ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA: LA GESTIÓN DE LA INFORMACIÓN EN REDES SOCIALES Y SU IMPACTO EN LA FUNCIÓN DE COMBATE PROTECCIÓN.

AUTOR: Mayor Miguel Ángel MAZZUCCHELLI

TUTOR: Coronel Martin Guillermo MENDOZA

AÑO: 2025

"Las ideas expuestas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta de la Universidad de la Defensa Nacional"

Resumen

En la última década, las redes sociales han revolucionado cómo se gestiona la información en conflictos armados, destacando la necesidad de examinar su impacto en la dinámica de la guerra moderna. Plataformas como X (anteriormente Twitter), Facebook, Instagram y Tik Tok han emergido como herramientas esenciales para la difusión de información en tiempo real, utilizadas tanto por actores estatales como no estatales para propaganda, desinformación y movilización de masas para contar con apoyo. Esta capacidad instantánea de compartir información facilita una coordinación más eficaz, aunque plantea desafíos en términos de veracidad y seguridad operativa. La función de combate de protección, cuya finalidad es la de preservar a las propias fuerzas, se ve directamente influenciada por la información diseminada en redes sociales. Esta puede proporcionar inteligencia crítica para la toma de decisiones, pero también exponer vulnerabilidades si no se toman medidas de seguridad para protegerla adecuadamente.

Ejemplos recientes en la guerra Ucrania y Rusia demostró cómo las redes sociales gestionan la información, afectando a actores principales y a países no involucrados directamente. Estas plataformas han sido utilizadas para, influir en la percepción pública y la moral de las tropas y civiles, así como para obtener apoyo internacional.

El estudio de la gestión de información a través de las redes sociales en relación con la función de combate protección es crucial para mejorar el planeamiento operativo y la seguridad en el teatro de operaciones. Esta investigación no solo beneficiará al personal militar en la planificación y ejecución de operaciones, sino también a académicos interesados en mitigar los riesgos asociados con la información en línea. Identificar mejores prácticas en el uso de redes sociales puede contribuir significativamente a la protección de civiles y la minimización de daños colaterales durante conflictos armados.

Palabra claves: Información – Redes – Sociales – Protección.

Tabla de contenido

INTRODUCCIÓN

En las últimas décadas, la evolución de los conflictos armados ha estado marcada por una creciente interconexión digital, donde las redes sociales han desempeñado un papel clave en la diseminación de información en tiempo real. Plataformas como X (anteriormente Twitter), Facebook, Instagram y TikTok se han convertido en entornos estratégicos, utilizados tantos por actores estatales como por entidades no estatales para la movilización de apoyo, la propaganda, la desinformación y la obtención de inteligencia. Este nuevo ecosistema informativo, caracterizado por su alcance global y su capacidad de influencia inmediata, ha desdibujado las líneas entre el campo de combate y el espacio digital, introduciendo nuevos desafíos para la seguridad de las fuerzas militares. En este contexto, la función de combate de protección es:

> La función de combate comprende el conjunto de actividades tendientes a preservar a las propias fuerzas respectos de las acciones del enemigo, permitiendo al comandante aplicar el mayor poder de combate para el cumplimiento de la misión. El conjunto de las actividades relacionadas con la protección, tanto del personal, los medios y la información de la Fuerza tienen por finalidad incrementar la capacidad de supervivencia contra los efectos de los sistemas de armas enemigos y mejorar las condiciones de vida en campaña (Conducción para la Fuerzas Terrestres, 2014, p. IV - 5).

Además esta función de combate, implica no solo las actividades tendientes a proteger a las propias fuerzas de la acción del enemigo, sino también a la protección de la población civil que se encuentra en el Teatro de Operaciones (TO) e Infraestructuras Criticas (IC). La información obtenida y diseminada a través de redes sociales puede influir directamente en estas operaciones. Por ejemplo, la inteligencia obtenida de publicaciones en redes sociales puede proporcionar una herramienta más al momento de tomar una decisión por parte del comandante del TO. Sin embargo, también puede exponer vulnerabilidades, como la ubicación de tropas o los posibles movimientos operacionales, información sobre planes, si no se adoptan las medidas necesarias para protegerla.

La función de combate Protección abarca un conjunto complejo de actividades dirigidas a mitigar y contrarrestar las amenazas que afectan a las tropas, a los medios, y a la información que estas manejan en condiciones de combate. Este

enfoque permite al comandante emplear el poder de combate óptimo para el cumplimiento de la misión y maximizar las probabilidades de éxito operacional (Ministerio de Defensa, 2014). “Los principios de Protección incluyen la defensa antiaérea, la guerra electrónica, guerra cibernética, la fortificación en campaña, medidas de engaño, la protección química, biológica y nuclear (QBN), y fuegos superficie-aire entre otras” (Conducción para la Fuerzas Terrestres, 2014, p. IV - 5). Estas actividades están diseñadas para incrementar la supervivencia de las fuerzas en condiciones hostiles y para asegurar la libertad de maniobras necesarias ante las acciones del enemigo. A medida que el campo de combate se extiende hacia el espacio informático, la protección de las emisiones propias y la afectación de las capacidades del oponente en el espectro electromagnético se han convertido en pilares de la ciberdefensa y ciberataques.

En el escenario actual, el uso de redes sociales supone una nueva dimensión para la función de combate protección. El rápido acceso a la información en estas plataformas expone tanto vulnerabilidades tácticas como oportunidades operacionales. Las redes sociales actúan como canales de comunicación que, si no son adecuadamente gestionados, pueden poner en riesgo la seguridad operativa mediante la exposición de movimientos de tropas, posiciones defensivas potenciales o movimientos logísticos sensibles. La capacidad del enemigo para obtener y explotar la información convirtiéndola en una ventaja operacional exige un marco de defensa integral que considere tanto el control de la gestión de la información que se emite como la neutralización de las operaciones de información del enemigo.

Las redes sociales, en este sentido representan un entorno de confrontación donde se disputa el control y la percepción de la narrativa del conflicto, afectando tanto a las fuerzas combatientes como la opinión pública nacional e internacional. La función de combate Protección requiere, por lo tanto, no solo una defensa de las capacidades físicas y tecnológicas, sino también una estrategia informativa que evite que las operaciones sean vulnerables a la influencia externa. En este contexto, la ciberdefensa y las operaciones de información, se vuelven indispensable para reducir el riesgo de exposición a través de plataformas digitales y salvaguardar el dominio de las comunicaciones propias.

La diferenciación entre los niveles estratégicos, operacional y táctico en esta función permite una asignación de responsabilidades acorde a la complejidad de las amenazas:

> La ciberdefensa, que se establece a niveles superiores de conducción, establece directrices para la protección de la IC de comunicación y los sistemas de información, mientras que la guerra cibernética opera a nivel táctico para asegurar la continuidad de las operaciones a través de la neutralización de amenazas digitales inmediatas en el campo de batalla. Estas operaciones requieren una integración optima con la maniobra y apoyo de fuego, buscando evitar interferencias y optimizar la complementariedad entre los distintos elementos de combate (Conducción para la Fuerzas Terrestres, 2014, p IV - 5).

El análisis de la información y del uso de las redes sociales en relación con la función de combate protección revela que la guerra moderna no solo implica una lucha por el control físico del territorio, sino también una competencia intensa por el control de la información y la narrativa en el dominio digital. Para los comandantes el desafío reside en gestionar esta función de manera que se minimicen las vulnerabilidades informativas, preservando la capacidad de las fuerzas para operar en un entorno seguro y libre de interferencias, y maximizando la resilencia de las operaciones frente a las capacidades tecnológicas y propagandísticas del enemigo.

La relevancia de la gestión de la información a través de las redes sociales y su relación con la función de combate protección radica en el cambio paradigmático que estas plataformas han impuesto sobre el control y la difusión de datos en tiempos de conflictos. En las últimas décadas las redes sociales se han convertido en un espacio que no solo amplifica la visibilidad de los eventos, sino que también influye directamente en las percepciones, la moral de la tropa, la seguridad operacional y la opinión pública internacional. Este nuevo orden comunicacional demanda una compresión profunda de como la función de combate Protección puede y debe adaptarse a la gestión de la información en un entorno digital omnipresente y en contante cambio.

La necesidad de adaptar la doctrina militar a un ámbito donde la exposición de información en redes sociales puede comprender seriamente la función de combate Protección, donde las actividades de protección de las fuerzas han sido tradicionalmente físicas y tecnológicas, las redes sociales suponen una nueva amenaza que, al no estar completamente controlada, permite al enemigo aprovechar grises en la seguridad, identificando vulnerabilidades en los despliegues y exponiendo a las fuerzas. Por ejemplo, la publicación en tiempo real de ubicaciones o

la diseminación no controlada de mensajes en redes sociales pueden alertar a los adversarios sobre movimientos operacionales, comprometiendo la seguridad de las tropas y de a IC.

Asimismo las redes sociales son un espacio donde se disputa la narrativa del conflicto; actores estatales y no estatales despliegan sus propias agendas para movilizar apoyo, influir en la opinión pública y afectar la moral de los combatientes. En un conflicto armado contemporáneo, la capacidad de manejar estas percepciones puede ser determinante para el éxito o el fracaso de una misión. Así la función de combate Protección debe extenderse hacia la defensa de la información y la contención de amenazas digitales en tiempo real, asegurando que las fuerzas propias no solo se protejan de ataque físicos, sino también de la manipulación y desinformación digital que pueda influenciar en la toma de decisiones en el nivel operacional.

La ciberdefensa se presenta como imprescindible que deben operar en conjunto con la función de combate Protección para asegurar las comunicaciones y la información que se posee y gestiona. Esta perspectiva amplía el concepto de seguridad, situándolo en un espacio donde cada emisión, mensaje y señal puede representar tanto un punto de apoyo como un riesgo operativo. En este sentido la capacidad de coordinar y asegurar las comunicaciones propias, mientras se neutralizan las operaciones de información del adversario, deben darle una gran importancia en el nivel operacional.

En el reciente conflicto entre Ucrania y Rusia, Labrador Blanes y Reyes Betanzo (2023) dicen que “las noticias falsas han alcanzado un rol preponderante y utilitaristas, no solo en la política y economía sino también como una herramienta en conflictos” (p.195), a través de las redes sociales han sido utilizadas para obtener apoyo global y exponer las narrativas de guerra desde una perspectiva particular, generando una presión internacional que ha influido en la dinámica del conflicto. Este fenómeno ilustra el poder de las redes sociales y cómo puede impactar en la función de combate Protección, permitiendo tanto el apoyo a la seguridad de las fuerzas propias como la desestabilización de la moral y las tácticas del enemigo. El análisis de la información gestionada en redes sociales se convierte así en un factor estratégico para las operaciones, demandando un planeamiento detallado que prevea los riesgos y aproveche las oportunidades de comunicación de manera segura y efectiva.

La importancia del trabajo radica en la necesidad de actualizar y completar la doctrina para que abarque en el campo de la información, orientando las prácticas y herramientas de los comandantes en el uso controlado y seguro de las redes sociales. Esto no solo permitirá contribuir a la función de combate Protección, sino que contribuirá al desarrollo de procedimientos en el nivel táctico y operacional para proteger a las propias fuerzas, IC y población en un entorno donde la información y su control son tan decisivos como el fuego, choque y maniobra operacional.

El objetivo del Trabajo Final Integrador es comprender cómo las redes sociales, influyen en los conflictos armados contemporáneos, en especial sobre las actividades tendientes a preservar a las propias fuerzas.

Es así que la hipótesis que planteo en el presente trabajo es; la forma en que se gestiona la información a través de las redes sociales facilita a la protección del personal, medios y de la maniobra operacional en el teatro de operaciones, suministrando al comandante más herramientas para su planeamiento.

Esto a su vez me permite plantear los siguientes objetivos particulares, en primer lugar identificar las diferentes redes sociales que fueron más utilizadas durante los conflictos más relevantes de los últimos 10 años, segundo, identificar las oportunidades que se presentan a través de la gestión de la información, tercero y último, analizar las prácticas de la gestión de la información utilizadas por los principales actores involucrados en los conflictos armados a fin de extraer lecciones aprendidas y volcarlas en nuestra organización.

La metodología del presente trabajo emplea un diseño analítico-descriptivo, utilizando análisis documentado de casos de estudio recientes (Ucrania, ISIS) y revisión de doctrina militar vigente, con enfoque en la gestión de información y en la función de combate protección.

Como método de recolección de información utilice doctrina vigente específica de nuestra nación donde contenía temas referidos a la gestión de la información y operaciones de información, también analice trabajos de investigación y artículos periodísticos relacionados a la temática.

CAPÍTULO 1

Redes Sociales y Los Conflictos Armados

Evolución de las Redes Sociales

En la última década, las redes sociales han evolucionado de ser plataformas meramente sociales a convertirse en una parte integral del ecosistema global, con un papel decisivo en los conflictos armados. La facilidad de acceso a internet y la proliferación de teléfonos móviles han democratizado la creación y difusión de contenidos.

El crecimiento del uso de redes sociales como X, YouTube, Instagram; Telegram y TikTok, han permitido la expansión de la guerra de la información, donde tanto actores estatales como no estatales compiten por controlar la narrativa. La instantaneidad de estas plataformas facilita la transmisión de eventos en tiempo real, proporcionando ventajas como desventajas para las fuerzas armadas. Es por esto que "el flujo de información no regulada en redes sociales ha multiplicado las posibilidades de manipulación y desinformación" (Hossein Derakhshan y Claire Wardle, 2017).

Dicho esto, el impacto estratégico de las redes sociales en los conflictos armados es profundo y multifacético. Desde el punto de vista del nivel operacional, estas plataformas han transformado la manera en que las fuerzas armadas y los grupos insurgentes obtienen y difunden la información. Como menciona Otero (2013) "La utilización de esta tecnología, trae aparejada la capacidad de poder grabar videos y tomar fotografías y publicarlas en tiempo real, lo que multiplica su impacto, acelera y potencia la respuesta del resto de la sociedad no solo local sino mundial" (p.16), Este fenómeno tiene implicancias directas para la función de combate Protección, ya que la rapidez en compartir imágenes puede exponer movimientos operacionales, comprometiendo la seguridad, esto hace que un comandante del TO, en base a la información obtenida a través de estas redes pueda tomar decisiones más acertadas, evitando la sorpresa por parte del adversario.

Este aspecto táctico es esencial, pero a nivel estratégico y operacional, las redes sociales permiten controlar la narrativa pública de un conflicto. Los gobiernos y las fuerzas armadas las utilizan para ganar apoyo local e internacional, justificando sus acciones ante la opinión pública. El uso de Twitter por parte de las Fuerzas de Defensa de Israel (IDF) durante la operación "Margen Protector" en 2014 es un

ejemplo claro de cómo las redes sociales son empleadas para informar, justificar y generar apoyo a las acciones militares en tiempo real. Cabe destacar que "Los documentos pueden modificarse (o fabricarse otros adicionales) para generar una mayor controversia y aumentar las percepciones y opiniones negativas a través de las redes sociales" (Ustarroz Molina, 2021, p. 15).

Sin embargo esto puede ser contraproducente ya que las redes sociales pueden ser utilizadas para la desinformación y propaganda, lo que puede tener consecuencias graves en términos del desarrollo de los conflictos bélicos y estabilidad política. Estudios realizados en la Universidad de Oxford en el año 2017 han demostrados como campaña de desinformación en redes sociales han sido utilizadas para influir en elecciones, polarizar poblaciones y desestabilizar gobiernos, efectos que se amplifican en gran medida en tiempos de conflictos bélicos.

Uso de las Redes Sociales en los Conflictos Armados

Las redes sociales han sido utilizadas de diversas maneras en los conflictos armados contemporáneos, adaptándose a las necesidades tácticas y estratégicas de las partes implicadas. Según Howard (2011) uno de los primeros ejemplos destacados fue su uso en la "Primavera Arabe", donde plataformas como Facebook y Twitter fueron herramientas esenciales para la organización de las protestas y la diseminación de información en tiempo real.

La guerra Rusia-Ucrania y en el conflicto de Israel con Hamas, son otro ejemplo que Jorquera Escobar (2023) refiere de cómo:

> El uso de redes sociales como Facebook, X (anteriormente Twitter), Instagram, Flickr o Youtube ha permitido que los contendientes o grupos parciales a uno u otro bando puedan recopilar información sobre las acciones y sus resultados. Estas imágenes o videos son presentadas conforme a los intereses que se tengan, buscando de esta forma influir a través de actividades de propaganda y contra propaganda (s.p).

Actores no estatales como ISIS, han explotado redes sociales como Twitter y Telegram para reclutar combatientes, difundir propaganda y coordinar ataques. El uso de Telegram, en particular, con su función de canales cifrados, ha permitido a estos grupos operar sin una supervisión directa.

Por su parte, los actores estatales también se han beneficiado de estas plataformas para operaciones de inteligencia y contrainteligencia. Un claro ejemplo

es el uso de redes sociales por parte de las fuerzas ucranianas en el conflicto con Rusia, donde las plataformas han permitido una rápida difusión de información sobre las tropas invasoras, ayudando a coordinar la resistencia. Jorquera Escobar (2024) aborda que "la información es un arma al igual que los misiles, las bombas, los torpedos, etc. Ahora queda claro que la confrontación informativa se convierte en un factor que tendrá un impacto significativo en el futuro de la guerra en su origen, curso y resultado" (s.p).

Facebook

"Fundada en 2004 por Mark Zuckerberg, Facebook comenzó como una plataforma de redes estudiantiles, pero rápidamente se expandió a nivel global, convirtiéndose en una de las plataformas sociales más influyentes" (Phillips, 2007 Carr, 2008).

Facebook fue clave durante el conflicto interno de Myanmar que surge en el año 1948 y que continúa hasta el día de hoy, donde la aparición de Facebook agilizo la forma de pelear la guerra, según Tonnesson, Zau Oo y Aung (2021) el grupo armado Arakan (AA):

> Utilizó las redes sociales para el mando y control en sus operaciones contra el Tatmadaw, y seguramente las utilizó para recopilar información, denunciar a los traidores y socavar la moral del adversario. Facebook Messenger y otras aplicaciones de comunicación bidireccional se utilizaron de maneras que antes se utilizaban con la radio de onda corta (p.16).

Además estos grupos armados como dicen Tonnesson, Zau Oo y Aung (2021) "utilizan las redes sociales principalmente para comunicarse con sus propios electores, no tanto para consultas sino para movilización, motivación y ocasionalmente para la recaudación de fondos y el reclutamiento" (p.21), lo cual llevo al gobierno de Myanmar a cerrar Internet en siete municipios de Rakhine entre junio de 2019 y febrero de 2021.

X (ex Twitter)

> "Twitter fue fundada en 2006 por Jack Dorsey, Biz Stone, Evan Williams y Noah Glass. Originalmente concebida como una plataforma para mensajes breves enviados por SMS, evolucionó rápidamente hacia una red social de gran alcance" (Rao, 2008). Desde su lanzamiento oficial, la plataforma evolucionó rápidamente y se convirtió en una de las principales redes sociales

del mundo, desempeñando un papel crucial en eventos sociales, políticos y de comunicación global (s.p.).

"Durante el conflicto de Gaza en 2014, Rodríguez (2015) comenta que "se trató de legitimar el papel de las FDI en el conflicto, argumentando la protección de los ciudadanos de Israel y Gaza frente a los ataques de Hamás" (p. 15). Además según Ramos, Murcia y Ufarte (2023) "Twitter ha favorecido la aparición de herramientas para la verificación periodística y cuyo papel también se ha estudiado durante la guerra de Ucrania" (p. 2), documentando en tiempo real las violaciones de derechos humanos. Grupos terroristas como ISIS también usaron Twitter para difundir propaganda y reclutar simpatizantes, lo que obligó a la plataforma a implementar políticas más rigurosas. También ha sido ampliamente utilizada por gobiernos y militares para comunicar estrategias y contrarrestar la propaganda enemiga.

YouTube

"Lanzada en 2005, YouTube se consolidó como la principal plataforma para compartir videos en línea, siendo adquirida por Google en 2006" (Burgess & Green, 2018).

En el trabajo de Howard y Hussain (2013) durante la guerra civil siria, "activistas compartieron videos en YouTube para documentar las atrocidades cometidas, creando un archivo visual de las violaciones de derechos humanos". Grupos como ISIS también utilizaron YouTube para publicar videos de propaganda dirigidos a reclutar nuevos combatientes. Aunque YouTube ha mejorado sus políticas de moderación de contenido, sigue siendo una plataforma de gran significancia para las narrativas de conflictos armados.

Instagram

"Lanzada en 2010, Instagram fue adquirida por Facebook en 2012, integrándose rápidamente como una plataforma visual clave dentro de la estrategia de la empresa" (Newton, 2016).

Instagram ha sido utilizada por activistas y periodistas para documentar visualmente los efectos devastadores que la guerra produce. Jorquera Escobar (2024) afronta que "en 2013, el soldado Mor Ostrovski fue arrestado tras compartir en su cuenta de Instagram una fotografía en la que se podía ver a un joven palestino en el punto de mira de su fusil", esto genero un fuerte impacto emocional en las audiencias globales. Otro ejemplo es el que cita Jorquera Escobar (2024) cuando previo a la

invacion de Rusia a Ucrania “las fotografías compartidas por un soldado ruso en su cuenta de Instagram lo geolocalizaban dentro de las fronteras ucranianas”, comprometiendo la versión oficial de Moscú sobre una posible invasión a Ucrania. Pero por lo contrario además, las fuerzas armadas han usado Instagram para humanizar sus operaciones y ganar apoyo público.

Telegram

“La red social fue lanzada en 2013 Pavel Durov y Nikolai Durov, ganando muchos adeptos gracias a su enfoque en la privacidad y el cifrado” (Janjevic, 2024).

Telegram “ha sido adoptada por grupos insurgentes y terroristas, como ISIS, debido a su capacidad para coordinar operaciones de forma segura y compartir contenido sin el mismo nivel de vigilancia que en otras plataformas” (Brooking y Singer, 2018). Durante el conflicto sirio, Telegram fue utilizado tanto por combatientes como por activistas para difundir noticias y coordinar operaciones.

TikTok

Según Conde del Rio (2021) “TikTok es una Red Social de vídeos cortos y transmisiones en directo con una duración máxima de 15 segundos y fue lanzada en 2016 por ByteDance” (p.4) y se ha convertido en una de las plataformas más populares para la creación de videos cortos, especialmente entre audiencias jóvenes.

Durante la invasión rusa de Ucrania en 2022, TikTok fue utilizada para compartir imágenes y videos que documentaban los efectos de la guerra. Estos videos ofrecieron una visión íntima del conflicto y abrieron debates sobre el impacto psicológico de la guerra en las audiencias jóvenes, según Suarez, Garcia y Garcia (2023) esta red social “cambio el estilo de narración, que en la mayoría de los casos es más formal. Solo se destaca el baile del único profesional que publica vídeos (un militar ucraniano)” (p. 14), dando a conocer que sigue con vida en la situación en la que está sumergido.

Redes Sociales más Utilizadas en los Conflictos Armados en los Últimos 10 años

El uso de las redes sociales en los conflictos armados ha sido diverso y ha evolucionado conforme las plataformas han desarrollado sus capacidades y popularidad. En los últimos 10 años, cinco plataformas han destacado por su relevancia en la difusión de la información, propaganda, coordinación de

operaciones, y documentación de eventos: Facebook, Twitter, YouTube, Telegram e Instagram.

Facebook

Esta plataforma ha sido una de las plataformas más influyentes, utilizada tanto por actores gubernamentales como también por insurgentes para coordinar y organizar movimientos sociales, protestas y propaganda en diferentes conflictos.

Características de esta red social:

- Difusión masiva de información.
- Capacidad de organización comunitaria a través de grupos.
- Amplia audiencia global.

Twitter

Twitter ha jugado un rol fundamental debido a su capacidad para viralizar información de forma rápida y concisa a través de los "hashtags", lo que ha sido especialmente útil en los conflictos como Gaza en 2014 y el conflicto sirio (Brooking y Singer, 2018). También ha sido ampliamente utilizada por gobiernos y fuerzas armadas para comunicar estrategias y contrarrestar la propaganda enemiga.

Características de esta red social:

- Información en tiempo real.
- Uso extensivo de "hashtags" para campañas de información.
- Accesibilidad para periodistas y activistas.

YouTube

Wille (2020) señala que "YouTube ha sido una plataforma clave para documentar violaciones en conflictos como el de Siria, aunque las políticas de moderación de contenido han generado desafíos en la preservación de estas pruebas". La red social YouTube se ha convertido en una plataforma clave para la difusión de videos que documentan violaciones de derechos humanos y operaciones militares. Desde que la red comenzó a crecer en el mundo, en los diferentes conflictos armados, esta red social fue utilizada por activistas y grupos insurgentes para publicar videos de ataques y atrocidades, siendo utilizada por grupos extremistas, por ejemplo, como ISIS, para difundir propaganda.

Característica de la red social:

- Impacto visual y emocional.

- Amplificación de narrativas a través de videos.
- Difusión de propaganda y reclutamiento.

Telegram

Telegram ha ganado popularidad debido a su cifrado y capacidad para mantener la privacidad de los usuarios, lo que ha convertido en una de las favoritas entre grupos insurgentes y terroristas, que según Ali (2023)

> Hamas ha utilizado Telegram para coordinar sus movimientos y divulgar mensajes de propaganda, presentando su versión de los ataques y llamando a la resistencia. Además Telegram se convirtió en un canal directo para informar a la población y sus combatientes, publicando comunicados en tiempo real y videos de operaciones. Esta plataforma ayudó a Hamas a difundir rápidamente su narrativa entre sus seguidores y a organizar su respuesta ante los ataques israelíes (p. 47).

También fue ampliamente utilizada por ISIS para coordinar operaciones y distribuir material propagandístico durante los conflictos en Siria e Irak.

Característica de esta red social:

- Comunicación cifrada.
- Canales privados y públicos de difusión.
- Popular entre insurgentes y grupos terroristas.

Instagram

Instagram inicialmente fue utilizada como la plataforma de imágenes personales, según Bruns (2017) “esta red ha sido utilizada en conflictos para mostrar imágenes visualmente impactantes que documentan la guerra, especialmente en Gaza y Siria”. Las fuerzas armadas también la utilizaron para humanizar su imagen en medio del conflicto.

Características de esta la red:

- Imágenes y videos de impacto emocional
- Uso para crear una narrativa visual de la guerra.
- Audiencia joven y conectada.

Impacto de las Redes Sociales en el Nivel Operacional

En la última década, las redes sociales transformaron en gran medida las dinámicas de los conflictos armados, no solo en términos de comunicación, sino también en la forma de pelear la guerra por parte de los actores implicados. A través

de las plataformas como Facebook, X (ex Twitter), YouTube, Instagram, Telegram, se han reconfigurado los métodos tradicionales de propaganda, reclutamiento, influencia psicológica. Esto demuestra que las redes sociales no son simples herramientas de comunicación, sino también armas que moldean el campo de combate moderno.

Uno de los impactos estratégicos más notables de las redes sociales en los conflictos armados ha sido su capacidad para facilitar la guerra de la información. Las plataformas sociales permites a los actores estatales y no estatales difundan propaganda de manera instantánea y global. Como lo señalan Brooking y Singer (2018) "las redes sociales han convertido la información en una herramienta de guerra, permitiendo que tanto gobiernos como grupos insurgentes manipulen narrativas para influir en la percepción pública y ganar apoyo internacional" (p.18). Un ejemplo claro lo demuestra Smith (2022) cuando dice:

Los operativos rusos emplearon Facebook y X para difundir información falsa con el objetivo de desmoralizar tanto a las tropas ucranianas como a la población civil. En particular, se han detectado cuentas falsas y bots que compartían noticias sobre supuestas derrotas militares y bajas significativas en las filas ucranianas. (Smith, R. (2022). Misinformation warfare on social media: Analysis of Russia's strategies. Journal of Military Ethics, p. 203).

Estas tácticas de desinformación buscaban erosionar la moral y la confianza en el liderazgo ucraniano.

Por otro lado, grupos terroristas como Hamas,

> Ha lanzado campañas a través de X que exageran sus logros militares, difundiendo información sobre ataques supuestamente exitosos para ganar apoyo y afectar la moral israelí, por su parte, ha respondido rápidamente con contramedidas digitales para neutralizar estas afirmaciones, demostrando como se puede contrarrestar la desinformación en tiempo real. (Sharipo, 2022, p 123).

Otro ejemplo de esto se vio cuando en 2022, durante la invasión de Ucrania por parte de Rusia, Petrov (2022) narra que "un soldado ruso público en VKontakte (red social rusa) una foto con la geo localización activada que revelaba la ubicación exacta de una base militar temporal en territorio ucraniano" (p. 103), este descuido informático alerto a las fuerzas ucranianas, quienes rápidamente analizaron la publicación y respondieron redirigiendo ataque de artillería hacia el área identificada.

Para minimizar el riesgo, el mando ruso decidió retirar sus fuerzas temporalmente de la ubicación señalada y reprogramar el movimiento de tropas, lo que genero un retraso considerable en las operaciones previstas.

La capacidad de alcanzar audiencias específicas y segmentadas a través de las redes sociales ha permitido a estos grupos movilizar a individuos sin necesidad de una infraestructura física o logística compleja.

Otro impacto que podemos identificar de las redes sociales también se manifiesta en su uso para la guerra psicológica. En los conflictos modernos, las plataformas sociales han sido utilizadas para difundir imágenes y videos diseñados para desmoralizar al enemigo y crear un sentimiento de vulnerabilidad entre las fuerzas contrarias. Un claro ejemplo de esto fue el uso de videos de ejecuciones por parte de ISIS, difundidos a través de YouTube y otras plataformas, los cuales no solo buscaban atemorizar a las audiencias locales, sino también generar terror psicológico entre los adversarios militares (Derakhsham y Wardle, 2017).

Esta dinámica no se limita a los actores no estatales. Durante la invasión de Ucrania por parte de Rusia en 2022, las redes sociales, particularmente TikTok, se convirtieron en una herramienta clave para mostrar el sufrimiento de la población civil y difundir mensajes de resistencia, lo que a su vez creó presión internacional y contribuyó a la narrativa ucraniana de victimización frente a la agresión rusa (Wintour, 2022).

CAPÍTULO 2

Gestión de la Información en Conflictos Armados

Teoría de la Gestión de la Información en Contextos Militares

El manejo de la información, como también su protección ha sido durante mucho tiempo fundamental para las operaciones militares y su evolución está estrechamente relacionada con el desarrollo tecnológico. En la guerra antigua, los sistemas de comunicación eran simples, basados en señales o mensajes simples que contenían información importante a largas distancias. A medida que avanza la tecnología, los ejércitos adoptan sistemas más sofisticados que pueden proporcionar datos rápidamente, una necesidad en el campo de combate moderno. Hoy en día, no sólo es una ayuda importante para los comandantes de los TO, sino también una herramienta estratégica.

Ayduh (2019) sostiene que el "planeamiento de las estrategias comunicacionales permitan al comándate una cierta libertad de acción para poder difundir aquella información que sea necesaria para lograr introducir aquellos factores que tornen la situación desfavorable en propicia" (p.32), esto supone que la gestión de la información en los conflictos modernos es importante para la supervivencia en situaciones adversas. De hecho, la ineficiencia en la seguridad y protección de la información puede generar grandes problemas de seguridad creando vulnerabilidades y permitiendo que el oponente se beneficie de esto explotando fallas en las comunicaciones.

Singer y Brooking (2018) "abordan cómo la información se ha convertido en un arma poderosa que redefine las dinámicas de los conflictos modernos", es decir que refieren al uso de la información como arma. Este concepto resalta la necesidad de controlar no sólo la transmisión de comunicaciones, sino también la capacidad de interrumpir las comunicaciones enemigas. En un conflicto armado, una comunicación eficaz puede significar la diferencia entre la victoria y la derrota, porque la capacidad de comunicarse de forma eficaz, rápida y segura influye en las decisiones que un comandante puede llevar a cabo de forma más crítica, acertada y en tiempo real.

La guerra de información no se trata solo de recopilar datos, sino también de garantizar que los datos se analicen y compartan con el órgano del Estado Mayor o el

personal adecuado en el momento adecuado. Este proceso, conocido como "ciclo de la información" (Inteligencia Táctica, 2008, p.11), es importante para mantener la coherencia y precisión en la toma de decisiones. Además, “el hecho de que la información pase entre diferentes niveles en la organización militar añade complejidad a su gestión, donde la confiabilidad de las fuentes y la verificación de los datos es muy importante” (Alberts y Hayes, 2006).

Por otro lado, la nueva doctrina militar reconoce la creciente importancia de la seguridad cibernética y la gestión de la información. Las comunicaciones, especialmente aquellas que dependen de redes digitales, son cada vez más vulnerables a ciber ataques que pueden afectar la integridad de los datos y neutralizar los sistemas Comando, Control, Comunicación, Inteligencia e Informatica (C^3I^2). “La capacidad de defender estas redes y asegurar que la información crítica permanezca protegida es ahora una parte esencial de la gestión de la información en contextos de conflicto” (Woolley y Howard, 2017, p.---).

Como se gestiona la información, no solo en operaciones militares, sino en el normal funcionamiento de las Fuerzas Armadas, agrupa tareas y conceptos que incluyen la obtención, análisis y la difusión de datos. Al mismo tiempo, muestra la necesidad de proteger la información de actores que quieran utilizarla para generar efectos en perjuicio nuestro, en un mundo donde la tecnología y la información están entrelazadas, la capacidad de gestionar eficazmente estos recursos se ha convertido en un factor fundamental para el logro del éxito en las operaciones militares.

Oportunidades en la Gestión de la Información a Través de las Redes Sociales

Con la llegada de las redes sociales, los conflictos armados han experimentado cambios en la forma en que se gestiona y utiliza la información. Las redes sociales como X, Facebook y YouTube han permitido a diferentes actores, hay sea estatales y no estatales, incluyendo al personal militar proporcionar una plataforma global para diseminar mensajes, contrarrestar la propaganda enemiga e involucrar a personas de todo el mundo, ganando la opinión pública internacional.

Uno de los aspectos más relevantes de las redes sociales es su capacidad para difundir información rápidamente a una audiencia global. Esto significa una oportunidad sin precedentes para que los hacedores de guerra influyan en las narrativas públicas y las interpretaciones de los acontecimientos. Por ejemplo, “durante el conflicto de Gaza en 2014, las FDI utilizaron Twitter de manera efectiva

para explicar su justificación de los ataques aéreos y para contrarrestar las declaraciones de Hamás en las redes sociales y los medios sociales" (Brooking y Singer, 2018).

Estas plataformas también permiten a los actores estatales desarrollar narrativas de eventos. Al utilizar cuentas legales y videos en tiempo real, los gobiernos pueden presentar su versión antes de que respondan las organizaciones de noticias tradicionales. Esto no sólo mejora el poder de la opinión pública, sino que también permite responder a cualquier crítica o malentendido proveniente de actores en conflicto o grupos de insurgentes.

Una oportunidad importante que las redes sociales presentan para hacer inteligencia es a través de la explotación de fuentes abiertas (Open Source Intelligence, OSINT). "Los analistas militares pueden monitorear las redes sociales, rastrear eventos y analizar señales de alerta temprana de amenazas" Jorquera Escobar (2024), este seguimiento y análisis del terrorismo para mejorar la prevención durante la guerra.

Un ejemplo que remarca Jorquera Escobar (2024):

> En agosto del 2019 un misil ucraniano impacto un edificio en la ciudad de Popasna destruyendo el cuartel general del grupo Wagner en dicha ciudad y provocando un número indeterminado de bajas. La ubicación del cuartel general fue identificada a partir de las fotografías que los soldados de Wagner subieron a sus redes sociales.

Sin embargo, es importante señalar que las oportunidades que presentan las redes sociales en cómo se gestiona la información son limitadas. La rápida divulgación de información a veces dificulta determinar la veracidad en la misma, lo que a menudo conduce a la entrega de información incorrecta o incompleta. A pesar de esto, las ventajas que ofrecen estas plataformas en términos de alcance y rapidez superan, en muchos casos, los riesgos asociados a su uso.

Desafíos y Riesgos en la Gestión de la Información

Si bien las redes sociales son una gran oportunidad para gestionar la información y la guerra, también presentan grandes desafíos que no pueden ser ignorados. Uno de los problemas más graves es la capacidad de los actores no estatales y grupos insurgentes para hacer uso de las redes sociales para difundir desinformación y propaganda. Este tipo de medios, conocidos como

"ciberpropaganda", se utilizan para confundir a los oponentes y manipular la opinión pública para promover su agenda.

El uso de bots y cuentas falsas ha permitido a estos actores aumentar sus perfiles y hacerlos parecer más grandes de lo que realmente son. Esta situación se documentó durante el conflicto de Ucrania en 2014, "cuando funcionarios rusos utilizaron las redes sociales para difundir información y engañar a la gente sobre la legitimidad de la intervención militar rusa (Woolley y Howard, 2017).

Además, la sobrecarga de información es un desafío importante en la gestión de información durante los conflictos. Los líderes militares y quienes toman decisiones se sienten abrumados por la diversa información disponible de diferentes maneras, lo que puede generar confusión y gracias a esto hacerlos tomar decisiones erróneas. El problema se ve agravado por la falta de tiempo para obtener, filtrar y analizar la información, lo que aumenta la posibilidad de que se utilicen datos incorrectos en las operaciones militares.

Para reducir estos problemas, es necesario que las fuerzas armadas implementen un sistema de información y análisis para que puedan encontrar rápidamente equipos confiables y eliminar los no confiables. "Los que toman decisiones también necesitan una formación adecuada para poder interpretar la información que reciben y tomar decisiones basadas en la información proporcionada" (Alberts y Hayes, 2006).

Finalmente, otro gran desafío es proteger los recursos digitales. Los sistemas de redes sociales son vulnerables a los ataques cibernéticos, que pueden comprometer la integridad de la información y permitir que actores malintencionados modifiquen o eliminen datos confidenciales. "Las fuerzas armadas debe invertir en ciberdefensa y desarrollar procedimientos sólidas para proteger sus sistemas de información y garantizar que la información confidencial no se vea comprometida" (Sing y Brooking, 2018).

CAPÍTULO 3

Práctica de la Gestión de la Información en Conflictos Armados

Análisis de Caso de Estudio

La rápida diseminación de información en redes sociales ha transformado en el entorno operativo en los conflictos armados contemporáneos. Los siguientes casos adicionales ofrecen un análisis detallado sobre la relevancia y el impacto de la gestión de la información en conflictos recientes. A continuación se mencionan ejemplos del uso de redes sociales

Uso de WhatsApp por las Fuerzas de Resistencia en Myanmar

En concreto, las fuerzas de resistencia y los ciudadanos pudieron organizarse y coordinar la resistencia mediante WhatsApp y Facebook para organizar protestas, establecer comunicaciones para las informar los movimientos de tropas en tiempo real y sobre los posibles enfrentamientos. . La capacidad de transmitir información rápidamente permitió a los civiles evitar áreas de riesgo y a las fuerzas de resistencia coordinar sus respuestas contra las fuerzas militares (Ko, 2023, p. 122).

Específicamente, WhatsApp llevó a cabo la aplicación de las notificaciones tempranas, proporcionando una alerta de seguridad activa en la medida en que ofrece seguridad y movilidad. Además, el uso de WhatsApp en Myanmar demostró cuánta información y cuán militarizada estaba la red, la moral y la capacidad organizativa de la insurgencia en la situación del caso en contra de un adversario convencional. Sin embargo, las autoridades militares intentaron interrumpir estas redes informativas, lo que subraya la importancia de proteger los canales de comunicación para asegurar la función de combate Protección en un entorno asimétrico (Ko, 2023, p. 125).

TikTok y la Propaganda del Estado Islámico en Siria e Irak

Durante el conflicto contra el Estado Islámico (ISIS) en Siria e Irak, TikTok fue utilizado por militares y simpatizantes de ISIS para difundir propaganda y reclutar nuevos combatientes. Los videos compartidos incluían imágenes editadas para mostrar escenas de combate y presentar una imagen heroica de los militantes. Esto no solo buscaba influir en la percepción pública y atraer reclutas, sino tambein

impactar negativamente la moral de las fuerzas opuestas al presentar una narrativa de invulnerabilidad (Baker, 2022, p. 67).

Podemos observar cómo la gestión de la información a través de las redes sociales puede ser utilizada de manera ofensiva para llevar a cabo una guerra psicológica, "las fuerzas de la coalición contra ISIS implementaron medidas de seguridad para evitar la proliferación de estos videos y minimizar su impacto, mostrando la relevancia de un enfoque proactivo en la gestión de la información para preservar la seguridad y la moral de las fuerzas" (Baker, 2022, p. 70).

Uso de Twitter y OSINT en la Guerra de Nagorno-Karabaj

En el caso de Nagorno-Karabaj, en 2020, entre la Armenia y el Azerbaiyán, ambos lados utilizaron Twitter y otras redes para recopilar información y realizar inteligencia de código abierto (OSINT) de la movilidad de la fuerza desplegada enemiga. Registros de imágenes y videos de soldados y civiles que publicaban de ambos bandos les permitieron deducir posiciones y movimiento de la fuerza enemiga estratégicamente. "Azerbaiyán, en particular, mostró una capacidad avanzada para recopilar y analizar información obtenida en redes sociales, utilizando drones para dirigir ataques basados en estas ubicaciones" (Khan, 2022, p. 142).

Este caso muestra como la forma correcta de gestionar la información obtenida a través de las redes sociales puede proporcionar una ventaja significativa en el nivel operacional, según Khan (2022) "la capacidad de Armenia y Azerbaiyán de emplear OSINT refleja la necesidad de incluir la seguridad de la información digital en la planificación de operaciones, evitando que las publicaciones inadvertidas comprometan la función de combate Protección" (p. 145).

La comparación de estos ejemplos muestra que, si bien las redes sociales son comúnmente utilizadas durante conflictos armados para gestionar información, la forma en que se usan y los resultados difieren significativamente con respecto a los contextos. En conflictos internos y de resistencia, como en el caso de Myanmar, las redes se dedican a la organización y la protección local, mientras que, en relación con conflictos de insurgencia como ISIS, las redes solo cumple las tareas de propaganda y reclutamiento. Finalmente, con relación a conflictos internacionales, como el de Nagorno-Karabaj, las redes sociales se convierten en una herramienta de inteligencia crítica, y, a su vez, la gestión de la información a través de las redes sociales se adapta a los objetivos operacionales de las fuerzas en conflicto.

Estos ejemplos muestran la importancia de implementar cómo se gestiona la información a través de redes sociales y finalmente, la elección de una herramienta que facilite a contribuir con la función de combate Protección.

Lecciones Aprendidas

A partir de los casos estudiados podemos extraer lecciones que resaltan la importancia de una gestión cuidadosa y el papel de las redes sociales en compartir la información contenida ahí.

El monitoreo de las redes sociales es necesaria para evitar la exposición de posiciones estratégicas. La lección más importante para el conflicto de Nagorno-Karabaj es que las redes sociales pueden convertirse en un excelente recurso para el enemigo con la publicación y la difusión de la información sin control adecuado. En particular en este caso, tanto Armenia y Azerbaiyán pudieron obtener información, incluso de posiciones y movimientos de tropas, gracias a las publicaciones con geolocalización activada. “Esto destaca la necesidad de monitorear y controlar las publicaciones de soldados y civiles en zonas de conflicto para evitar la exposición de información sensible” (Khan, 2022, p. 142).

La capacitación en seguridad de la información para todo el personal en la zona de conflicto se es de carácter fundamental ya que soldados y civiles que comparten imágenes y videos con ubicaciones geográficas específicas y pueden, sin saberlo, comprometer la seguridad de las operaciones. Esto se hace posible porque el adversario puede obtener información a través de OSINT. “Esto subraya la importancia de capacitar a todos los involucrados en la operación, incluyendo personal militar y civiles, en prácticas de seguridad de la información, enfatizando las consecuencias potenciales de publicar contenido en redes sociales desde el área de operaciones” (Khan, 2022, p. 144).

Uso de OSINT como herramienta para la superioridad informática

Otra lección que nos deja estos estudios es que la inteligencia de código abierto puede proporcionar una ventaja significativa en el campo de combate cuando se gestiona la información de manera efectiva. En Nagorno-Karabaj, la capacidad de utilizar OSINT permitió a las fuerzas armadas de Azerbaiyan coordinar ataques basados en datos obtenidos de redes sociales, lo que mostro su precisión operativa. Esta lección resalta la necesidad de integrar la recopilación de OSINT en medidas de seguridad contra inteligencia para lograr alcanzar una superioridad en operaciones de

información en el conflicto.

Desarrollo de Protocolos de Inteligencia para Neutralizar OSINT del Enemigo

Las medidas de seguridad de contrainteligencia (MSCI) ha desarrollado en los conflictos modernos específicamente al digital y, en particular, a la recopilación de la propia inteligencia tanto por el enemigo como de fuentes abiertas. Este caso en especial, el conflicto de Nagorno-Karabay reafirmó el poder y capacidad de las fuerzas armadas de Azerbaiyán de recomponer publicaciones de redes sociales y datos geolocalizados de los soldados y civiles para directamente dirigir ataques contra objetivos armenios.

Esto, de hecho, "exige a que las fuerzas armadas deben implementar MSCI para mitigar los riesgos de OSINT y prevenir que el enemigo explote información inadvertidamente expuesta en plataformas públicas" (Khan, 2022, p. 146).

Desarrollar protocolos efectivos de contrainteligencia para neutralizar la OSINT enemiga requiere un enfoque integral que abarque la protección de las propias emisiones de información y la disrupción de los esfuerzos de recopilación adversarios. En primer lugar, es básico monitorear a largo plazo redes sociales y otras plataformas de comunicación pública, para detectar publicaciones que puedan comprometer la seguridad operativa. Estableciendo sistemas de alerta temprana son necesarios para detectar publicaciones que revele la posición, el movimiento y las intenciones operativas de las fuerzas. Cuando identificado, permite actuar y eliminar el contenido de inmediato para reducir el riesgo de exposición (Khan 2022, p. 146).

Para mitigar el riesgo, además de deshabilitar las funciones de geolocalización en los dispositivos móviles y forzar que no se creen futuras redes en el aire, se deben establecer políticas que prohíban que el personal tenga una ilimitada libertad para acceder a las redes sociales.

Sin lugar a dudas, si la geolocalización no se administra convenidamente, cada publicación o fotografía puede realizarse en un punto exacto del campo de batalla, proporcionando al adversario información precisa sobre las posiciones sensibles. Otra práctica preventiva requerida dentro de los protocolos son la seguridad digital y las políticas de dispositivos en el campo de combate.

Otra herramienta que puede ser utilizada para neutralizar OSINT es difundir información falsa o confusa, lo que implica saturar las redes con información errónea para llevar al error a los mandos militares enemigos llevando a cabo mayores

esfuerzos de inteligencia. Esto promueve la publicación controlada de información que, a pesar de su apariencia de ser auténtica, pretende llevar la atención del enemigo por un tiempo mayor y reducir la precisión en la obtención de información.

La implementación de esto en el nivel operacional requiere un planeamiento meticuloso para evitar daños propios, su potencial para manipular la percepción del adversario y proteger las verdaderas intenciones y movimientos.

Para esto es necesario contar con elementos en ciberdefensa para enfrentar y mitigar los riesgos asociados con las amenazas en el ciberespacio. Estos elementos no solo se encargan de proteger IC, sino que también desempeñan un papel en la recopilación y análisis de inteligencia, la protección de datos sensibles y la neutralización de amenazas en tiempo real). Estas capacidades "deben incluir el monitoreo de redes sociales y otros espacios digitales para detectar posibles amenazas de seguridad, ataques de desinformación y otros tipos de vulnerabilidades que puedan ser explotados por adversarios" (Clarke y Knake, 2019, p. 152).

Esto es fundamental en su relación con la función de combate Protección, donde las redes sociales representan una ventaja como un riesgo al momento de obtener información, ya que esto:

Destacan además que la integración de estas unidades especializados en la estructuras de defensa nacional permite responder con rapidez a ciberataques y gestionar la información de manera más segura. Para ello, es esencial desarrollar una infraestructura que respalde la comunicación y coordinación interagencial, de modo que si se recibe algún ataque puedan ser identificados rápidamente y contrarrestados de forma inmediata antes de que afecte las operaciones o comprometan la seguridad de las fuerzas armadas. (Clarke & Knake, 2019, p. 175).

Empleo de Lecciones Aprendidas en Nuestra Organización

Las lecciones que podemos tomar de los casos estudiados implican la adopción de procedimientos para mejorar cómo se gestiona la información y de esta manera favorecer en la función de combate protección. Para aplicar estas lecciones y volcarlas en nuestra doctrina y de esta forma colaborar en mejorar las medidas de seguridad en nuestra organización, se sugiere establecer control de los datos o información en las redes sociales y que regulen el uso de dispositivos móviles y publicaciones en deferentes plataformas por parte de personal militar y civil en áreas de conflicto. Esto debería incluir instrucciones claras sobre el uso de geolocalización

y restricciones específicas sobre la publicación de imágenes y videos en redes.

Además de lo anterior, podemos implementar un sistema de capacitación continua en explotación de fuentes abiertas, que ya existe, asegurando que los analistas comprendan cómo utilizar estas plataformas de manera segura y efectiva en el ámbito de la inteligencia militar, deduciendo de manera precisa de forma exacta posibles movimientos de tropa enemigos o posibles operaciones a desarrollar para estar preparado de la mejor manera evitando ser sorprendido.

Para contribuir con la función de combate Protección, en lo que respecta a la preservación de fuerzas propias, es fundamental implementar medidas de contrainteligencia digital que permita identificar y neutralizar campañas de desinformación en tiempo real. En conflictos recientes, se ha demostrado que el uso de redes sociales para debilitar la moral de las tropas es una procedimiento común que se planifica en el nivel operacional, “establecer un equipo dedicado a la supervisión de contenido en redes sociales y a la contramedida de desinformación ayudaría a asegurar que las fuerzas militares mantengan el control narrativo y minimicen el impacto de los ataques psicológicos externos” (Brown, 2023, p. 34).

CONCLUSIONES

Las redes sociales han evolucionado para convertirse en una herramienta de gran importancia con la que cuenta el comandante del TO durante el desarrollo de los conflictos armados. Estas plataformas no solo permiten a los actores del conflicto difundir información y controlar narrativas, sino que también actúan como una forma de comunicación estratégica que impacta en la función de combate Protección. En este sentido, permite influir en la percepción pública y en la moral de las fuerzas propias y del adversario, a través de la información que circula en las redes sociales, siendo un factor que permite ampliar el poder de combate de las fuerzas contribuyendo a su protección.

La relación entre la guerra electrónica y cómo se gestiona la información a través de las redes sociales, en un espacio de combate digital donde las operaciones de información tienen un papel fundamental junto a las operaciones psicológicas. Esto hace hincapié en cómo los actores en conflicto emplean las redes sociales para recolectar información y realizar Inteligencia, aprovechando las vulnerabilidades del entorno cibernético y de esta manera pueden lanzar ciberataques. Es por esto que las redes sociales transforman el TO, convirtiéndose en un pilar fundamental en el nivel operacional para la conducción, colaborando en la protección de las fuerzas mediante la protección de la información.

Una correcta y eficaz gestión de la información en las redes sociales puede obtener una ventaja significativa para la protección de las fuerzas. La posibilidad de recopilar información en tiempo real mediante la explotación de fuentes abiertas permite a los comandantes inferir movimientos de fuerzas enemigas y posibles operaciones que puedan llevar adelante, facilitando la anticipación y evitando la sorpresa. Esta capacidad de poder incidir a las acciones del enemigo permite que una gestión de la información planificada de forma correcta no solo potencie la seguridad en las operaciones, sino que también proporciona información crítica que puede utilizarse para la colaborar con la función protección del personal y optimizar los movimientos militares.

La necesidad de proteger información sensible, que pueden ser posteo sin intenciones maliciosa del personal, en las redes sociales, más aún cuando se están llevando adelante diferentes operaciones, existiendo datos que puede ser aprovechada por adversarios durante el conflicto, sumado a los riesgos de

desinformación y manipulación en el ámbito cibernético, demuestran la necesidad de contar con procedimientos de ciberseguridad y medidas de contrainteligencia para neutralizar posibles amenazas. Todo esto enfatiza cómo la información que se encuentra disponible en las redes sociales, al no ser protegida adecuadamente, puede vulnerar la integridad de las operaciones. Esto contribuye a explorar las oportunidades que la información contenida en las redes sociales en conflictos armados, destacando que el control efectivo de la información es un elemento crucial la protección de las fuerzas.

Los conflictos recientes, como la resistencia en Myanmar y el uso de redes sociales por ISIS, evidencian la relevancia de incorporar más capacitación en ciberseguridad y en explotación de fuentes abiertas, como el caso de las redes sociales, dentro de la organización. Esto no solo permite mejores medidas de protección de la información, sino que también capacitan a las fuerzas para identificar, neutralizar y adaptarse a las amenazas en el espacio digital. La implementación de estos procedimientos hace que una gestión proactiva de la información fortalece las capacidades de protección en los entornos digitales.

La implementación de medidas de seguridad contra inteligencia digital permite preservar la cohesión y la moral de las tropas en el campo de combate, protegiendo al personal militar de las acciones del enemigo. La posibilidad de identificar y neutralizar estas amenazas en redes sociales confirma que la protección en el ambiente digital es tan fundamental como en el campo físico, contribuyendo a la función de combate protección y fortaleciendo el poder de combate de las fuerzas. Esto demuestra que las redes sociales, cuando se gestionan adecuadamente, actúan no solo como plataformas de información, sino como mecanismos defensivos para proteger la seguridad y moral de las fuerzas en escenarios de conflicto.

Por lo expuesto anteriormente se demuestra el profundo impacto que las redes sociales han tenido en la función de combate protección en los conflictos armados de la última década. El control y uso de forma planificada de las plataformas sociales ofrece a los comandantes una ventaja operativa significativa, permitiéndoles proteger al personal, los medios y las maniobras dentro del teatro de operaciones.

La capacidad de emplear redes sociales de manera controlada representa una herramienta vital, pero también un desafío constante que exige un enfoque multidisciplinario en ciberdefensa y operaciones de información. Las redes sociales, al integrarse en el planeamiento de ciberdefensa y contrainteligencia, no solo

fortalecen la seguridad informativa, sino que también permiten a los comandantes neutralizar amenazas antes de que afecten el teatro de operaciones.

Las lecciones aprendidas en este trabajo refuerzan que las redes sociales son un elemento crítico en la gestión de la información, actuando como un multiplicador de fuerzas que extiende la capacidad de los comandantes para mantener la moral, cohesión y efectividad operativa de sus tropas frente a las amenazas de la guerra híbrida. En un contexto donde las fronteras entre el espacio físico y el digital se han desdibujado, la gestión de la información en redes sociales no solo permite una respuesta oportuna y coordinada ante posibles amenazas, sino que colabora con la función de combate protección al reducir la exposición a riesgos.

Una gestión eficiente y defensiva de la información en redes sociales no solo protege la integridad de las fuerzas propias, sino que también se constituye como una herramienta muy importante en la guerra moderna, contribuyendo así, con la protección operativa en los conflictos armados actuales y futuros.

En un entorno donde cada publicación y mensaje puede tener repercusiones en el campo de combate, la gestión de la información en redes sociales se consolida como una extensión indispensable de la función de combate protección en el teatro de operaciones moderno.

La gestión de información en redes sociales debe integrarse en la doctrina de nuestra nación, sirviendo a la función de combate Protección mediante protocolos claros de contrainteligencia y capacitación en ciberseguridad para personal militar.

BIBLIOGRAFIA

- Ali, R. (2023). Digital warfare: The role of social media in the Israel-Hamas conflict. *Journal of Conflict Studies.*
- Ayhud F. S. (2019) *El Nivel Operacional, la Opinión Pública y las Redes Sociales como herramienta de manejo de medios de comunicación*. Buenos Aires. Escuela Superior de Guerra Conjunta.
- Baker, L. (2022). Propaganda warfare: The role of TikTok in ISIS recruitment and influence. *Middle Eastern Studies Quarterly*.
- Brown, K. (2023). The role of psychological operations in the Russia-Ukraine conflict. *Defense Studies Journal*.
- Belkis Wille (10 de septiembre de 2020). "Video no disponible" Las plataformas de redes sociales elimina evidencias de crímenes de guerra. Human Rights Watch. https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes
- Burgess, J., & Green, J. (2018). YouTube: Online Video and Participatory Culture. Polity Press.
- Clarke, C., & Knake, R. K. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin.
- Derakhshan, H., & Wardle, C. (2017). Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe.
- Darko Janjevic (28 de agosto de 2024). ¿Quién es Pavel Durov, el magnate que fundó Telegram? DW. https://www.dw.com/es/qui%C3%A9n-es-pavel-durov-el-multimillonario-fundador-de-telegram/a-70074441#:~:text=En%202013%2C%20Pavel%20Durov%20y,a%20su%20casa%20en%20Rusia
- Ejército Argentino (2014). *ROB–00–01* Conducción para la Fuerzas Terrestres, p. IV – 5.
- Ejército Argentino (2008). *ROD 11-01* Inteligencia Táctica, p.11.
- Jorquera Escobar René (12 de Abril de 2024). *Redes sociales y guerra híbrida, un desafío para la defensa*. Pucara. https://www.pucara.org/post/redes-sociales-y-guerra-h%C3%ADbrida-un-desaf%C3%ADo-para-la-defensa
- Kilcullen, David. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford University Press, 2013.

- Khan, R. (2022). OSINT and social media in the Nagorno-Karabakh conflict. *International Journal of Intelligence and Security*.
- Ko, T. (2023). Civil resistance and social media in Myanmar. *Asian Conflict Analysis Review.*
- Labrador Blanes Maria Jose y Reyes Betanzo Claudia; *La comunicación científica como herramienta contra la desinformación en la neoglobalización;* RIL; 2023; p. 195.
- Leticia Rodríguez Fernández (2015). *El uso de Facebook y Twitter de las Fuerzas de Defensa de Israel en la operación "Margen Protector"*; Universidad Antonio Nebrija. https://core.ac.uk/download/pdf/38816987.pdf
- Manuel Antonio Conde del Rio (2021). *Estructura de TikTok: Estudio de caso de la red social de los más jóvenes. Revista de Ciencias de la Comunicación e Información*.
  https://www.revistaccinformacion.net/index.php/rcci/article/view/126/348
- Newton, C. (2016). The Story of Instagram's Acquisition by Facebook. The Verge.
- Otero, S. (2013). *Redes sociales y conflictos modernos*. Centro Argentino de Estudios Estratégicos.
- Petrov, I. (2022). *Social media mishaps in modern warfare: Case studies from the Russia-Ukraine conflict*. *Journal of Military Intelligence*, p. 101-106.
- Phillips, S. (2007). *A brief history of Facebook. The Guardian.*
- Rubén Ramos Antón, Francisco José Murcia Verdú y María José Ufarte Ruiz (20 de junio de 2023). *Contar la guerra a partir de Twitter: Estudio de caso de Descifrando la Guerra. Dialnet*. https://revistas.ucm.es/index.php/ESMP/article/view/84872/4564456566815
- Rao, L. (2008). *Twitter's History: First 140 Characters*. *TechCrunch.*
- Rebeca Suárez Álvarez, Antonio García Jiménez, Beatriz Catalina García (diciembre de 2023). *Guerra Rusia-Ucrania en TikTok. La representación de la actualidad y su impacto*. ISSN. https://analisi.cat/article/view/v69-suarez-garcia-catalina/3587-pdf-es
- Singer P.W. y Brooking E. (2018). LikeWar: The Weaponization of Social Media. National Defense Industrial Association.
- Smith, R. (2022*). Misinformation warfare on social media: Analysis of Russia's*

strategies. Journal of Military Ethics, p. 203.

- Stein Tønnessona, Min Zaw Oo y Ne Lynn Aung (04 de Mayo de 2021). *Pretendiendo ser Estados: el uso de Facebook por parte de las fuerzas armadas Grupos en Myanma. Taylor and Francis Group*. https://doi.org/10.1080/00472336.2021.1905865
- Woolley, S. C., & Howard, P. N. (2017). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.