TRABAJO FINAL INTEGRADOR

TEMA:

Redes sociales y operaciones militares

TÍTULO:

Oportunidades y riesgos del empleo de las redes sociales en operaciones militares

SIMON, Rubén Ariel

2021

RESUMEN

Las nuevas tecnologías de la información y la comunicación han generado un nuevo frente de combate, el mundo de las redes sociales; más problemático y difícil de contener, ya que el espacio en el cual se desarrolla permite la filtración de estas operaciones a cada rincón de la internet.

La falta de identificación de las oportunidades y del valor fundamental que han tomado las redes sociales en todo proceso de comunicación y de cómo explotarlas en el nivel operacional puede derivar en una insuficiente manera de informar y ser aprovechado por el adversario para influir en diferentes niveles y actores. Asimismo, el empleo de las redes sociales para comunicar sin reconocer los riesgos que implica, las vulnerabilidades que presenta y las posibilidades de neutralizar sus efectos, puede generar resultados contrarios a los que se buscan.

El presente trabajo tiene por objetivo determinar las principales oportunidades y riesgos del empleo de las redes sociales como operaciones de información en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales; a la luz de los hechos históricos más trascendentales en esta materia. Desde Pillar of Defense en el año 2012, bautizada por los medios de comunicación como *la primera guerra en redes sociales*, se analizará la evolución en los conflictos en los que las redes sociales se hayan empleado con mayor magnitud, identificando las oportunidades y riesgos que se presentan en el contexto militar dentro de un escenario de guerra de información.

Dicho objetivo tiene su correlato en el interrogante que guía este trabajo. ¿Cuáles son las principales oportunidades y riesgos del empleo de las redes sociales en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales?

Palabras Claves:

Información. Operaciones. Oportunidades. Redes. Riesgos.

CONTENIDO

INTRODUCCIÓN

Las operaciones de información son tan antiguas como los conflictos mismos, ya Sun Tzu proponía “Todo el Arte de la Guerra se basa en el engaño. El supremo Arte de la Guerra es someter al enemigo sin luchar” (Biblioteca Virtual Universal, 2003, pág. s/n). De esta frase, se puede observar la utilización del engaño para evitar la batalla. Esta necesidad de evitar el choque físico o al menos disminuir su magnitud le ha dado una gran relevancia a las operaciones de información, ya que su aplicación puede ahorrar vidas humanas y contribuir al éxito de la misión.

Las operaciones de información están influenciadas por las herramientas tecnológicas disponibles en un momento dado. Por lo tanto, con el avance de la tecnología de la comunicación, desde la prensa escrita y la radio hasta la televisión por satélite e internet móvil de alta velocidad, el alcance y la velocidad de los mensajes de los propagandistas se han multiplicado.

Ya en el siglo XIX, Clausewitz escribió entre sus notas “cada época tenía su propio tipo de guerra, sus propias condiciones limitantes, y sus propias ideas preconcebidas peculiares. De ello se desprende que los acontecimientos de cada época deben juzgarse a la luz de sus propias peculiaridades" (Clausewitz, 1976, pág. s/n). La falta de identificación de las oportunidades y del valor fundamental que han tomado las redes sociales en todo proceso de comunicación y de cómo explotarlas en el nivel operacional puede derivar en una insuficiente manera de informar y ser aprovechado por el adversario para influir en diferentes niveles y actores. Asimismo, el empleo de las redes sociales para comunicar sin reconocer los riesgos que implica, las vulnerabilidades que presenta y las posibilidades de neutralizar sus efectos puede generar resultados contrarios a los buscados.

“Pensé que una vez que todos pudieran hablar libremente e intercambiar información e ideas, el mundo automáticamente sería un lugar mejor”, confesó el cofundador de Twitter, Evan Williams. “Me equivoqué en eso” (Oneal, 2019, pág. s/n). Así como el internet moderno interrumpió el mundo del entretenimiento, los negocios y las citas, ahora también interrumpe en la guerra y la política, convirtiéndose en una revolución que ningún líder, grupo, ejército o nación puede permitirse ignorar.

Durante el presente trabajo se observará el empleo de las redes sociales en el desarrollo de operaciones de información como contribución al logro de los objetivos

operacionales en diferentes campañas. Desde la operación Pillar of Defense en el año 2012, bautizada por los medios de comunicación como *la primera guerra en redes sociales* y observando su evolución en las operaciones que con mayor magnitud se hayan utilizado y contribuido al logro de los objetivos, identificando las oportunidades y riesgos en el contexto militar dentro de un escenario de guerra de información.

Contexto Situacional

La operación Pillar of Defense, que tuvo lugar en el año 2012, fue bautizada por los medios de comunicación como *la primera guerra en redes sociales* y ofreció un vistazo de una forma emergente de guerra. Fue un conflicto en el que cada lado se había organizado para burlarse y engañarse mutuamente en línea, incluso mientras se involucraban en una lucha de vida o muerte en el mundo real. Sus batallas atrajeron a millones de combatientes internacionales, algunos eran partidarios apasionados de alguno de los dos bandos y otros se encontraron de casualidad con la guerra mientras buscaban noticias o entretenimiento en internet. De todos modos, dieron forma a la lucha, fortaleciendo la voz de una facción u otra y, en pequeño grado, alterando el curso de los acontecimientos en el terreno.

Ahora había tres frentes en juego, explicó el director de información de Israel, dos eran predecibles: la lucha *física* que Israel dominó fácilmente y la lucha *cibernética* en la que las Fuerzas de Defensas Israelíes (FDI) derrotaron cómodamente los esfuerzos de los piratas informáticos palestinos. También mencionó que había un tercer frente, *el mundo de las redes sociales*; este frente resultó más problemático y difícil de contener, y pronto se filtró en todos los rincones de internet. Un conflicto físico relativamente pequeño, librado en un área de tamaño acotada, se convirtió en un compromiso global que provocó el intercambio de más de 10 millones de mensajes encendidos solo en Twitter (Moody, 2013).

Asimismo, las FDI y los militantes de Hamas lucharon en múltiples *guerras de Twitter* ante una audiencia global. Las FDI se tomaron esta pelea, y cómo influyó en la opinión mundial, tan seriamente que el volumen de *me gusta* y retweets influyó en los objetivos que eligió y el ritmo de las operaciones en el terreno.

Las FDI desplegaron una cuenta de Twitter, páginas de Facebook en varios idiomas, páginas de blogs de Tumblr, un canal de YouTube e incluso una página de Pinterest; había infografías ingeniosas y un flujo de videos y estadísticas. Maximizando

la participación de los seguidores, el blog oficial de las FDI ofrecía pequeñas recompensas digitales para usuarios habituales.

Por el contrario, los esfuerzos de propaganda de los militantes de Hamas estaban menos estructurados. La mayor parte de su respuesta en las redes sociales provino de millones de observadores no afiliados de todo el mundo, que observaron con horror la difícil situación de los civiles palestinos y se unieron a la refriega. El hashtag de Twitter #GazaUnderFire se convirtió en una corriente interminable de atrocidades: imágenes de edificios bombardeados, niños muertos, padres llorando. Incluso, mientras los misiles volaban, las FDI y Hamas continuaban narrando el conflicto, cada uno publicando alertas, actualizaciones y una serie constante de burlas.

Después de que las partes establecieron un alto el fuego se tuvo la idea de que esta extraña guerra de internet era un montón de ruido digital, pero eso hubiera sido un error. Años después de que la Operación Pillar of Defense desapareciera de la mente del público, el profesor de la Universidad Americana Thomas Zeitzoff llevó a cabo un estudio minucioso de cientos de miles de tweets, que luego trazó a lo largo de cada hora del lado físico del conflicto de ocho días. Lo que encontró fue impactante. En el caso de Israel, un repentino aumento en la simpatía en línea por Hamas redujo más de la mitad el ritmo de los ataques aéreos israelíes y dio como resultado un salto de tamaño similar en los propios esfuerzos de propaganda de Israel. Registrando el sentimiento (pro-Israel o pro-Palestina) de estos tweets en una línea de tiempo, no solo se podría inferir lo que estaba sucediendo en el terreno, sino que también podría predecir qué haría Israel a continuación. Los políticos israelíes y los comandantes de las FDI no se habían limitado a estudiar detenidamente los mapas del campo de batalla, también habían estado vigilando sus feeds de Twitter, el campo de batalla de la guerra de las redes sociales (Singer & Brooking, 2018)

La lección fue clara: la guerra moderna no solo requiere de una campaña militar bien planificada, también requiere de una campaña de marketing viral. En el futuro, tanto israelíes como palestinos aplicarían esta lección, aunque de formas muy diferentes. Sus enfoques son ampliamente representativos de las dos estrategias que caracterizan cómo los combatientes abordan las operaciones de información en las redes sociales en la actualidad, débilmente interconectadas u organizadas centralmente.

El siguiente gran estallido de guerra real que se volvió a reproducir en la red se produjo en el año 2014, cuando Israel y Hamas cayeron en otro conflicto más sangriento

e incluso más desigual, que culminó con la Operación Margen Protector, la invasión terrestre de las FDI de la ciudad de Gaza.

Hamas solicitó activamente imágenes de las víctimas de los ataques aéreos israelíes, la de niños eran las más buscadas por ser las que mayor impacto causarían y las publicó en línea lo antes posible, *No hay nada de malo en publicar imágenes de los heridos,* instó un video de la web. Las imágenes reales de la devastación pronto se mezclaron con un mar de falsificaciones y aunque las FDI ganaron todas las batallas, a medida que aumentaban las bajas, la charla en las redes sociales se hizo implacable en sus críticas al ejército israelí. En un solo mes, el hashtag #GazaUnderAttack se usó más de 4 millones de veces, veinte veces más que el que impulsaban las FDI, #IsraelUnderFire (Blanco, 2014).

Cuando la Operación Margen Protector terminó siete semanas después de su inicio, muchos israelíes estaban furiosos, sentían que su gobierno se había derrumbado bajo la presión internacional; nueve de cada diez creían que los militares no habían logrado sus objetivos (Singer & Brooking, 2018).

Estado Actual del Tema

Este nuevo entorno que enlaza a personas mediante vínculos sociales amplificados por la tecnología está generando nuevos escenarios en los que los internautas están cada vez más informados. Con estas nuevas herramientas, los usuarios son consumidores y productores de contenidos colaborativos, saben mejor lo que quieren y se organizan en un amplio abanico de redes sociales estimuladas por las Tecnologías de Información y Comunicación (Maqueira & Bruque, 2009).

El conflicto de información está cambiando y reorganizándose espontáneamente debido a la influencia disruptiva de otro sistema complejo: las redes sociales. La relación entre las redes sociales y el conflicto de información aún no ha alcanzado su estado final, lo que dificulta predecir el futuro con algún grado de certeza. Sin embargo, las redes sociales son una herramienta ideal para los conflictos basados en la información.

Dada su naturaleza ubicua, se puede esperar que las redes sociales se vuelvan más frecuentes en los conflictos basados en la información y sus roles pueden inicialmente volverse más significativos. La utilización de las herramientas que ofrecen

las redes sociales para extraer datos necesarios permite analizar los efectos causados por las publicaciones, y es muy importante para la generación de los próximos contenidos por publicar. Por lo tanto, el seguimiento constante de los efectos causados es vital para una eficaz difusión, ya que una misma actividad puede ser mostrada de diferentes maneras, y así llegar a distintos grupos de personas.

Desde las naciones más poderosas del mundo hasta los combatientes comunes han convertido las redes sociales en un arma. Todos luchan por doblegar el entorno de la información global a su voluntad. Internet, que alguna vez fue un lugar luminoso y aireado de conexión personal, desde entonces se ha transformado en el sistema nervioso de un campo de batalla donde la información misma es el arma.

Las redes sociales son una parte integral de la evolución de la web, se han convertido en una tecnología casi ubicua a la que se puede acceder tanto desde computadoras de escritorio tradicionales hasta muchos y diferentes dispositivos móviles, y su utilización desempeña un papel importante en conflictos basados en la información. Asimismo, y teniendo en cuenta las expectativas que se generan debido a este fenómeno, son necesarios la constante revisión y nuevos análisis que ayuden a medir y comprender en qué momento del desarrollo se encuentra y si se están cumpliendo o no los objetivos, pero también de disponer de casos prácticos que permitan contar con estadísticas que guíen el camino para el futuro.

Para lograr la victoria se deben cumplir los objetivos propuestos, encontrar y neutralizar el *centro de gravedad* de un adversario. Este suele ser el ejército de un rival, cuya destrucción suele poner fin a su capacidad de lucha, aunque no siempre derrotar a un ejército es el camino más eficaz. “Los elementos morales se encuentran entre los más importantes en la guerra”, escribió Clausewitz, y “constituyen el espíritu que impregna la guerra en su conjunto. Establecen una estrecha afinidad con la voluntad que mueve y lidera toda la masa de fuerza. La victoria se consigue acabando con la determinación del contrario para luchar, más que destruyendo sus tropas” (Clausewitz, 1976, pág. 187). Por lo tanto, si se encuentra la forma de socavar el espíritu de lucha del rival, se podría lograr la victoria, aun evitando al ejército enemigo.

“Lo que no se comunica no existe. O existe solamente para unos pocos. Por eso es importante que las organizaciones cuenten con una estrategia de comunicación que les sirva de guía a la hora de comunicarse con sus públicos” (Aced, 2013, pág. 19). Las redes sociales han cambiado no solo el mensaje, sino también la dinámica del conflicto.

La forma en que se accede a la información, se manipula y se difunde ha adquirido un nuevo poder. Quién estuvo involucrado en la pelea, dónde se ubicaron e incluso cómo lograron la victoria, se ha torcido y transformado; de hecho, lo que está en línea puede cambiar el curso de una batalla o eliminar por completo su necesidad.

Este trabajo analizará el papel de las redes sociales en los conflictos de información, con el objetivo de encontrar las principales oportunidades que brinda su utilización y los riesgos a los que se expone. Asimismo, se abordará desde la definición de conflictos de información como una aplicación de los conceptos de guerra de la información en el contexto militar y "el empleo integrado de las capacidades relacionadas con la información durante las operaciones militares, en concierto con otras líneas de operación para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios al mismo tiempo que se protegen las propias" (De Vergara & Trama, 2017, pág. 154).

Las Fuerzas Armadas argentinas no disponen de un marco doctrinario que regule el empleo de las redes sociales en operaciones de información; poseen deficiencias en poder emplear estas nuevas herramientas para contribuir al logro de los objetivos operacionales, y sus formas de abordaje para influir positivamente. El uso de las redes sociales en las diferentes fuerzas se ha limitado a la comunicación institucional, dirigida principalmente al reclutamiento, publicaciones de efemérides, actividades de ceremonial.

Para el presente trabajo, se considera necesario que dentro del proceso de planeamiento de una campaña se contemple el empleo de las redes sociales como parte de las operaciones de información. Sin embargo, antes de poder hacer esto, se deben identificar correctamente las oportunidades y los riesgos que se deben enfrentar para que su uso contribuya al logro de los objetivos operacionales perseguidos.

Planteo Del Problema

Según lo analizado anteriormente, y teniendo en cuenta la trascendencia que implica el desarrollo de las operaciones de información contribuyendo al logro de los objetivos establecidos, surge la necesidad de formularse la siguiente pregunta de investigación: ¿Cuáles son las principales oportunidades y riesgos del empleo de las redes sociales en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales?

Alcances y Limitaciones de la Propuesta

El presente trabajo abordará la temática buscando comprender cómo el empleo de las redes sociales, como parte integrante de las operaciones de información, puede contribuir al logro de los objetivos operacionales perseguidos dentro de una campaña, reconociendo las oportunidades que presenta, como así también los riesgos que conlleva.

Basado en el análisis de los principales conflictos bélicos en los cuales las redes sociales han tenido una gran influencia en el nivel operacional de una campaña, tomando como inicio del análisis a la operación Pillar of Defense en 2012 y observando su evolución hasta la actualidad. Si bien es sabido que las operaciones en redes sociales también han sido empleadas para generar manifestaciones y protestas en contra de gobiernos, como lo fue la Primavera Árabe, o influir en elecciones de otros países, como el ejemplo de la supuesta interferencia de Rusia en las elecciones de los Estados Unidos; estos casos no serán objeto del estudio por no desarrollarse en el nivel operacional de una campaña, aunque sí pueden ser nombrados como comparaciones o ejemplos de operaciones de información en el presente trabajo.

Aportes Teóricos y Prácticos al Campo Disciplinar

El presente trabajo busca realizar un aporte al proceso de planeamiento en el nivel operacional de toda campaña y en mayor magnitud en aquellas en las cuales las operaciones de información tengan un papel preponderante. Debido a los complejos escenarios que se presentan en la actualidad y que seguramente serán de mayor complejidad en el futuro, se requiere de la utilización de todas las herramientas posibles que contribuyan al logro de los objetivos perseguidos.

El empleo de las redes sociales como operaciones de información es una herramienta fundamental que permite llegar a millones de usuarios de todo el mundo, si se las utiliza de manera correcta y con una estrategia acertada. Por lo cual, es necesario conocer y mantener actualizado constantemente cuáles son las oportunidades y beneficios de su utilización, pero también tener el conocimiento de los riesgos a los que se expone.

Por lo expresado anteriormente, el presente trabajo busca identificar las oportunidades y riesgos al utilizar las redes sociales como operaciones de información,

desde la comprensión de su uso en diferentes conflictos bélicos y el análisis de su contribución al logro de los objetivos operacionales perseguidos en el desarrollo de una campaña.

Objetivos

Para el desarrollo del presente trabajo se han establecido un objetivo general y dos objetivos particulares que se desarrollarán en los capítulos que conforman la investigación a desarrollar.

Objetivo General

Determinar las principales oportunidades y riesgos del empleo de las redes sociales como operaciones de información en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales.

Objetivos Particulares

Identificar las principales oportunidades y riesgos que brindan las redes sociales a las operaciones de información en los conflictos modernos para contribuir al logro de los objetivos operacionales.

Describir el empleo de las redes sociales en los conflictos modernos de la última década para contribuir al logro de los objetivos operacionales.

Hipótesis

El empleo de las redes sociales en el desarrollo de una campaña con el fin de contribuir al logro de los objetivos operacionales presenta oportunidades como influenciar en la opinión pública, legitimar las operaciones propias, degradar al oponente; lo cual representa una mayor libertad de acción para el comandante, asumiendo los riesgos que su empleo también presenta por las vulnerabilidades propias de las redes sociales.

Metodología

La presente investigación será realizada mediante el empleo de la metodología del tipo cualitativa con un diseño descriptivo para poder lograr un necesario grado de familiaridad de cómo el empleo de las redes sociales ha contribuido al logro de los objetivos operacionales en los conflictos modernos. Se recurrirá a fuentes secundarias

para realizar un análisis documental de la doctrina de fuerzas armadas, como las de Brasil y los Estados Unidos, y un análisis bibliográfico de libros de autores reconocidos, sitios webs oficiales de fuerzas armadas de otros países, trabajos de investigaciones publicados, revistas y publicaciones webs validados sobre la temática, lo que permitirán cumplir con los objetivos trazados y, de manera práctica y concreta, ir dando respuesta al interrogante planteado.

Estructura Formal del Trabajo

La estructura formal del presente trabajo se dividirá en dos capítulos, siendo el primero denominado "CARACTERÍSTICAS DE LAS REDES SOCIALES", donde se identificarán las características principales que crean oportunidades para llevar a cabo las operaciones de información, y se analizarán las formas en que las redes sociales han creado un nuevo entorno para el conflicto, transformando la velocidad, la difusión y la accesibilidad de la información, cambiando la naturaleza misma del secreto.

Continuando con el segundo capítulo "EL EMPLEO DE LAS REDES SOCIALES EN LOS CONFLICTOS MODERNOS" donde se describirán como diferentes actores han realizado operaciones de información empleando las redes sociales en los conflictos más recientes y su contribución al logro de los objetivos operacionales.

Finalmente, se desarrollarán las "CONCLUSIONES" a las que se ha llegado mediante el presente trabajo de investigación, respondiendo los interrogantes planteados y cumpliendo con los objetivos particulares y generales trazados en la introducción.

CAPÍTULO I: CARACTERÍSTICAS DE LAS REDES SOCIALES

Desde sus inicios las redes sociales han evolucionado tanto, que a través de complejos sistemas de algoritmos e inteligencia artificial, recuerdan el comportamiento de los usuarios en Internet y predicen cuáles serán los movimientos futuros con precisión milimétrica (Oliva, 2020). El gran aumento de popularidad internacional de las redes sociales y su utilización masiva por parte de la población en general, representa un acontecimiento trascendental para los conflictos modernos. A continuación, se describen las principales características de las redes sociales que permiten entender a las mismas y comprender las oportunidades y riesgos que presentan para su empleo en la realización de operaciones de información.

Principios Básicos

En su libro Likewar, The Weaponization of Social Media, los autores Singer y Brooking (2018) establecen cinco principios básicos que forman los cimientos de las redes sociales y la masividad de su empleo; el primer principio es que luego de décadas de crecimiento Internet se ha convertido en el medio principal de comunicación, comercio y política global. En la actualidad Internet es verdaderamente global e instantáneo: la combinación definitiva de conexión individual y transmisión masiva. A través de las redes sociales, la web continuará creciendo en tamaño, alcance y membrecía, pero su forma esencial y su centralidad en el ecosistema de la información no cambiarán. Internet ha alcanzado un punto de madurez en el que la mayoría de sus jugadores clave seguirán siendo los mismos.

En segundo lugar, Internet se ha convertido en un campo de batalla, por muy integral que se haya vuelto para los negocios y la vida social, ahora es igualmente indispensable para los militares y los gobiernos, los autoritarios y activistas, los espías y los soldados. Es una plataforma para lograr los objetivos de cualquier actor que lo manipule con mayor eficacia. Todos lo utilizan para librar guerras que no observan fronteras claras y el resultado es que cada batalla parece personal, pero cada conflicto es global.

En tercer lugar, este campo de batalla cambia la forma en que se libran los conflictos. Las redes sociales han hecho que los secretos sean esencialmente imposibles de guardar; si sucede algo, es probable que haya un registro digital de ello (una imagen,

un video o un tweet) que saldrá a la luz en unos segundos o años. Sin embargo, un evento solo tiene poder si las personas también creen que sucedió. La naturaleza de este proceso significa que un evento fabricado puede tener poder real, mientras que un evento demostrablemente verdadero puede volverse irrelevante, por lo que, debido a que la viralidad puede confundir a la verdad, lo que se conoce se puede remodelar. El "poder" en este campo de batalla no se mide por la fuerza física o el hardware de alta tecnología, sino por el mando de la atención y el resultado es una disputa de manipulación psicológica y algorítmica, que se libra a través de un sinfín de eventos virales en competencia.

Como cuarto principio, esta batalla cambia lo que significa "guerra". Ganar estas batallas en línea no solo gana la web, sino que gana el mundo. Estos resultados se convierten en la base de la próxima batalla inevitable por la verdad en línea, desvaneciendo aún más la distinción entre acciones en los ámbitos físico y digital con la consecuencia de que en internet, "guerra" y "política" han comenzado a fusionarse. Obedeciendo las mismas reglas y habitando el mismo espectro, sus tácticas e incluso los jugadores son cada vez más indistinguibles, no siempre son los políticos, generales, abogados o diplomáticos quienes están definiendo las leyes de esta nueva lucha.

En quinto y último lugar, todos son parte de esta guerra. Si está en línea, su atención es como un trozo de territorio en pugna, en el que se disputan conflictos que pueden o no darse cuenta de que se desarrollan a su alrededor. Todo lo que se "ve", "gusta" o "comparte" representa una pequeña onda en el campo de batalla de la información, privilegiando un lado a expensas de otros. Su atención y sus acciones en línea son, por lo tanto, objetivos en una serie interminable de batallas.

La Veracidad contra la Viralidad

Internet ha creado el equivalente a varios miles de millones de periódicos, hechos a la medida de los gustos de cada usuario de redes sociales del planeta. En consecuencia, ya no hay un solo conjunto de hechos, sino que existe un conjunto de "hechos" para cada punto de vista concebible. Con unas pocas pulsaciones de teclas, Internet puede conectar a personas de ideas afines a grandes distancias e incluso superar las barreras del idioma. No importa si la causa es peligrosa (apoyo a un grupo terrorista), mundana (apoyo a un partido político) o absurda (creencia de que la tierra es plana), las redes sociales garantizan que se puede encontrar a otras personas que

compartan sus puntos de vista. Aún más, los propios algoritmos de las plataformas lo guiarán hacia ellos y a medida que los grupos crecen, incluso las causas más remotas pueden coordinarse y organizarse, ganar visibilidad y encontrar nuevos reclutas.

Estudios, en numerosos países, en los que participaron millones de personas, han revelado una regla fundamental que explica cómo se difunde la información a través de Internet, así como da forma a nuestra política, los medios de comunicación y las guerras. El mejor predictor no es la precisión ni el contenido; es el número de amigos que comparten el contenido primero. Es más probable que crean lo que dice y luego lo compartan con otros que a su vez, creerán lo que dicen ellos. Este fenómeno se llama "homofilia", que es la tendencia de las personas por la atracción a sus homónimos, lo que hace a los humanos seres sociales capaces de congregarse en grupos grandes y de ideas afines (Anagnostopoulos, 2014).

Este término explica el crecimiento de la civilización y las culturas, pero también es la razón por la que una falsedad en Internet, una vez que comienza a extenderse, rara vez se pueda detener. A medida que los usuarios responden positivamente a ciertos tipos de contenido, los algoritmos que impulsan las fuentes de noticias de las redes sociales aseguran que se vean cada vez más. Cada una de estas pequeñas decisiones se expande hacia afuera, alterando el flujo de información en todo el sistema; pero hay una trampa, estas ondas también reverberan hacia adentro. Por lo tanto, cuando se decide compartir un contenido en particular, no solo está influyendo en el entorno de información futuro, sino que también está siendo influenciado por cualquier información que ya haya pasado por su camino.

En una serie exhaustiva de experimentos, los investigadores de la Universidad de Yale encontraron que las personas eran significativamente más propensas a creer un titular si habían visto uno similar antes. No importaba si la historia era falsa; ni siquiera si la historia iba precedida de una advertencia de que podría ser falsa, lo más significativo fue la familiaridad. Cuanto más a menudo se escuche un reclamo, menos probabilidades tendrán de evaluarlo críticamente y cuanto más tiempo permanezca en una comunidad en particular, más se repetirán sus afirmaciones hasta que se conviertan en obviedades, incluso si siguen siendo lo opuesto a la verdad (Pennycook, Cannon, & Rand, 2018).

Después de todo, el hecho es una cuestión de consenso, elimina ese consenso y el hecho se convierte en una cuestión de opinión, aprenda a dominar y manipular esa

opinión, y tendrá derecho a remodelar la estructura del mundo. “Desafortunadamente, ya no existen los hechos” (Holmes, 2016, pág. s/n), una afirmación extraña pero en cierto modo real. En las redes sociales, además hay otro fenómeno en acción y es que todos pueden tener derecho a sus propios hechos, pero rara vez se forman sus propias opiniones, hay alguien más fabricando las creencias que se vuelven virales en línea.

La Narrativa

Las narrativas son los bloques de construcción que explican cómo los humanos ven el mundo y cómo existen en grandes grupos. Proporcionan la lente a través de la cual nos percibimos a nosotros mismos, a los demás y al entorno que nos rodea; son las historias que unen lo pequeño con lo grande, conectando la experiencia personal con una noción más amplia de cómo funciona el mundo. Cuanto más fuerte es una narración, más probabilidades hay que se la retenga y recuerde y el poder de una narrativa depende de una confluencia de factores, pero el más importante es la coherencia: la forma en que un evento se vincula lógicamente con el siguiente. Las mentes humanas están programadas para buscar y crear narrativas y para que la misma sea exitosa tiene que tener tres rasgos característicos: simplicidad, resonancia y novedad (Rodriguez, 2019).

Como primera regla la simplicidad es un ejemplo lo sucedido durante las elecciones de Estados Unidos en el 2016. Los investigadores de la Universidad Carnegie Mellon estudiaron y clasificaron la complejidad del lenguaje de los candidatos y descubrieron que el vocabulario de Trump se midió en el nivel más bajo de todos los candidatos, comprensible para alguien con una educación de quinto grado. Este fenómeno puede parecer sin precedentes, pero es coherente con un patrón histórico más amplio. Comenzando con el primer discurso inaugural de George Washington, que se midió como uno de los más complejos, en general los presidentes estadounidenses se comunicaron a nivel universitario solo cuando los periódicos dominaban la comunicación de masas, pero cada vez que se implantaba una nueva tecnología, la puntuación de complejidad bajaba. Descendió con el advenimiento de la radio en la década de 1920, nuevamente con la entrada de la televisión en la década de 1950, y ahora una vez más con las redes sociales. Para decirlo de otra manera: cuanto más accesible es la tecnología, más simple se vuelve una voz ganadora (University, 2016).

La segunda regla de la narrativa es la resonancia, donde casi todas las narrativas efectivas se ajustan a lo que los científicos sociales llaman "marcos", productos de un lenguaje y una cultura particulares que se sienten instantáneamente y profundamente familiares.

La tercera y última regla narrativa es la novedad. Así como los marcos narrativos ayudan a generar resonancia, también sirven para hacer que las cosas sean predecibles. Sin embargo, demasiada previsibilidad puede resultar aburrida, especialmente en una época de períodos de atención microscópicos y entretenimiento ilimitado. Los narradores más eficaces modifican, subvierten o "rompen" un marco, jugando con las expectativas de la audiencia para obtener nuevos niveles de atención.

Estos tres rasgos determinan qué narrativas se mantienen y cuáles fracasan. Controlar la narrativa es dictar a una audiencia quiénes son los héroes y villanos; qué está bien y qué está mal; qué es real y qué no. Como dijo el yihadista Omar Hammami, líder del grupo terrorista con sede en Somalia Al-Shabaab, "la guerra de narrativas se ha vuelto incluso más importante que la guerra de armadas, napalm y cuchillos". Los grandes perdedores en esta batalla narrativa son aquellas personas o instituciones que son demasiado grandes, demasiado lentas o demasiado vacilantes para tejer tales historias (Cottee, 2015).

La Estrategia en Línea

Desde los inicios de la humanidad, cuando un ciudadano de una nación se comunicaba directamente con uno de otra nación, generalmente los Estados participaban en el proceso, ya sea certificando el franqueo postal o regulando el tráfico de las líneas telegráficas internacionales. Si los dos Estados entraban en guerra, en una disputa comercial o simplemente no se agradaban, esa comunicación prácticamente se detenía. Se interceptaban cartas, cortaban cables, el flujo de información se reducía notablemente; Internet cambió esto rápidamente.

Un artículo revolucionario de 1993 titulado “Cyberwar Is Coming!” en un momento en el que Internet aún no se había abierto a la actividad comercial, los autores observaron que la información se estaba convirtiendo en un recurso estratégico y su valor e influencia en la era postindustrial resultaba equivalente al capital y el trabajo en la era industrial. En consecuencia, los conflictos futuros se ganarían no por las fuerzas físicas, sino por la disponibilidad y manipulación de la información. Advirtieron sobre

la "guerra cibernética", batallas en las que los piratas informáticos podrían atacar de forma remota las economías y desactivar las capacidades militares. Y también predijeron que la ciberguerra iría acompañada de la "guerra en red", con el significado de intentar interrumpir, deteriorar o transformar la comprensión que la población objetivo tiene sobre sí misma y el mundo que la rodea (Arquilla & Ronfeldt, 1993).

Rusia es el ejemplo más obvio: un gobierno cuyos medios estatales, fábricas de trolls y redes de bots conspiran para librar una guerra de información global. Haciendo eco del lenguaje de los propagandistas de ISIS, los estrategas militares rusos describen cómo una fuerte ofensiva de información puede tener un impacto estratégico similar al lanzamiento de una bomba atómica. Advierten sobre el poder de la información extranjera para difuminar los valores espirituales y morales tradicionales de Rusia y, en cambio, abogan por un sistema de educación espiritual y patriótica y el desarrollo de información, como medidas destinadas a prevenir o reducir la amenaza de acciones destructivas de un estado atacante. En esta línea de razonamiento, el gobierno ruso no recurre a la guerra en red porque quiera, sino porque no ve otra opción. La mejor defensa, después de todo, es una buena ofensiva (Darczewska, 2014).

Por su parte en 2011, la División de Investigación de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), creadora de la propia Internet, lanzó el nuevo programa Social Media in Strategic Communications para estudiar el análisis y la manipulación en línea. Casi al mismo tiempo, el Comando Central del Ejército de los EE.UU. comenzó a supervisar la Operación Earnest Voice, un esfuerzo de varios cientos de millones de dólares para luchar contra los yihadistas en todo Medio Oriente con el objeto de distorsionar las conversaciones árabes de las redes sociales. Una parte de esta iniciativa fue el desarrollo de un servicio de gestión de personas en línea, esencialmente software sockpuppet, "para permitir que una persona de EE.UU. controle hasta 10 identidades separadas en todo el mundo" (Fielding & Cobain, 2011, pág. s/n). Y a partir de 2014, el Departamento de Estado de EE.UU. invirtió grandes cantidades de recursos creando una serie de organizaciones en línea para contrarrestar a ISIS lanzando sus propias ofensivas de información.

Otros casos que demuestran la importancia de la estrategia en línea, son los de: Gran Bretaña, que en 2015 formó la 77º Brigada de 1.500 soldados, destinada a ser un "agente de cambio a través de actividades de información y divulgación específicas"; la alianza de la OTAN lanzó su Centro de Excelencia de Comunicaciones Estratégicas

(STRATCOM), centrado específicamente en la militarización de las redes sociales; el impresionante brazo digital de las FDI, el creciente ejército patriótico de trolls de Turquía, las florecientes redes de bots del gobierno mexicano y las iniciativas de propaganda cibernética de docenas de otros países.

El Centro de Entrenamiento de Preparación Conjunta en Fort Polk ocupa un lugar especial en la historia militar; creado como parte de las maniobras de Luisiana, una serie de ejercicios de entrenamiento masivos que se llevaron a cabo justo antes de que Estados Unidos entrara en la Segunda Guerra Mundial. Desde entonces, ha servido como un laboratorio de campo continuo donde el Ejército de los Estados Unidos se entrena para las batallas del futuro. Después del 11 de septiembre, el sitio de casi 30.000 hectáreas se transformó en la provincia falsa de Kirsham, repleta de aldeas de madera, una fuerza opuesta de insurgentes simulados y decenas de actores que interpretan a civiles atrapados en el medio; todo lo que el ejército pensó que necesitaba para simular cómo la guerra estaba cambiando. Fort Polk cuenta con una innovación para esta tarea: el Social Media Environment and Internet Replication (SMEIR) (Kleeman, 2016).

El SMEIR simula blogs, medios de comunicación y cuentas de redes sociales que se entrelazan para formar un campo de batalla virtual encima del físico. Un equipo de contratistas de defensa y oficiales militares simulan la actividad de Internet de una ciudad pequeña (publicaciones incoherentes, tweets inocuos y la propaganda viral ocasional) desafiando a las tropas que luchan en los juegos de guerra de Kirsham a navegar por el terreno digital. Para los soldados agotados y estresados que esquivan las bombas y balas enemigas, no es suficiente salvaguardar a la población local y luchar contra los malvados insurgentes; ahora deben ser conscientes del flujo y reflujo de la conversación en línea. Este experimento en Polk representa un primer y pequeño paso para abordar un nuevo y enorme desafío operativo (Kleeman, 2016).

Ganar las Redes

La Internet moderna no es solo una red, sino un ecosistema de miles de millones de almas, cada una con sus propios pensamientos y aspiraciones, cada una capaz de imprimir una pequeña parte de sí mismos en el vasto patrimonio digital; ellos no son el objetivo de una sola guerra de información, sino de muchas de ellas. Aquellos que la pueden manipular, para dirigir su dirección y flujo, pueden lograr un bien increíble, pueden liberar a la gente, denunciar delitos, salvar vidas y sembrar reformas de gran

alcance. Pero también pueden lograr un mal asombroso, pueden fomentar la violencia, avivar el odio, sembrar falsedades, incitar guerras e incluso erosionar los pilares de la democracia misma. Quien triunfe depende, en gran parte, de cuánto aprenda el resto a reconocer esta nueva guerra por lo que es.

Para “ganar" Internet, se debe aprender a fusionar los elementos de narrativa, emoción, autenticidad, comunidad e inundación y si puede "ganar" Internet, se pueden ganar simples contiendas, elecciones y guerras por igual. Incluso puede deformar la forma en que las personas se ven a sí mismas y al mundo que las rodea (Gleick, 2012).

La victoria requiere una apreciación de la naturaleza de la viralidad y las formas caprichosas de la economía de la atención, así como un talento para transmitir narrativa, emoción y autenticidad, combinado con la construcción de comunidad y un suministro permanente de contenido (inundación). Y debido a que todo tiene lugar en la Internet abierta, cada uno de estos conflictos se convierte en una disputa global con un número desconocido de jugadores.

El primer paso y más importante es tomar en serio este nuevo campo de batalla. Las redes sociales ahora forman la base de la vida comercial, política y cívica, pero también son un espacio de conflicto de inmensas consecuencias para la seguridad de los ciudadanos, tanto nacionales como individuales. Así como la amenaza de la guerra cibernética fue reconocida y luego organizada y preparada durante las últimas dos décadas, ahora también debe abordarse este nuevo frente.

En 2017, el general Mark Milley, jefe de estado mayor del ejército de los EE.UU., resumió lo que esto significa para los militares: "Por primera vez en la historia de la humanidad, es casi imposible pasar desapercibido" (Singer & Brooking, 2018, pág. 58). En la preparación para el Día “D” en junio de 1944, los aliados acumularon dos millones de soldados y decenas de miles de tanques, cañones, jeeps, camiones y aviones en las Islas Británicas; la inteligencia alemana sabía que las fuerzas aliadas estaban allí, sin embargo nunca supieron dónde o cuándo atacarían, esa información llegó solo cuando los primeros estadounidenses irrumpieron en la Playa de Utah. Hoy en día, la cuenta de Facebook de un solo soldado o civil local es suficiente para revelar toda la táctica, de hecho, incluso su silencio digital puede ser suficiente para delatarlo también.

Vulnerabilidades

Las características anteriormente descriptas, claramente pueden ser clasificadas como oportunidades o riesgos, según las características y capacidades de cada actor; sin embargo el empleo de las redes sociales conlleva riegos debido a las vulnerabilidades propias de las redes sociales, de las redes en general y de Internet como medio. Como ejemplo se pueden mencionar el robo de identidades, de denegación de servicios, el software malicioso.

De la misma manera, un riesgo latente en su empleo, es el factor humano y los errores que pueden afectar la estrategia planificada. El ser humano es parte del sistema y es una vulnerabilidad, las personas cometen errores como operadores o programadores. Una limitación principal de cualquier sistema cibernético es el nivel de confianza que el ser humano tiene en el sistema. Con demasiada confianza, los operadores se vuelven dependientes del sistema y son víctimas cuando falla, ya que no pueden realizar la tarea de una manera diferente. Por el contrario, si el usuario no tiene suficiente confianza en el sistema, pierde los beneficios que puede proporcionar el ciberespacio. Continuando la secuencia de riesgos, una mala planificación de la estrategia para el empleo de las redes sociales, puede derivar en un perjuicio para el logro de los objetivos perseguidos.

Luego de haber identificado las características principales que crean oportunidades y riesgos para llevar a cabo las operaciones de información; analizado las formas en que las redes sociales han creado un nuevo entorno para el conflicto, transformando la velocidad, la difusión y la accesibilidad de la información; y ejemplificado como algunos Estados reconocen la importancia de desarrollar un estrategia en línea, orientando su doctrina y entrenamiento para el conflicto en este ambiente, es que en el siguiente capítulo se describirán como diferentes actores han realizado operaciones de información empleando las redes sociales en los conflictos más recientes y su contribución al logro de los objetivos operacionales.

CAPÍTULO II: EL EMPLEO DE LAS REDES SOCIALES EN LOS CONFLICTOS MODERNOS

Las plataformas de comunicación virtual se han convertido en una parte integral de la estrategia de guerra. Los recientes conflictos han demostrado que las redes sociales se utilizan ampliamente para coordinar acciones, influir sobre el proceso de toma de decisión del adversario, recopilar información y para influir en las creencias y actitudes de las audiencias objetivo, incluso para movilizarlas para la acción (Svetoka, 2016). Las características descriptas en el capítulo anterior, han sido aprovechadas por diferentes actores para que el empleo de las redes sociales contribuya al logro de los objetivos operacionales. En el presente capítulo, se realiza una descripción de cómo dicho empleo en los conflictos modernos han influido con mayor relevancia en el nivel operacional de una campaña.

Caída de Mosul (2014)

En el verano de 2014, combatientes del autoproclamado Estado Islámico (también conocido como ISIS o Daesh en árabe) aparecieron en el norte de Irak, avanzando rápidamente por el desierto. Lejos de mantener su operación en secreto, se aseguraron de que todos lo supieran, realizaron una campaña coreografiada en las redes sociales para promoverlo, organizada por fanáticos y amplificada por un ejército de bots de Twitter. Incluso había una aplicación para teléfonos inteligentes, creada para que los fanáticos yihadistas que seguían en casa pudieran vincular sus cuentas de redes sociales, impulsando aún más los mensajes de los invasores.

Pronto #AllEyesOnISIS había logrado su objetivo en línea y se convirtió en el hashtag de mayor tendencia en Twitter árabe, llenando las pantallas de millones de usuarios, incluidos defensores y residentes de ciudades en la mira del Estado Islámico. Las demandas de los militantes de una rápida rendición se extendieron tanto a nivel regional como personal, jugando con los teléfonos en las manos de sus objetivos; tal como lo describe la autora “los medios sociales no sustituyen a los medios de comunicación tradicionales pero cambian la manera de comunicar. En internet, la comunicación deja de ser masiva para pasar de ser de persona a persona” (Aced, 2013, pág. 76)

Los videos de ISIS también mostraron la espantosa tortura y ejecución de quienes se atrevieron a resistir. ISIS logró su objetivo en el mundo real: #AllEyesOnISIS asumió el poder de un bombardeo invisible, con miles de mensajes en espiral frente a la fuerza que avanzaba. Su detonación sembraría terror, desunión y deserción. El objetivo preciado de ISIS era Mosul, una metrópolis multicultural de 1,8 millones de habitantes de 3.000 años de antigüedad. A medida que la vanguardia de ISIS se acercaba y #AllEyesOnISIS se volvía viral, la ciudad se consumía en el miedo. Los vecinos sunitas, chiítas y kurdos se preguntaban si eran reales las decapitaciones y ejecuciones que se subían a la red en alta definición, y si eso mismo pasaría allí. Entonces, jóvenes sunitas inspirados por las imágenes de la indomable horda negra se lanzaron a actos de terror haciendo el trabajo de los invasores (Barrancos Larráyoz, 2014).

El ejército iraquí que era unas veinte veces superior a ISIS estaba dispuesto a proteger la ciudad de esta pequeña pero temible horda, al menos en teoría. Sin embargo, poco a poco miles de soldados salieron de la ciudad dejando atrás sus armas y vehículos; gran parte de la policía de la ciudad los siguió. Entre los ciudadanos de Mosul, los mismos rumores generaron un pánico masivo y así casi medio millón de civiles huyeron. Cuando la fuerza invasora del ISIS finalmente llegó a las afueras de la ciudad, quedaron asombrados por su buena suerte, solo un puñado de soldados y policías valientes (o confundidos) se quedaron a defender la ciudad. No fue una batalla sino una masacre, debidamente filmada y editada para el próximo ciclo de fácil distribución en línea.

Militantes de ISIS publicaron con alegría imágenes del arsenal que habían capturado, montañas de armas y municiones, y miles de vehículos de última generación fabricados en Estados Unidos que iban desde Humvees hasta tanques de batalla M1A1 Abrams y media docena de Black Helicópteros Hawk. Organizaron desfiles llamativos para celebrar su improbable triunfo. Quienes así lo deseaban podían seguir estos eventos en tiempo real, cambiando entre los puestos de los combatientes de ISIS que marchaban por las calles y los que los veían marchar. Cada punto de vista era diferente, pero todos prometían lo mismo: más, mucho más, por venir (Sisk, 2015).

Lo sucedido era difícil de entender en ese momento, no era solo que ciudades enteras se habían perdido a manos de un ejército heterogéneo de millennials, sino que cuatro divisiones enteras del ejército iraquí, entrenadas y armadas por la nación más

poderosa del mundo, se habían evaporado esencialmente en el aire. ISIS fue pionero en un tipo diferente de guerra relámpago, uno que utilizó Internet como arma. Las mismas camionetas y las armas de segunda mano de innumerables grupos guerrilleros del pasado habían adquirido un nuevo poder cuando se combinaban con el filtro de Instagram correcto, especialmente cuando se compartían cientos de miles de veces por admiradores y cuentas automatizadas. Con una edición cuidadosa, un tiroteo indeciso podría reformularse como una victoria heroica en el campo de batalla. Quienes intentaban contrariar las puestas en escena, no podían probar sus dichos, estos videos e imágenes se movían más rápido que la verdad.

En los meses que siguieron, el impulso de ISIS continuó, el grupo reclutó a más de 30.000 extranjeros de casi un centenar de países para unirse a la lucha en su autoproclamado "califato". La exportación de su mensaje resultó igualmente exitosa. ISIS se diseminó en todas partes, formando filiales desde Libia y Afganistán hasta Nigeria y Bangladesh. Donde éstas no eran posibles, la propaganda de ISIS incitó a "lobos solitarios" a atacar, inspirando decenas de ataques terroristas desde París y Sydney hasta Orlando y San Bernardino (Chulov, Grierson, & Swaine, 2017).

Batalla de Mosul (2016-2017)

Dos años después de que ISIS tomó Mosul, un ejército iraquí reconstituido regresó a Mosul en 2016, esta vez equipado para el nuevo campo de batalla que se extendía mucho más allá de las calles de la ciudad iraquí. Camiones avanzaban pesadamente tras los tanques y los vehículos blindados de transporte de personal, arrastrando torres de teléfonos móviles portátiles para garantizar el ancho de banda para sus propios mensajes. El ejército iraquí emitió un flujo rápido de actualizaciones de Facebook, YouTube y Twitter tanto prácticas (el estado de la operación) como extrañas (selfies sonrientes de soldados iraquíes mientras detonaban los restos de camiones suicidas de ISIS). Naturalmente, la operación tenía su propio hashtag: #FreeMosul (La Información, 2016).

Los aliados militares estadounidenses de los iraquíes también se lanzaron a esta nueva lucha. Así como las fuerzas estadounidenses coordinaron ataques aéreos y datos de objetivos para el ejército iraquí, también buscaron dar forma al flujo de conversaciones en línea en Irak y más allá. Durante meses, los operadores especiales y los oficiales de guerra de información estadounidenses se habían entrenado para el

asalto practicando "maniobras cognitivas" contra los supuestos propagandistas del ISIS. Publicaron mensaje tras mensaje que reflejaba lo que habían aprendido y mientras tanto, cientos de contratistas empleados por el Departamento de Estado de EE.UU. acecharon las conversaciones de posibles reclutas de ISIS, recordándoles la barbarie de ISIS y su inminente derrota (Tucker, 2016).

La multitud en línea no solo miraba lo que ocurría; incluso se involucró de otras formas más positivas. En una inversión de cómo ISIS había explotado por primera vez la tecnología para tomar Mosul, se formó una red global de voluntarios en línea, dedicada a usar las redes sociales para salvar vidas allí. Exploraban las redes en línea en busca de cualquier fragmento de información sobre dónde quedaban civiles atrapados en el fuego cruzado, y llevaban a los rescatistas del hospital local a su ubicación. Un centro para este esfuerzo fue @MosulEye, dirigido por un hombre iraquí que trabajaba detrás de las líneas de ISIS como un nuevo tipo de quinta columna en línea por la paz. Describió este esfuerzo como "un gran cambio poder llegar a aquellos que fueron rescatados y escuchar sus voces, sabiendo que ayudé a rescatarlos y salvarles la vida no tiene precio" (Lynch, 2017, pág. s/n).

En la batalla en Mosul, que fue más extensa y dificultosa de lo previsto, ISIS demostró su capacidad y resiliencia para variar sus tácticas y sus habilidades para reclutar seguidores y organizar atentados y ataques en todo el mundo, más aún cuando su situación en la ciudad iraquí comenzó a verse comprometida. Aun habiendo sido limitada física y digitalmente, nunca dejó de imponer su narrativa proyectando su propia visión de los eventos y preparando a sus seguidores ante una posible derrota militar; con la consigna de que mantener la verdadera fe islámica era más virtuoso que el control del territorio.

Rusia en Ucrania (2014-2016)

Este conflicto ha demostrado la capacidad rusa de utilizar la guerra cibernética y de información para influir en las operaciones para apoyar objetivos militares y políticos, y la preparación continua del entorno cibernético para crear una gama de opciones para acciones futuras (Clapper, 2016). La estrategia de Rusia en éste nuevo entorno fue utilizar la información obtenida de sus campañas de explotación de redes informáticas para influir en el proceso de toma de decisiones, moldear intencionalmente la opinión pública, distorsionar las percepciones internacionales, la comprensión de la

situación para limitar las acciones oportunas y mantener su posición dominante en Ucrania sin interferencia internacional.

Rusia utilizó el acceso global y regional a través del dominio cibernético para dar forma al entorno narrativo y político, bajo tres premisas fundamentales; desarrollando medios de comunicación enfocados interna y externamente con una presencia en línea significativa; usando las redes sociales para garantizar que las narrativas rusas lleguen a la audiencia más amplia posible; y puliendo su contenido en términos de lenguaje y presentación para que suene verdadero en varios entornos culturales (Geers, 2015).

La capacidad rusa de capitalizar los medios tradicionales, Internet y las redes sociales le permitieron dar forma a la narrativa a nivel nacional, regional y mundial. Asimismo, el amplio esfuerzo y las capacidades le posibilitaron controlar el ritmo estratégico y operacional a través de la narrativa, confundiendo la claridad de las percepciones y la comprensión de la situación para otros actores internacionales interesados. La confusión deliberada y la narrativa contraria socavaron la credibilidad del gobierno de Ucrania al tiempo que interrumpieron su capacidad para comunicarse con los partidarios nacionales y la comunidad mundial. Las acciones rusas facilitaron la defensa eficaz del entorno informativo y la configuración para operaciones ofensivas y control reflexivo.

Cabe aclarar que basándose en que un actor realiza el proceso de toma de decisiones fundado en la información que dispone del adversario para tratar de alcanzar los objetivos propios, la doctrina rusa define al control reflexivo como el proceso por el que un actor manipula las motivaciones o fundamentos para la toma de decisiones a otro. Cuando uno de los actores alcanza el control reflexivo de su adversario, puede influir en la precepción que éste tiene del escenario, llevándolo a una situación reactiva e incapaz de determinar las intenciones reales del primero. La desinformación tiene un rol fundamental dentro de éste control reflexivo, y en éste entorno, las redes sociales ofrecen múltiples oportunidades (Martínez Pontijas, 2020).

Para adentrarse en el conflicto, el mismo comenzó cuando en medio de crecientes protestas, el impopular presidente de Ucrania Viktor Yanukovych huyó del país en lo que se conoció como Euromaidan. Como prueba del poder emergente de las redes sociales, el nombre de esta revuelta ucraniana fue tomado de un hashtag de Twitter (combinaba "Europa", por el deseo de los manifestantes de asociarse con

Europa en lugar de Rusia, y "Maidan Nezalezhnosti", la plaza en Kiev donde se iniciaron las manifestaciones). Pero así como los revolucionarios habían usado la nueva forma de Internet para unir y derrocar a su enemigo, Rusia la usó para destrozar a Ucrania, ya que estaba lista para crear un nuevo conjunto de condiciones políticas sobre el terreno y manipular las aspiraciones de los rusos étnicos, empujándolos a declarar su independencia de Ucrania (Stern, 2014).

Ucrania resultó ser un caso de prueba crítico. Los artículos de noticias negativos en ruso sobre Ucrania se duplicaron y luego se triplicaron en número. Los rusos étnicos dentro de Ucrania, que ya estaban nerviosos, pronto se llenaron de resentimiento hacia los activistas que habían derrocado al gobierno que apoyaban. Mientras tanto, comandos rusos se infiltraron en Crimea, reclutando y armando células de separatistas prorrusos, que generaron oleadas de protestas y violencia, seguidos de un creciente caos. (Shevchenko, 2014). El punto de inflexión llegó en la ciudad de Odessa, donde decenas de manifestantes prorrusos, tomaron un gran edificio sindical de la era soviética que pronto se incendió en medio de una lluvia de balas y bombas Molotov. Las oportunidades de espionaje y la estrategia de relaciones públicas rusa se aceleraron.

Rusia aprovechó hábilmente el caos, orquestando una campaña mediática que Ucrania no podía igualar. La red de información Rusia Today RT (2014) publicó detalles sangrientos que eran imposibles de verificar, legiones de trolls sembraron las historias a través de las redes sociales y desplegaron memes de la teoría de la conspiración. Mientras tanto, el gobierno ruso se alimentaba de los mismos titulares que había ordenado que se escribieran. El ministro de Relaciones Exteriores ruso Serguéi Víktorovich Lavrov declaró que, dada la noticia de las atrocidades, ahora era el deber solemne de Rusia no permitir que el fascismo se extienda por Europa y el mundo en general. A medida que pasaba el tiempo, las supuestas atrocidades se volvieron aún más preocupantes. No había nada en forma de prueba, pero no tenía que haberla. No se trataba de ser sincero, sino de justificar una invasión.

En el mundo, nadie sabía qué hacer, Estados Unidos y sus aliados europeos impusieron sanciones y entraron en su máxima alerta militar desde la Guerra Fría, todo por algo que oficialmente no estaba sucediendo. Fue una invasión que no lo fue, un gran conflicto que un lado se negó rotundamente a reconocer que estaba luchando. Rusia había utilizado las redes sociales no solo para avivar el conflicto, sino también para crear algo parecido a un conflicto que deformaba la percepción y la realidad. No fue una

invasión militar tradicional; fue una guerra híbrida en la que los objetivos se lograron incluso antes de que el adversario entendiera lo que estaba pasando, explicó el ex embajador de Estados Unidos en la OTAN, Ivo Daalder (Daalder, 2017). Su homólogo militar, el general Philip Breedlove, entonces comandante supremo aliado de la OTAN, lo denominó como la guerra relámpago de información más asombrosa que hemos visto en la historia de la guerra de información (Vandiver, 2014).

El periodista Patrikarakos se desplazó por las noticias de las redes sociales ucranianas mientras el conflicto se desarrollaba en las afueras de la ciudad. Según sus palabras, entendió que estaba atrapado en dos guerras: una peleada en tierra con tanques y artillería, y una guerra de información librada a través de las redes sociales, y contrariamente a la intuición, importaba más quién ganara la guerra de palabras y narrativas, que quién tenía el armamento más potente. El resultado fue un caos violento, confuso y paralizante, precisamente como pretendía Rusia (Patrikarakos, 2017).

Como resumen de las operaciones rusas en Ucrania, se pueden encontrar tres grandes fases; primero se realizaron operaciones de configuración de información de fase cero; donde mediante la guerra cibernética y de información antes del comienzo de las operaciones de combate terrestre crearon una parálisis estratégica de los actores internacionales y Ucrania, generando tiempo y espacio para que los comandantes rusos del nivel operacional y táctico se apoderaran de un terreno clave, instalen un liderazgo rebelde, creando y promulgando una campaña de información viable para apoyar las operaciones.

En segundo lugar, se realizaron operaciones cibernéticas para interrumpir y negar el mando y control de Ucrania y apoderarse del terreno físico y cibernético clave; las operaciones cibernéticas y de información establecieron las condiciones para que a medida que avanzaba la invasión, la inteligencia rusa y las fuerzas de operaciones especiales crearan efectos entre dominios, mediante la instalación de dispositivos de interceptación de datos y aislaron físicamente la infraestructura de telecomunicaciones e Internet de Ucrania.

Finalmente, mediante la realización de operaciones de ciberespionaje para obtener una ventaja operativa y táctica, y obtener inteligencia valiosa a través del reconocimiento cibernético para proporcionar información sobre la planificación y las operaciones del gobierno, el ejército y las fuerzas del orden de Ucrania (Geers, 2015).

Guerra Civil Siria (2011-Actualidad)

La Primavera Árabe, fue una sucesión de manifestaciones públicas, que se realizaron por el descontento con la falta de democracia y derechos sociales, organizada por la población árabe mediante el uso de las de redes sociales principalmente, y que tuvo sus inicios en Tunes, replicándose en gran parte del mundo árabe, norte de África y Medio Oriente. Las oposiciones a los diferentes regímenes vieron la oportunidad de exigir una mayor libertad y más democracia. Sin embargo, a diferencia de Túnez y Egipto, las protestas en Siria no lograron el derrocamiento del presidente sirio Bashar al-Assad, que estaba preparado para tal contingencia y reprimió violentamente las protestas mientras vigilaba Internet y otras comunicaciones. El país entró en una guerra civil, que también tomó un giro religioso y el conflicto evolucionó aún más hacia una guerra indirecta entre chiítas apoyados por Irán y Líbano, contra sunitas apoyados por Arabia Saudita, Turquía y Qatar.

En esta guerra es donde ISIS saltó a la fama por primera vez, casi todos los grupos rebeldes usaron YouTube para reclutar, recaudar fondos y entrenar. Internet era el escenario preferido para la recaudación de fondos para el terrorismo, por las mismas razones por las que ha demostrado ser tan eficaz para las empresas emergentes, las organizaciones sin fines de lucro y las campañas políticas. No solo permitió un amplio alcance geográfico sino que expandió el círculo de recaudaciones de fondos. Como se explicó en The Economist (2016), este fue uno de los factores claves que alimentaron la Guerra Civil Siria, que al momento ya lleva diez años.

Los combatientes obtuvieron los fondos necesarios aprendiendo a financiar colectivamente su guerra usando Instagram, Facebook y YouTube. A cambio de una idea de cómo fue realmente la guerra, los combatientes pidieron donaciones a través de PayPal. Los recaudadores de fondos también se volvieron creativos a través de lo que se conoció como *yihad financiera,* donde algunos clérigos argumentaron que las contribuciones en línea permitían a los donantes cumplir con sus deberes religiosos de la misma manera que lo harían si hubieran servido en la batalla.

Tan pronto como comenzaron las protestas, el presidente sirio Bashar al-Assad expulsó a los periodistas extranjeros del país para controlar la cobertura de prensa de los eventos. Estas medidas permitieron al gobierno sirio controlar el acceso a Internet, implementar la censura y realizar ciberespionaje. A su vez, el régimen del presidente

sirio Bashar al-Assad utilizó Instagram para proyectar un rostro amigable al mundo, mientras lanzaba gases a sus propios ciudadanos.

En mayo del 2011 se creó el Ejército Electrónico Sirio (SEA) que está activo en las principales plataformas de redes sociales para promover sus acciones y apoyar al gobierno sirio. Grohe (2015) argumenta que el gobierno sirio utiliza el SEA como contra narrativa a las publicaciones en las redes sociales publicadas por actores antigubernamentales. Durante el primer año del conflicto, el SEA creó una página de Facebook de la que las personas pudieron descargar y aprender a usar una herramienta para lanzar ataques DDoS (de denegación de servicios) contra BBC News, Al Jazeera, OrientTV y Al-Arabyia TV. Al comienzo de la guerra, las acciones del grupo consistieron principalmente en el uso de vulnerabilidades del sitio web para desfigurarlo con mensajes e imágenes progubernamentales. Reporteros sin Fronteras sostiene que el gobierno sirio utiliza el SEA como una herramienta de ciberinteligencia (Al-Rawi, 2014).

La guerra en el ciberespacio evolucionó en paralelo al teatro físico pero siempre se mantuvo en una intensidad bastante baja. La mayor parte de las actividades cibernéticas relevantes consistieron en propaganda en las redes sociales, publicidad obtenida a través de la desfiguración de sitios webs y algunas campañas de ciberespionaje. El empleo de las redes sociales se caracterizó por la propaganda en la que intentaba desacreditar a los enemigos, una internacionalización del conflicto a través de actividades realizadas en el ciberespacio por simpatizantes de ambos lados del conflicto y un aumento de la desconfianza entre los miembros de los grupos antigubernamentales objetivo de la suplantación de las cuentas de redes sociales (Nissen, 2014).

Después de 2015, la cantidad de ataques cibernéticos disminuyó hasta desaparecer casi por completo, como consecuencia de la intervención internacional contra ISIS y otros desarrollos que desviaron las prioridades de los numerosos actores del ciberespacio.

Para finalizar, y luego de describir como las características de las redes sociales permiten el empleo de las mismas para contribuir al logro de los objetivos operacionales de una campaña, es que se puede dar paso a desarrollar las conclusiones a las que se han arribado.

CONCLUSIONES

La realización del presente trabajo de investigación sobre las oportunidades y riesgos del empleo de las redes sociales en operaciones militares, fue iniciada con un recorrido por los antecedentes y el estado actual del tema, en los cuales se observan las características de su uso como operaciones de información en apoyo a las operaciones militares cinéticas.

Seguidamente se formuló el interrogantes que diera respuesta a la problemática planteada, siendo ¿Cuáles son las principales oportunidades y riesgos del empleo de las redes sociales en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales?; y posteriormente se planteó el objetivo general para el desarrollo del mismo que consistió en, determinar las principales oportunidades y riesgos del empleo de las redes sociales como operaciones de información en el desarrollo de una campaña, con el fin de contribuir al logro de los objetivos operacionales.

A los fines de dar respuesta a la problemática planteada se desarrollaron dos capítulos; el primero en el cual se identificaron las características principales que crean oportunidades para llevar a cabo las operaciones de información, y se analizaron las formas en que las redes sociales han creado un nuevo entorno para el conflicto, transformando la velocidad, la difusión y la accesibilidad de la información, cambiando la naturaleza misma del secreto, con lo cual se dio cumplimiento al primer objetivo particular. Y el segundo capítulo en el cual se escribieron cómo han sido empleadas las redes sociales en los conflictos modernos de la última década para contribuir al logro de los objetivos operacionales.

Retomando los objetivos establecidos y luego de haber desarrollado el contenido referido, se pueden obtener ciertas conclusiones que contribuyen a comprender mejor las implicancias que tiene el empleo de las redes sociales; por lo que en el primer capítulo se analizaron las formas en que las redes sociales han transformado la velocidad, la difusión y la accesibilidad de la información, creando un nuevo entorno para el conflicto; se describieron las principales características que las mismas tienen y que generan oportunidades para los actores que sepan aprovecharlas, mientras que se pueden convertir en riesgos para aquellos que no cuenten con un estrategia en línea, doctrina y entrenamiento orientado para el conflicto en este ambiente.

Asimismo, también se identificaron vulnerabilidades propias de las redes sociales, como lo son el robo de identidades, la de denegación de servicios, el software malicioso y riesgos latentes como el factor humano y una mala planificación de la estrategia en línea, cumplimentando de ésta forma con el primer objetivo particular propuesto.

Posteriormente, en el segundo capítulo se describieron como diferentes actores emplearon las redes sociales para contribuir al logro de los objetivos operacionales en cuatro conflictos de la última década y que se pueden destacar, como en la Caída de Mosul (2014) ISIS realizó una campaña coreografiada en las redes sociales para promover su operación, organizada por fanáticos, amplificada por un ejército de bots de Twitter y hasta mediante una aplicación para teléfonos inteligentes, en lugar de mantenerla secreto y buscar una ventaja mediante la sorpresa, lo que quizás un ejército regular y tradicional haría.

Volviendo viral el hashtag #AllEyesOnISIS inspirando a jóvenes sunitas a actos de terror y atemorizando a toda la ciudad, incluido el ejército iraquí entrenado y armado por la nación más poderosa del mundo y veinte veces superior a ISIS y fuerzas de seguridad, que junto con cientos de miles de civiles huyeron de la ciudad, dejándola indefensa. Lo que fue aprovechado por las fuerzas de ISIS, para nuevamente realizar una campaña de propaganda de su victoria con la cual lograron reclutar a unos 30.000 extranjeros. En resumen, ISIS empleó las redes sociales para influenciar en la opinión pública y degradar al oponente, lo cual contribuyó al objetivo operacional de tomar la ciudad de Mosul casi sin necesidad de combatir.

Dos años después en la Batalla de Mosul (2016-2017) el ejército de los EE.UU entrenado para el asalto practicando "maniobras cognitivas" junto con un ejército iraquí reconstruido, limitaron física y digitalmente la capacidad de narrativa de ISIS, y aunque la batalla física fue extensa, lograron recuperar la ciudad evitando nuevos reclutamientos, controlando sus conversaciones en las redes, imponiendo el hashtag #FreeMosul y difundiendo la inminente derrota de ISIS.

El siguiente caso de estudio fue el de las operaciones de Rusia en Ucrania (2014-2016), donde la estrategia de Rusia en éste nuevo entorno fue utilizar la información obtenida de sus campañas de explotación de redes informáticas para influir en el proceso de toma de decisiones, moldear intencionalmente la opinión pública, distorsionar las percepciones internacionales, la comprensión de la situación para limitar

las acciones oportunas y mantener su posición dominante en Ucrania sin interferencia internacional.

La capacidad rusa de capitalizar los medios tradicionales, Internet y las redes sociales le permitieron dar forma a la narrativa y a través de ésta, controlar el ritmo estratégico y operacional, confundiendo la claridad de las percepciones y la comprensión de la situación para el resto de los actores, socavar la credibilidad del gobierno de Ucrania, mientras facilitaron la defensa eficaz del entorno informativo, el control reflexivo y la configuración para operaciones ofensivas con fuerzas mínimas para apoderarse de terrenos clave durante las operaciones terrestres.

La sinergia entre dominios lograda en el estudio de caso proporcionó múltiples opciones para el comandante operacional, creando conmoción y retraso en el ciclo de toma de decisiones del enemigo, y permitiendo a los rusos ganar y mantener la iniciativa, lo que obligó a la culminación del nivel operacional del oponente. De esta manera, Rusia logró influenciar en la opinión pública, legitimar las operaciones propias que terminó con la anexión de Crimea a la Federación Rusa, degradar al oponente e influenciar el proceso de toma de decisiones de Ucrania; lo cual representa una mayor libertad de acción para el comandante.

Finalmente, en el último caso de estudio, la Guerra Civil Siria demostró inicialmente la capacidad de las redes sociales para influenciar en la opinión pública y organizar manifestaciones de civiles. Seguidamente ISIS al igual que en Irak las empleó para reclutar, recaudar fondos y entrenar a sus milicias. Por su parte, el régimen del presidente sirio Bashar al-Assad las empleó para mostrar una imagen amigable al mundo y el SEA como propaganda en las redes sociales para desacreditar a los enemigos, una internacionalización del conflicto, desfiguración de sitios webs y campañas de ciberespionaje.

En función de las descripciones efectuadas en el segundo capítulo se da cumplimiento al segundo objetivo particular; y habiendo expuesto las conclusiones, se puede observar el cumplimiento del objetivo general y que la hipótesis planteada ha sido corroborada, finalizando de ésta manera el presente trabajo de investigación.

BIBLIOGRAFÍA

Aced, C. (2013). *Relaciones Públicas 2.0 cómo gestionar la comunicación corporativa en el entorno digital.* Barcelona: Editorial UOC.

Al-Rawi, A. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review* , 420–428.

Anagnostopoulos, A. (2014). *Viral Misinformation: The Role of Homophily and Polarization.* Recuperado el 23 de Agosto de 2021, de ResearchGate: https://www.researchgate.net/publication/268226778_Viral_Misinformation_The_Role_of_Homophily_and_Polarization

Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar Is Coming!* Recuperado el 28 de Agosto de 2021, de RAND Corporation: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

Barrancos Larráyoz, D. (2014). *Los Community Managers del Terror: La propaganda online de ISIS y su ofensiva sobre Irak.* Recuperado el 9 de junio de 2021, de Instituto Español de Estudios Estratégicos: http://www.ieee.es/en/Galerias/fichero/docs_opinion/2014/DIEEEO82bis-2014_ISS_DavidBarrancos.pdf

Bergh, A. (2019). *Social network centric warfare – understanding influence operations in social media.* Oslo: Norwegian Defence Research Establishment (FFI).

Biblioteca Virtual Universal. (2003). *Biblioteca Virtual Universal.* Recuperado el 2 de junio de 2021, de https://biblioteca.org.ar/libros/656228.pdf

Blanco, P. R. (2014). *La estrategia de las redes sociales en Gaza*. Recuperado el 8 de junio de 2021, de El País: https://elpais.com/internacional/2014/08/20/actualidad/1408553372_613519.html

Chulov, M., Grierson, J., & Swaine, J. (2017). *Isis faces exodus of foreign fighters as its 'caliphate' crumbles*. Recuperado el 30 de Agosto de 2021, The Guardian: https://www.theguardian.com/world/2017/apr/26/isis-exodus-foreign-fighters-caliphate-crumbles

Clapper, J. R. (2016). *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community.* Recuperado el 02 de Septiembre de 2021, de OFFICE of the DIRECTOR of NATIONAL INTELLIGENCE: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Clausewitz, C. v. (1976). *On War, ed. and trans. Michael Howard and Peter Paret.* Nueva Jersey: Princeton University Press.

Cordy, J. (2017). *The Social Media Revolution: Political and Security Implications.* Canadá: NATO Commitee on the Civil Dimension of Security.

Cottee, S. (2015). *Por qué es tan difícil detener la propaganda de ISIS*. Recuperado el 16 de Agosto de 2021, de The Atlantic: https://www.theatlantic.com/international/archive/2015/03/why-its-so-hard-to-stop-isis-propaganda/386216/

Daalder, I. H. (2017). *Respondiendo al resurgimiento de Rusia*. Recuperado el 04 de Septiembre de 2021, de Foreign Affairs: https://www.foreignaffairs.com/articles/russia-fsu/2017-10-16/responding-russias-resurgence?cid=int-fls&pgtype=hpg

Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study.* Recuperado el 17 de Agosto de 2021, de Centre for Eastern Studies (OSW): https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

De Vergara, E., & Trama, G. A. (2017). *Operaciones Militares Cibernéticas: Planeamiento y Ejecución en el Nivel Operacional.* Buenos Aires, Argentina: Visión Conjunta.

Fielding, N., & Cobain, I. (2011). *Revealed: US spy operation that manipulates social media*. Recuperado el 12 de Agosto de 2021, de The Guardian: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

Fridman, O. (2013). *The Power of Social Media: Analyzing Challenges and Opportunities for the Future Military Operations.* Londres: University of London.

Geers, K. (2015). *Cyber War in Perspective: Russian Aggression Against Ukraine.* Recuperado el 03 de Septiembre de 2021, de Cooperative Cyber Defence Centre of Excellence OTAN: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Gleick, J. (2012). *The Information: A History, a Theory, a Flood.* Vintage Books.

Grohe, E. (2015). The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict. *Comparative Strategy* , 133-148.

Holmes, J. (2016). *A Trump Surrogate Drops the Mic: 'There's No Such Thing as Facts'*. Recuperado el 27 de Agosto de 2021, de Esquire: https://www.esquire.com/news-politics/videos/a51152/trump-surrogate-no-such-thing-as-facts/

Kleeman, S. (2016). *The US Military's Training Facility for Fighting Online Terrorism Sounds Bonkers*. Recuperado el 24 de Agosto de 2021, de Gizmodo: https://gizmodo.com/the-us-militarys-training-facility-for-fighting-online-1787676732

La Información. (2016). *La ofensiva en Mosul, en directo a través de Facebook Live y Periscope*. Recuperado el 30 de Agosto de 2021, de La Información: https://www.lainformacion.com/mundo/ofensiva-Mosul-Facebook-Live-Periscope_0_963803881.html

Lynch, H. (2017). *Twitter-sourced rescue ops saving civilian lives in Mosul*. Recuperado 30 de Agosto 2021, de Rudaw: www.rudaw.net/english/middleeast/iraq/160320172

Maqueira, J. M., & Bruque, S. (2009). *Marketing 2.0: El nuevo marketing en la web de las redes sociales.* Madrid: Editorial RA-MA.

Martínez Pontijas, J. (2020). *Control reflexivo: mucho más que desinformación a la rusa.* Recuperado el 03 de Septiembre de 2021, de Instituto Español de Estudios Estratégicos: https://dialnet.unirioja.es/servlet/articulo?codigo=7772851

Matejic, N. (2015). *Social Media Rules of Engagement: why your online narrative is the best weapon during a crisis.* Melbourne: Wiley.

Mercy Corps. (2019). *The Weaponization of Social Media: How social media can spark violence and what can be done about it.* Oregon: Mercy Corps.

Moody, C. (2013). *Gaza Goes Viral: An Analysis of Influence – Google Ideas Summit*. Recuperado el 03 de Agosto de 2021, de The GDELT Project: https://blog.gdeltproject.org/gaza-goes-viral-an-analysis-of-influence-google-ideas-summit/

Nissen, T. E. (2016). *Social Media´s Role in Hybrid Strategies.* Bruselas: NATO StratCom COE.

Nissen, T. E. (2014). *Terror.com - IS's Social Media Warfare in Syria and Iraq.* Copenhague: Royal Danish Defence College.

Oliva, A. E. (2020). *El otro lado de las redes sociales.* Recuperado 05 de junio de 2021, de Univ. Veracruzana: https://www.uv.mx/iiesca/files/2021/03/02CA2020-02.pdf

Oneal, S. (2019). *"LikeWar," Social Media is a Cesspool*. Recuperado el 15 de junio de 2021, de Rush To Judgement: https://therushtojudgement.wordpress.com/2019/01/03/likewar-social-media-is-a-cesspool/

Patrikarakos, D. (2017). *War in 140 Characters.* New York: Basic Books.

Pennycook, G., Cannon, T., & Rand, D. G. (2018). *Prior exposure increases perceived accuracy of fake news.* Recuperado el 25 de Agosto de 2021, de SSNR: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958246

Phillips, G. E. (1997). *Information Operations - A New Tool for Peacekeeping.* Kansas, Estados Unidos: School of Advanced Military Studies United States Army Command and General Staff College.

Prier, J. (2017). *The Command of the Trend: Social Media as a Weapon in the Information Age.* Alabama, Estados Unidos: School of Advanced Air and Space Studies, Air University.

RAND Arroyo Center. (2009). *Understanding Commanders' Information Needs for Influence Operations.* Santa Monica: RAND Corporation.

Rodriguez, N. (2019). *Las Redes Sociales como Herramienta de Guerra 3.0*. Recuperado el 18 de Agosto de 2021, de Quixote Globe: https://quixoteglobe.com/es/redes-sociales-como-herramienta-guerra-3-0/

Rusia Today RT. (2014). *La tragedia de Odessa 'fascismo en acción'*. Recuperado el 02 de Septiembre de 2021, de Rusia Today RT: https://www.rt.com/news/157292-lavrov-odessa-ukraine-fascism/

Shevchenko, V. (2014). *¿"Hombrecitos verdes" o "invasores rusos"?* Recuperado el 03 de Septiembre de 2021, de BBC: https://www.bbc.com/news/world-europe-26532154

Singer, P. W., & Brooking, E. T. (2018). *Likewar, The Weaponization of Social Media.* New York: Houghton Mifflin Harcourt Publishing Company.

Sisk, R. (2015). *ISIS Captures Hundreds of US Vehicles and Tanks in Ramadi from Iraqis*. Recuperado el 29 de Agosto de 2021, de Military.com: https://www.military.com/daily-news/2015/05/20/isis-captures-hundreds-of-us-vehicles-and-tanks-in-ramadi-from-i.html

Stern, D. (2014). *La guerra de Twitter: el papel de las redes sociales en los disturbios de Ucrania.* Recuperado el 03 de Septiembre de 2021, de NATIONAL GEOGRAPHIC: https://www.nationalgeographic.com/science/article/140510-ukraine-odessa-russia-kiev-twitter-world

Svetoka, S. (2016). *Social Media as a Tool of Hybrid Warfare.* Latvia: NATO StratCom COE.

The Economist. (2016). *Why an ordinary man went to fight Islamic State*. Recuperado el 02 de Septiembre de 2021, de The Economist: https://www.economist.com/christmas-specials/2016/12/24/why-an-ordinary-man-went-to-fight-islamic-state

Tucker, P. (2016). *How Special Operators Trained for Psychological Warfare Before the Mosul Fight*. Recuperado el 30 de Agosto de 2021, de Defense One: https://www.defenseone.com/technology/2016/11/how-special-operators-trained-Psychological-warfare-mosul-fight/133166/

University, C. M. (2016). *La mayoría de los candidatos presidenciales hablan en el nivel de sexto a octavo grado*. Recuperado el 23 de Agosto de 2021, de Cision PR Newswire: https://www.prnewswire.com/news-releases/most-presidential-candidates-speak-at-grade-6-8-level-300237139.html

Vandiver, J. (2014). *SACEUR: Los aliados deben prepararse para la 'guerra híbrida' de Rusia*. Recuperado el 02 de Septiembre de 2021, de Stars and Stripes: https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464

Vertuli, M., & Loudon, B. (2018). *Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations.* Kansas: Army University Press.