referencia a ese grupo de personas y recursos materiales e inmateriales de los que dispone para facilitar la toma de decisiones del mando. En la parte estratégica, los altos mandos planean los medios y los recursos que se deben entregar al Ejército de combate, así como los tiempos, las fuentes y los estándares de calidad. Además, son el canal para establecer una relación directa con el Gobierno Central, promueven el cumplimiento de los objetivos nacionales ordenando las instituciones en función de estos y acatan la estrategia del Presidente como Comandante en Jefe de las Fuerzas Militares.

En el nivel operativo se recibe la información, los medios y los recursos pensados y ejecutados por el nivel estratégico, los cuales se utilizan en la realización de planes de operaciones diseñados en este nivel para garantizar la efectividad operacional. Por último, las unidades tácticas materializan el planeamiento operacional entregado por el nivel operativo. Los comandantes del nivel táctico emplean el personal, el medio y los recursos necesarios para conducir las misiones y cumplir las tareas.

Fundamentos operacionales para las Fuerzas Especiales frente a las operaciones de desinformación

Una vez se ha analizado el marco conceptual y teórico de las operaciones de desinformación, es posible establecer algunos lineamientos que pueden evidenciar en qué dirección se deben constituir los fundamentos operacionales frente a la desinformación.

Si se analiza la desinformación desde una perspectiva integral según las funciones, capacidades y alcance de los tres niveles de la fuerza pública, se puede concluir que en el nivel estratégico se requiere de medidas para mitigar el efecto de las operaciones de desinformación, sobre todo cuando estas amenazas interfieren

en la imagen institucional y la estabilidad político-administrativa. De igual manera, se requiere de la planeación de recursos materiales e inmateriales para capacitar y dotar al personal con las últimas tecnologías para detectar fuentes de información, origen de noticias falsas o ataques cibernéticos, proteger las bases de datos oficiales y todo tipo de táctica de esta especie.

Por su parte, en el nivel operativo se recopila la información de Inteligencia por medio de la cual se aproxima y caracteriza el adversario en todas sus áreas, capacidades, técnicas y tácticas (Guzmán, 2019), además de coordinar los esfuerzos para recolectar información en el nivel táctico. En este sentido, se requiere de tácticas que permitan identificar que la información obtenida sea veraz y que no contenga una intención de confundir, engañar la Fuerza o dificultar la toma de decisiones entorpeciendo sus procesos.

El reto en este punto es manejar la incertidumbre, ya que, a diferencia del nivel estratégico, más allá de intentar afectar la imagen institucional o la legitimidad del Gobierno, en este caso la desinformación tiene el poder de incidir en la toma de decisiones y el éxito operacional. En este sentido, obtener información falsa o manipulada afecta la integridad de la tropa y la capacidad de la Fuerza para obtener el éxito operacional esperado (Guzmán, 2019).

A nivel táctico, la inteligencia humana y demás técnicas para recoger información son procesos fundamentales que deben ser fuertemente entrenados en habilidades para detectar las fuentes de información, su calidad y sus posibles consecuencias. De igual manera, se deben emplear operaciones de información como medida disuasiva frente al adversario. En este caso, la desinformación obtiene las condiciones propicias para causar un impacto estratégico durante un tiempo limitado, el cual es equivalente al período en el que se mantengan las debilidades institucionales que dan cabida a una inestabilidad producida por la desinformación (Guzmán, 2019).

Un ejemplo de esto son las operaciones de apoyo a la información militar, que es una capacidad de las FF. EE. y es transversal a los tres niveles de la Fuerza. Por medio de estas se busca analizar y abordar la estrategia psicológica en el terreno operacional, así como apoyar las actividades de información de la institución, en coordinación con otras entidades y las autoridades civiles nacionales, entre otros (Ejército Nacional de Colombia, 2017).

Para proteger la Fuerza en la conducción de las operaciones, las FF. EE., en el cumplimiento de sus funciones y en el marco de sus competencias, pueden y deben soportar la seguridad de la información mediante instrumentos tecnológicos y

capacidades cibernéticas. Esta condición es fundamental, ya que cuentan con la misión para proteger esta acción en defensa de la soberanía y la independencia.

De esta manera lo establece la publicación conjunta *ADP 3-13* de los Estados Unidos sobre las operaciones de información, en la cual se determina que las operaciones militares en el ámbito de la información deben emplear de manera integrada la guerra electrónica, las operaciones de redes de computadoras, las operaciones psicológicas, las técnicas y tácticas de engaño militar y la seguridad de operaciones, de tal manera que sea posible afectar los procesos y las decisiones del adversario, a la vez que proteger su funcionamiento propio (Department of the Army, 2023).

Además, señala que la conducción de cualquier operación militar requiere unos procesos de apoyo que permitan el cumplimiento de la misión y de las tareas asignadas. En este caso, se necesita un soporte que garantice la seguridad de la información y la seguridad física, prevenir o anticipar ataques físicos, el desarrollo de operaciones de contrainteligencia y la cámara de combate (Estado Mayor Conjunto de los Estados Unidos de América, 2006).

Desde otro punto de vista, las operaciones de información requieren del fortalecimiento de las relaciones cívico-militares y la diplomacia militar para, por un lado, recolectar información veraz y afianzar los vínculos con la población civil y, por otro, para respaldar las funciones de Inteligencia y promover la conducción de operaciones con información certera que permita reducir el riesgo inherente a las Fuerzas Militares (Estado Mayor Conjunto de los Estados Unidos de América, 2006).

En el caso de Colombia, todas estas estrategias se deben alinear con la Ley de Inteligencia y los demás parámetros nacionales e internacionales que regulan la actuación de la fuerza pública. Además, las operaciones de información deben convertirse en una columna vertebral de cualquier operación militar, teniendo en cuenta que la desinformación es un recurso sutil pero muy efectivo del adversario para entorpecer la toma de decisiones, el éxito operacional, lograr la ventaja en el teatro de operaciones y fidelizar audiencias.

De esta forma surge una necesidad de soporte, la cual consiste en la capacidad de recolectar, almacenar y gestionar información en tiempo real con exactitud y pertinencia, buscando oportunidades de recolectar la que esté disponible, que sea de fácil comprensión y concisa (Estado Mayor Conjunto de los Estados Unidos de América, 2006). Esta información va a proporcionar al mando los datos necesarios para la toma de decisiones, de manera que dicha información requiere un esquema de seguridad específico para salvaguardar la vida de la tropa, los activos

estratégicos, la infraestructura y demás recursos materiales y no materiales del Estado colombiano para defender la soberanía, la independencia, la integridad del territorio y el orden constitucional.

Específicamente, la cámara de combate es un aspecto fundamental de las Fuerzas Militares, en el entendido de que se enfrenta a una serie de operaciones psicológicas en las que se cuestiona el accionar de las instituciones para mantener el imperio de la ley y el orden nacional. Esta es una herramienta para difundir las acciones de la Fuerza, su apoyo a la población civil, la atención del riesgo de desastres y las emergencias de diversa índole, el desarrollo de operaciones militares para la construcción de una paz estable, la desarticulación de estructuras criminales que violentan las comunidades, entre otras.

Además, por medio de las cámaras de combate se involucra la nación como testigo de la intercesión de la Fuerza, el uso de técnicas y tácticas protegidas por la normativa nacional e internacional, y los principios y valores característicos de la cultura militar. De esta forma se generan mecanismos para proteger la imagen institucional y como defensa jurídica frente a testimonios en contra del accionar de la fuerza pública.

En cuanto a las *fake news* o manipulación de contenido, es fundamental contar con un departamento o unidad que, desde el nivel estratégico en el cuartel general de la fuerza pública e incluso desde el Comando General de las Fuerzas Militares (CGFM), suministre directamente el contenido informativo a los medios de comunicación. De esta forma se va a proteger la legitimidad institucional y a contribuir a la defensa del orden constitucional y los valores sociales.

No obstante, la relación es cíclica e interdependiente, ya que se requiere de buena imagen y reputación para que los medios de comunicación, que en su mayoría son del sector privado y en algunos casos son independientes de cualquier forma de gobierno o poder público, estén en disposición de confiar en el contenido que emiten directamente las Fuerzas Militares.

De igual manera, es necesario determinar el tratamiento de las situaciones de crisis en las cuales se vea involucrada la credibilidad de las Fuerzas Armadas. Una situación puede afectar directamente las instituciones, pero también se puede presentar que se difunda falsa o maliciosamente mensajes que generen miedo e incertidumbre en cuanto a la seguridad y la defensa nacionales. Un ejemplo de esto podría ser un ataque por parte de un grupo ilegal o la invasión de otro país. Este tipo de contenido también se debe presentar en el concepto operacional de las FF. EE. constituidas para contener las operaciones de desinformación.

Conclusiones

La desinformación ataca los diferentes niveles de las Fuerzas Militares, torpedean sus procesos, dificultan la toma de decisiones y afectan la imagen institucional. Entre los diferentes ataques se encuentran la entrega, la publicación o el manejo de información falsa para caracterizar el adversario, lo cual dificulta el planeamiento operacional y la integridad de los miembros de la Fuerza. De igual manera, se vulneran las bases de datos oficiales, la legitimidad de las instituciones y la estabilidad político-administrativa.

Debido a lo anterior, cada nivel de la Fuerza tiene una serie de tareas específicas relacionadas con sus capacidades para responder a la desinformación. Principalmente, se habla de fortalecer las habilidades del arma de Inteligencia, por un lado, en la recolección de información para el desarrollo de operaciones militares y en la identificación de grupos al margen de la ley y su modo de operación. Por otro lado, se deben fortalecer los mecanismos de ciberdefensa y, en apoyo con las comunicaciones estratégicas, generar iniciativas en protección de la imagen institucional.

Frente a esto, las TIC han generado audiencias que reciben y transmiten el mensaje a velocidades vertiginosas. Estas audiencias, algunas veces por desconocimiento de los temas publicados, como reacción instintiva o en respuesta a unos estímulos, generan afinidad política, una dinámica entre bandos, ilegitimidad de las instituciones, entre otros comportamientos que afectan la estabilidad política y administrativa de los gobiernos.

En este sentido, se requieren unidades de FF. EE. capaces de contener ataques cibernéticos para salvaguardar la información que permite la toma de decisiones y el desarrollo de operaciones militares. Así mismo, para proteger la información audiovisual que podría ser sacada de contexto para desarrollar operaciones de desinformación en contra de la fuerza pública. Desde otro punto de vista, se necesitan operaciones especiales para determinar la fuente u origen de las noticias falsas o sacadas de contexto que buscan alterar el orden político y administrativo de la nación.

En todo caso, la fuente primaria de la desinformación la difunde o publica con la intención de afectar al adversario para genera apoyo político que rechace las creencias, posturas y/o el actuar del oponente. Los medios que las utilizan están soportados en la manipulación de las masas, para lo cual se dirigen a su sistema de creencias y en contra de sus valores sociales para generar una reacción idealmente violenta.

Este fenómeno desencadena unos eventos que ponen en crisis el sistema político y administrativo, lo cual permite que la fuente emisora del mensaje de desinformación cumpla sus fines políticos. Los efectos pueden ser tan potentes que incluso podrían desencadenar la caída de una institución, entidad o gobierno. Como resulta evidente, este nivel de fragilidad pone en riesgo a los Estados.

En tal sentido, estos retos implican una nueva área de experticia para el sector defensa y seguridad, el cual debe diseñar estrategias para controlar el impacto estratégico de las operaciones de desinformación y prevenir su aparición. Con este propósito, deben fortalecer su sistema tecnológico, las capacidades de la Fuerza en cuanto a la manipulación de herramientas tecnológicas y de la información, así como establecer tecnologías que le permitan reaccionar de la manera más eficiente posible.

Inicialmente, las FF. EE. deben desplegarse con fundamentos operacionales para proteger la información sensible de las entidades del Estado. De igual manera, deben inclinarse por la veracidad de la información produciendo contenido que contrarreste las operaciones de desinformación, para lo cual deben darle la posibilidad a los medios de comunicación de obtener constantemente datos de primera mano. De igual manera, es necesario que ingenien estrategias para evitar y contener la difusión de información incompleta, falsa y maliciosa.

Como complemento del análisis sobre los ejércitos que han tenido conflictos con otros países –por ejemplo los Estados Unidos, que han generado una doctrina funcional e implementado estas capacidades de apoyo para el desarrollo de las diferentes operaciones militares–, se deben generar unas tareas diferenciales para la FF. EE. colombianas, de manera que maximicen estos ataques físicos sobre la moral del adversario y así puedan sincronizar el planeamiento de operaciones de desinformación.

Referencias

- Andrade, W., Martínez, J. F., & Pineda, J. C. (2011). *Las operaciones de información en las guerras de información* [Trabajo de especialización, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. <https://tinyurl.com/3f7vpwer>
- Antoine, F. (2019). Desinformación y “maskirovka” en la guerra psicopolítica soviética: El caso afgano. *Política Revista de Ciencia Política*, (diciembre), 129-137. <https://tinyurl.com/d8wxjc43>
- Arteaga, M. (2020a). El conflicto híbrido, una contribución para la incertidumbre. En Academia de Guerra del Ejército de Chile (Ed.), *El conflicto híbrido y sus efectos en la conducción operacional y táctica* (pp. 19-43). Centro de Estudios Estratégicos CEEAG. <https://tinyurl.com/2rbbvrfx>
- Clark, B. (2010). Las operaciones de información como elemento disuasivo para el conflicto armado. *Military Review*, (septiembre-octubre), 2-11. <https://tinyurl.com/3nt9b794>
- Comisión Europea. (2018). The 2022 Code of Practice on Disinformation. <https://tinyurl.com/4evc6mhe>
- Comisión Europea. (2021). Lucha contra la desinformación. <https://tinyurl.com/52cw4yd2>
- Contreras, F. (2001). La muerte del soldado: Hacia la deshumanización de las tecnologías de guerra. En F. Contreras & F. Sierra, *Culturas de guerra: Medios de información y violencia simbólica* (pp. 275-308). Cátedra.
- Department of the Army (2023). *ADP 3-13 Information*. <https://tinyurl.com/4bjc5n52>
- Doble Check. (2020). Fake news y otras 6 formas de desinformación [Video]. YouTube. https://www.youtube.com/watch?v=ZllaBk_8J2o
- Ejército Nacional de Colombia. (2017). *Manual Fundamental de Referencia del Ejército MFRE 3-05 Operaciones Especiales [Público]*. Imprenta Ejército. <https://tinyurl.com/32dbw83e>
- Guzmán, A. (2019). La desinformación estratégica como recurso disuasivo durante la crisis. *Revista Ensayos Militares*, 5(2), 99-114. <https://tinyurl.com/44vvvcmt>
- Hernández Sampieri, R., Fernández, C., & Baptista, L. (2010). *Metodología de la investigación* (5.a ed.). McGraw-Hill.
- Levy, G. (2021, 10 de agosto). La creciente industria de la desinformación. <https://tinyurl.com/y3dts9av>
- LISA Institute. (2019, 20 de mayo). Qué es la guerra híbrida y cómo nos afectan las amenazas híbridas. <https://tinyurl.com/258439er>
- López, C. (2007, agosto). La guerra informática. *Boletín del Centro Naval*, (817), 219-224. <https://tinyurl.com/bdcrauey>
- Medina, A (2022, 28 de enero). ¿Qué es la guerra híbrida? La estrategia de Rusia contra Ucrania. *El Debate*. <https://tinyurl.com/mtv564bt>

- Noguera, A. (2013, 20 de noviembre). *Propaganda de guerra, una estrategia adaptada al conflicto colombiano: Análisis de la propaganda de guerra empleada por Uribe y Santos para combatir los grupos guerrilleros* [Tesis de pregrado, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/mzvtnc43>
- Paladino, A, Villalba, M., & Miguel, M. (2021). Entrevista a Martín Alfredo Becerra: Desinformación, fake news y posverdad. *Palabra Clave*, 10(2), e133. <https://doi.org/10.24215/18539912e133>
- Rini, R. (2017). Fake news and partisan epistemology. *Kennedy Institute of Ethics Journal*, 27(S2), 43-64. <https://doi.org/10.1353/ken.2017.0025>
- Rodríguez, A. (2017). Fundamentos del concepto de desinformación como práctica manipuladora en la comunicación política y las relaciones internacionales. *Historia y Comunicación Social*, 23(1), 231-244. <https://tinyurl.com/ykxyu2yz>
- Sierra, F. (2003). La guerra en la era de la información: Propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Publica*, (3), 253-268. <https://tinyurl.com/4bk6c97h>
- U. S. Department of State. (2021, 7 de junio). The extraordinary scope and breadth of Russian propaganda and disinformation [Global Engagement Center Counter-Disinformation Dispatches, n.º 10]. <https://tinyurl.com/3239wjvr>
- U. S. Department of State. (2022a, 13 de enero). Exploiting primal fears [Global Engagement Center Counter-Disinformation Dispatches, n.º 13]. <https://tinyurl.com/2mysnc4w>
- U. S. Department of State. (2022b, 20 de enero). Las cinco principales narrativas de desinformación en las que insiste Rusia. <https://tinyurl.com/navpzd67>
- Ustarroz, M. (2021). *Del fenómeno de la desinformación: Marco conceptual y análisis comparativo del marco legal en la Unión Europea* [Tesis de maestría, Universidad de Barcelona]. Repositorio UB. <https://tinyurl.com/zbd cynur>