Escuela Superior de Guerra "General Rafael Reyes Prieto"

Estudios en
SEGURIDAD y DEFENSA

estud.segur.def. Bogotá, D. C., Colombia. V. 16 N.° 32 pp. 266. Julio - diciembre de 2021. ISSN 1900-8325 - eISSN 2744-8932

Revista científica *Estudios en Seguridad y Defensa*

Revista colombiana de seguridad y defensa
Bogotá, D.C., Colombia

ISSN: 1900-8325 - eISSN: 2744-8932
esdeguerevistacientifica.edu.co

Lineamientos desde el sector defensa para enfrentar campañas de manipulación social hostil que se gestan en Colombia a través del ciberespacio

Alexander Fraile López
https://orcid.org/0000-0001-5837-8725
frailealim@gmail.com

Luis Velásquez
https://orcid.org/0000-0002-7446-2959
luis.ale.velasquez.hu@gmail.com

Cómo citar

Fraile López, A., & Velásquez, L. (2021). Lineamientos desde el sector defensa para enfrentar campañas de manipulación social hostil que se gestan en Colombia a través del ciberespacio. *Estudios en Seguridad y Defensa, 16*(32), 343-378. https://doi.org/10.25062/1900-8325.321

Publicado en línea
Diciembre de 2021

Para mayor información:
revistacientificaesd@esdegue.edu.co

Para enviar un artículo:

https://esdeguerevistacientifica.edu.co/index.php/estudios/login?source=%2Findex.php%2Festudios%2Fsubmission%2Fwizard

Cómo citar este artículo

Fraile López, A., & Velásquez, L. (2021). Lineamientos desde el sector defensa para enfrentar campañas de manipulación social hostil que se gestan en Colombia a través del ciberespacio. *Estudios en Seguridad y Defensa, 16*(32), 343-378. https://doi.org/10.25062/1900-8325.321

Lineamientos desde el sector defensa para enfrentar campañas de manipulación social hostil que se gestan en Colombia a través del ciberespacio[1]

Guidelines from the Defense Sector to Confront Hostile Social Manipulation Campaigns that are Managed in Colombia through Cyberspace

Diretrizes do setor de defesa para enfrentar as campanhas hostis de manipulação social que são administradas na Colômbia por meio do ciberespaço

ALEXANDER FRAILE LÓPEZ[2]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

LUIS VELÁSQUEZ[3]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Fecha de recepción

27 de octubre de 2021

Fecha de aceptación

2 de noviembre de 2021

Palabras clave

Ciberespacio, Redes sociales, Desinformación, Campañas de manipulación, Internet, Cuarta Revolución Industrial.

Keywords

Cyberspace, Social Networks, Disinformation, Manipulation Campaigns, Internet, Fourth Industrial Revolution.

Palabras-chave

Ciberespaço, Redes sociais, Desinformação, Campanhas de manipulação, Internet, Quarta Revolução Industrial.

Resumen

El impacto de internet en la sociedad, el surgimiento de tecnologías y desarrollos característicos de la Cuarta Revolución Industrial, la vigencia de diversas formas de influencia o desinformación, y la manifestación del ciberespacio como escenario predominante y transversal para la guerra constituyen una agrupación de elementos y métodos que

1. Artículo de investigación de reflexión vinculado al proyecto de Investigación titulado "Consideraciones de ciberseguridad y ciberdefensa de cara a los retos que impone el siglo XXI", vinculado al grupo de investigación Masa Crítica, categorizado en B COL0123247, inscrito en MinCiencias y adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.
2. Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Especialista en Política y Estrategia Marítima y Profesional en Ciencias Navales de la Escuela Naval "Almirante Padilla". Administrador de Empresas de la Universidad Militar Nueva Granada. Contacto: frailealim@gmail.com
3. Candidato a doctor y magíster en Ciberseguridad en la Universidad Tecnológica de Tallin. Ingeniero naval electrónico de la Escuela Naval de Cadetes "Almirante Padilla". Especialista en Estrategia Marítima y Política. Contacto: luis.ale.velasquez.hu@gmail.com

han sido aprovechados para afectar la estabilidad política, económica y social de las naciones e, incluso, su imagen internacional. Mediante un desarrollo investigativo con enfoque cualitativo, se evidenció la práctica de *manipulación social hostil* sobre tres objetivos: el estudio de casos en los ámbitos nacional e internacional; la identificación de técnicas y modalidades practicadas en dichos casos, y la determinación de lineamentos para contrarrestar ese tipo de campañas. Se obtuvieron como resultados: la efectividad de su implementación, los enormes retos que debe enfrentar Colombia ante un desafío de tal magnitud y la necesidad de tomar medidas oportunas con el fin de mitigar el impacto negativo en la nación.

Abstract

The impact of the internet on the society, the emergence of new technologies and the development of the Fourth Industrial Revolution, added to the validity of various forms of influence related with disinformation, and the cyberspace as the predominant and transversal scenario for war. Settled up a group of elements and methods that have been used to affect the country's political, economic and social stability. In this sense, through a research development from a qualitative approach, the practice of Hostile Social Manipulation was evidenced based on three objectives explained as follows: First, the study cases at national and international level comparing the Colombian scenario in front of external examples. Secondly, the identification of techniques and modalities practiced in those countries related with disinformation. Finally, the determination of guidelines to counteract and control this type of campaigns and environments that affect significantly the security and stability at studied countries. Obtaining as results the effectiveness of its implementation, the enormous challenges that Colombia must face on and the necessity of take timely measures in order to mitigate the negative impact of the disinformation and the manipulation campaigns.

Resumo

O impacto da internet na sociedade, o surgimento de tecnologias e desenvolvimentos característicos da Quarta Revolução Industrial, a validade de várias formas de influência ou desinformação e a manifestação do ciberespaço como cenário predominante e transversal de guerra, constituem um conjunto de elementos. e métodos que têm sido usados para afetar a estabilidade política, econômica e social das nações, afetando até mesmo sua imagem internacional. Por

meio de um desenvolvimento investigativo com abordagem qualitativa, a prática da Manipulação Social Hostil foi evidenciada em três objetivos, o estudo de casos em nível nacional e internacional, a identificação das técnicas e modalidades praticadas nos mesmos e a determinação de diretrizes para contrariar este tipo de campanhas. Obter como resultados a eficácia de sua implementação, os enormes desafios que a Colômbia deve enfrentar diante de um desafio de tal magnitude, e a necessidade de tomar medidas oportunas para mitigar os impactos negativos sobre a nação.

Introducción

La era tecnológica del siglo XXI puede ser considerada la consecuencia de la masificación del internet desde 1990, cuando se desarrollaron nuevas formas de comunicación y acceso a la información (Rodríguez, 2017). Como resultado de los constantes cambios estructurales mediante su uso frecuente y trascendental, como lo mencionan Castells (2002) y Rodríguez (2019), el ciberespacio se ha convertido en el dominio de interacción de la sociedad.

Eissa et al. (2012) y Rivolta (2012) reivindican el ciberespacio como el quinto dominio de la guerra, donde se refleja una dinámica de expansión y crecimiento acelerado, que potencializa el uso de las redes sociales como la columna vertebral de la comunicación y fuente fundamental de consulta, y que implica el intercambio permanente de datos de carácter público y forma un escenario de alto riesgo en la seguridad nacional (Blanco, 2016). La privacidad es otra variable afectada, debido al contexto en el cual se encuentra inmerso el conjunto de recursos utilizados para causar efectos adversos en la población, a través de actores que reconocen plenamente su potencial incorporando prácticas, técnicas y estrategias, que podrían catalogarse como amenazas (Torres, 2017).

Dada esta necesidad constante de mantenerse informado en tiempo real (Arjona, 2020), el ciberespacio propicia el escenario adecuado para que personas o grupos especializados suban inescrupulosamente a las diferentes redes sociales contenidos que no son reales o están fuera de contexto, y así tergiversan la realidad y polarizan la sociedad, para afianzar o desarrollar una postura ideológica determinada que satisfaga intereses particulares (Badillo, 2019).

Como efecto de la desinformación y de la migración a un ambiente digital en los últimos años, se han incrementado la capacitación, la planeación y la ejecución de operaciones de inteligencia y monitoreo en ciberseguridad y ciberdefensa por parte de las Fuerzas Militares (FF. MM.) hacia las redes sociales, los sistemas electorales, las infraestructuras nacionales críticas, etc., procurando contrarrestar, evitar y eliminar los riesgos asociados a los que puede verse expuesta la nación por causa de diversas formas de influencia constituidas en el pasado (Bigelow, 2019).

La configuración de estas actividades y estos modos de influir podrían categorizarse como una *ciberagresión*, en la cual se involucra una gran variedad de campañas y técnicas, denominadas *manipulación social hostil* (MSH), práctica emergente que manifiesta una versión renovada de diferentes formas de influencia, mediante las cuales se busca generar y difundir información, intencional y sistemáticamente, a fin de obtener una ventaja competitiva que desencadene consecuencias sociales, políticas y económicas perjudiciales para un Estado, por medio de la afectación de opiniones, actitudes y conductas (Mazarr, Bauer et al., 2019).

De esta manera, se conforma un escenario con un entorno avanzado de información, en el cual el sistema agresor busca no atacar físicamente al Estado, sino desestabilizarlo; por tanto, son más eficientes los ataques a las creencias sobre un gobierno y a la capacidad de la población para distinguir entre la realidad y el engaño, a la hora de generar riesgos con una connotación significativa, así como respuestas oportunas para reducir el impacto que ello podría tener si se combina con otras tecnologías, cuyos resultados amenazan las democracias abiertas, lo cual es de gran relevancia en la competencia estratégica global (Mazarr, Casey et al., 2019).

Con lo anterior, se manifiesta una amenaza a la estabilidad de un Estado en su naturaleza política, económica, social e internacional, y se plantea como tesis central *la necesidad de establecer los lineamientos que permitan prevenir, identificar y contrarrestar campañas de MSH que afecten la integridad de Colombia a través de las redes sociales, y que sirvan de elemento orientador e integrador de las diferentes capacidades e instituciones estatales para tomar decisiones que coadyuven con la mitigación del riesgo y sus posibles consecuencias para la seguridad y defensa nacional*.

En este orden de ideas, se planteó la pregunta de investigación: *¿Cómo contrarrestar las campañas de MSH que se gestan a través de las redes sociales en Colombia?* Mediante un análisis comparativo de dos casos internacionales: las elecciones presidenciales de 2016 en Estados Unidos (EE. UU.) y el papel de Cambridge Analytica (CA), en el caso de las manifestaciones violentas 2019-2021 en todo el territorio nacional, se identificaron métodos relacionados con operaciones de información y MSH, y se propusieron líneas de acción para contrarrestarlos.

Metodología

El planteamiento y el desarrollo investigativo para lograr los objetivos planteados partieron del enfoque cualitativo, aplicando el método de recolección y análisis de datos para afinar las preguntas de investigación, aprobar o rechazar hipótesis planteadas a partir de un entorno específico y revelar resultados que permitiesen la generación de nuevo conocimiento que coadyuve con el proceso de toma de decisiones (Hernández et al., 2014).

Por lo anterior, se consideró que el método elegido sería el más apropiado, por las características de la investigación relacionadas con la MSH, pues permite abordar objetivamente el problema, con un margen de flexibilidad para la comprensión del fenómeno en función del diagnóstico de los eventos nacionales e internacionales.

Ahora bien, siguiendo los planteamientos de Hernández et al. (2014), para el presente estudio ni la muestra ni su tamaño son relevantes, en la medida que, al buscar los resultados, el objeto no es generalizar en los diferentes casos observados, sino estructurar un análisis particular que permita dar solución a los interrogantes generados y proponer alternativas que se ajusten a las circunstancias y los contextos.

Asimismo ocurre con el instrumento de investigación determinado para recolectar los datos que permiten obtener información para dar validez es el análisis de documentación. Este implica la compilación de estudios relacionados con el tema involucrando la observación y el estudio de casos que relacionen prácticas de MSH, noticias falsas, desinformación social y el uso del ciberespacio y las redes sociales, y fundamentándose en la revisión de literatura académica disponible en metabuscadores, documentos publicados en revistas indexadas, libros y reportes generados por parte de diversas instituciones (Instituto Colombiano para la Evaluación de la Educación [ICFES], 1996), y la mayoría de ellos, en idioma inglés.

Por lo planteado, la orientación de la investigación fue en tres fases. La primera abordó la exploración literaria de acontecimientos internacionales y nacionales, con el objeto de analizar e identificar prácticas de MSH en Estados o eventos relevantes, y enmarcar de esta manera los conceptos para la descripción del fenómeno. En la segunda se efectuaron el análisis y la comparación de los casos sobre la base de las técnicas o los métodos para comprobar y obtener insumos como patrones de comportamiento que orienten la última etapa, consistente, a su vez, en determinar, partiendo de los resultados derivados, las conclusiones y las soluciones que puedan aplicarse al caso colombiano.

Estudio de casos de manipulación social hostil

El desarrollo del objetivo se observó con un marco teórico bajo el concepto de la *seguridad multidimensional*, mediante el que se establecen la presencia y la diversificación de desafíos a la seguridad que implican un cambio en la perspectiva tradicional, para abarcar amenazas contemporáneas que involucran aspectos que requieren múltiples respuestas desde diferentes sectores (organizaciones, gobiernos, sector privado, sociedad civil), de manera adecuada y conforme a las leyes de cada Estado (Mejías & De Sousa, 2015). Propuesto en 2003 por la Organización de Estados Americanos (OEA), el mencionado concepto evidencia que existen nuevas amenazas sociales relacionadas con problemas contemporáneos, y abre el panorama hacia otras dimensiones; específicamente, las concernientes a la implementación de tecnologías emergentes.

Las redes sociales y los medios de comunicación masiva inciden en la comprensión y la percepción de las personas bajo dicho enfoque, dentro de un escenario donde no existen actividades políticamente inertes o neutrales, sino que todas están matizadas por intereses, valores e ideologías; por lo tanto, la propagación de una conciencia social puede surgir naturalmente o puede ser inducida. La era de la información, la inteligencia colectiva, la sociedad red, las nuevas tecnologías, la posverdad, la arqueología de los saberes y los nativos digitales, entre otros, son condiciones propias en un ámbito de gran conflictividad que enfrentamos a diario. Su entendimiento permite advertir el potencial peligro que se genera en una institución militar si no se toman medidas para afrontarlo, pero también, la variedad de oportunidades para cumplir con su misión (Rivolta, 2012).

Un ejemplo de cómo asumir estos retos es la Organización del Tratado Atlántico Norte (OTAN), que desde el final de la Guerra Fría (1948-1991) ha ampliado su alcance no solo en términos de integrantes y socios, sino también, en su forma de operar. Como coalición comprometida a escala mundial, se prepara permanentemente para abordar las amenazas cibernéticas donde la verdadera integración de las operaciones requiere una amplia educación de los miembros sobre estas, planificación operativa cibernética y entrenamiento para crear memoria muscular y evaluar rigurosamente las lecciones aprendidas (Ablon et al., 2019).

Adicionalmente, en esta dinámica se incluye la tendencia de las nuevas tecnologías, la Cuarta Revolución Industrial y la evolución de amenazas emergentes en el ciberespacio, que implican para la estrategia de ciberdefensa de la nación partir de una valoración de fortalezas y debilidades observadas en las diferentes instituciones y sectores, y abarcando ámbitos doctrinales, organizacionales, sobre recursos, de talento humano, de infraestructura y demás, que proporcionen elementos determinantes de la condición actual para poder trabajar en objetivos y visiones a corto, mediano y largo plazo (Realpe & Cano, 2020).

De igual forma, la ciberdefensa nacional debe abordarse mediante perspectivas holísticas, en armonía con los dominios aéreo, marítimo, terrestre y espacial de la guerra, de modo que puedan velar y proteger los intereses nacionales como consecuencia de expandirse en un conflicto multidimensional más allá de los escenarios físicos, como son la información, el cognitivo y el social, y llegar a trascender en una *guerra de quinta generación* (G5G) (Álvarez et al., 2017).

Estudio de caso internacional

Para este aparte, se tomó como ejemplo el hito marcado por las elecciones presidenciales de EE. UU. en 2016, CA y la posible intervención de Rusia, en cuanto al análisis metodológico de información personal utilizada para generar estrategias electorales, lo cual tiene un peso estratégico y preponderante por su vínculo en otros escenarios; para ser más específicos, los resultados del referéndum sobre la permanencia del Reino Unido en la Unión Europea, el 23 de junio de 2016 (Brexit).

La campaña de Donald Trump en 2016 se vio acompañada por técnicas y operaciones de influencia que tenían matices evidentes de MSH. Algunas de ellas fueron como se detalla a continuación.

Proyecto Álamo

Según la agencia de *marketing* digital Semantiko, el mencionado proyecto consistió en una base de datos personalizada con información de aproximadamente 220 millones de estadounidenses, y que contenía referencias de historiales de compras, perfiles psicológicos, registros de votantes y propietarios de armas. Fue una campaña de gran magnitud, centrada en la generación de noticias falsas, la recuperación de datos de CA y diversas acciones que buscaban la abstención del voto por parte de sectores de interés para Hillary Clinton.

La estrategia iba dirigida a tres grupos fundamentales: a liberales blancos idealistas, a mujeres jóvenes y a afroamericanos. Álamo empleó la información para desarrollar diversas líneas de acción: una fue *deterrence*, en la que utilizó 3,5 millones de usuarios en Facebook mediante *bots* donde se tenían datos de perfiles grupales ordenados por procedencia étnica, género y distrito de origen de comunidades inmigrantes provenientes de África, Suramérica y Asia (Lindholm, 2017).

Mediante la difusión de información falsa a través de *bots* automatizados, se afirmaba que los inmigrantes no saldrían a votar, lo cual creó una tendencia entre usuarios de los distritos donde la población es mayoritariamente inmigrante, con el fin de hacer que se abstuvieran de elegir la oposición o motivar su voto por Trump (Timberg & Stanley-Becker, 2020).

Por otra parte, de acuerdo con Winston (2017), estuvo *superpredator*, término acuñado por Hillary Clinton en 1996, y con el cual consideraba a los jóvenes inmigrantes de bajos recursos sin empatía ni conciencia, dispuestos a matar por obtener drogas, dinero fácil o ilícito. Trump retomó el vocablo en su campaña para crear una animación de Clinton utilizando un fragmento del audio original (C-SPAN, 2016) resaltando en un texto de dibujos animados: *Hillary piensa que los afroamericanos son superdepredadores*.

Facebook entregó este tipo de publicación a cierta población votante afroamericana, mediante mensajes privados. Finalmente, Brad Parscale, director de la campaña digital para Trump y creador del Proyecto Álamo, manifestó a *Wired* que Facebook y Twitter fueron las razones por las cuales dicho candidato había sido elegido (Lindholm, 2017).

La producción de contenidos con mensajes peyorativos, falsas noticias, difamación o generación de narrativas elaboradas para generar odio o rechazo contra Clinton en redes sociales, mediante un discurso de hace más de 20 años, fue una herramienta útil para aumentar el racismo, polarizar a la sociedad y disminuir el número de personas que votarían por ella.

Cambridge Analytica

Contratada por la campaña de Trump en junio de 2016, esta compañía privada analizaba datos e información en temas de seguridad, así como servicios de consultoría, a gobiernos de diferentes naciones (Seadle, 2020). Se especializaba en una metodología denominada *perfilamiento psicográfico*, mediante la cual, a través de datos recopilados en línea, se predecían perfiles de personalidad o psicológicos sobre la población votante, que era clasificada de acuerdo con su comportamiento o su orientación, y hacia donde se elaboraban contenidos digitales específicos que buscaban influir en la decisión al momento de votar (Illing, 2018).

En julio de 2019, la Comisión Federal de Comercio de Estados Unidos ordenó a Facebook pagar una multa de 5000 millones de dólares por compartir irregularmente 87 millones de datos con CA; asimismo, y de acuerdo con el testimonio de un exempleado de dicha firma, se recolectó —al parecer, sin autorización— información de 50 millones de usuarios, y esta habría sido utilizada para modelar técnicas de influencia hacia la población votante en EE. UU. y el referendo del Brexit, en Reino Unido, en 2016 (*BBC News Mundo*, 2019).

Diferentes expertos en el tema relacionaron otro tipo de técnicas utilizadas en este caso. Según Samuel Woolley, director del Proyecto Propaganda Computacional en 2018, la cantidad de información difundida durante los comicios a favor de Trump y publicaciones anti-Hillary por medio de *bots* fue desmedida: llegó, incluso, a una proporción de cinco a uno (Oxford Internet Institute, 2021). Adicionalmente, Woolley expresó en CNN News que Rusia utilizó Twitter como arma para influir en las elecciones (*CNN Video*, 2017).

Martin Moore, director del Centro de Estudios de Medios, Comunicación y Poder (King's College), expresó a *The Guardian* que para la campaña de Donald Trump se usaron entre 40.000 y 50.000 variedades de publicaciones diarias, las cuales constantemente evaluaban respuestas, se adaptaban y luego variaban,

dependiendo de dicha respuesta; los anuncios se difundieron principalmente a través de bots, y aquellos que más obtuvieron "me gusta" se compartieron y se retuitearon; se los reprodujo y se los redistribuyó en función de dónde eran populares y a quién apelaban (Cadwalladr, 2016).

Los análisis de CA también se utilizaron en tiempo real: al determinar dónde repercutían los mensajes, se acomodaba, en consecuencia, el plan de viajes de Trump; por consiguiente, al detectar tendencias sobre cualquier publicación en algún lugar de interés para el candidato, este se dirigía allí, y reforzaba en su discurso tal contenido (Illing, 2018).

En tercera instancia, se identificó, por parte de autoridades estadounidenses, la posible interferencia y la posible manipulación del gobierno de Rusia, a través de varios ciberataques, a la cuenta de correo personal de Hillary Clinton y la sede demócrata de EE. UU. Los datos hurtados fueron publicados por la organización WikiLeaks[4], y correspondían parcialmente a correos filtrados desde 2009, cuando la rival demócrata era secretaria de Estado, en tiempos de la administración de Barack Obama (Bassets, 2016).

La comunidad de inteligencia de EE. UU. concluyó que el gobierno ruso buscaba quebrantar la legitimidad del proceso democrático, menoscabar a la candidata y afectar su favorabilidad mediante una operación de influencia que habría ido más allá de un ciberataque, e incluido desinformación y propagación de comunicaciones falsas por medio de redes sociales. *Diferentes empresas de seguridad informática declararon que los ataques cibernéticos fueron cometidos por los grupos rusos de inteligencia Fancy Bear y Cozy Bear* (Sánchez, 2019).

Estudio de caso colombiano

A finales de 2019, Colombia vivió un *estallido social* (Farinetti, 2002), el cual, por su naturaleza y a partir de la identificación de prácticas de MSH, se materializó con más fuerza y prolongación el 28 de abril de 2021.

En este entorno, existe un ecosistema de desinformación y propaganda, conformado por una suma de canales y plataformas de comunicación, *proxy* y no atribuidos, para crear y amplificar narrativas falsas sobre diversos objetivos (Departamento de Estado de los Estados Unidos, 2020), y donde el ciberespacio se convierte en otro escenario de incitación para cometer acciones violentas y

4 WikiLeaks es una organización internacional islandesa que trabaja publicando información clasificada de fuentes anónimas.

causar inestabilidad en el Estado, todo lo cual resalta su importancia como escenario de conflicto de las G5G, relacionada con dicho entorno.

A continuación se relacionan algunos elementos identificados durante la última versión del *Paro Nacional* (2021).

Cadenas y medios de comunicación

Se ha apreciado cómo cadenas internacionales que cuentan con espacios en español, conformados por plataformas digitales, publican informes respecto a la crisis política, social y económica que vive Colombia: por ejemplo, Russia Today (RT), que, según la revista *Semana*, es financiada por el gobierno ruso con un presupuesto que supera los 500 millones de dólares, genera contenido en distintos idiomas, se encuentra registrada dentro de los activos estratégicos de Rusia y está vinculada a la organización estatal ante el Ministerio de Justicia. De igual forma, medios como CBS News y *The New York Times*, la califican como un arma para transmitir noticias falsas (Semana, 2020).

Mediante un seguimiento de contenidos relacionados con el paro nacional, transmitidos por RT, saltó a la vista la tendencia polarizada de noticias en contra del Gobierno nacional o de instituciones de Colombia: se apreció que en ninguna emisión hubo declaraciones de alguno de sus funcionarios. De igual modo, se identificó que diferentes cadenas internacionales actuaron similarmente, fomentando desaprobación o percepciones desfavorables, como se muestra en la tabla 1.

Televisoras internacionales como Deutsche Welle (DW), France 24, BBC Mundo y TeleSURtv hicieron un seguimiento detallado al paro nacional colombiano, donde se identificó que a través de corresponsales en el país, el análisis de medios de comunicación nacionales y la publicación casi permanente de contenidos, también se hicieron acercamientos polarizados de la realidad frente a esta situación: fueron apreciables publicaciones sobre abusos y exceso en el uso de la fuerza, la respuesta agresiva del Gobierno nacional en contra de los manifestantes, la desaparición de jóvenes por enfrentamientos o acciones de la Fuerza Pública, o declaraciones en las que ciudadanos aseguran tener miedo a ser asesinados por el Estado (*BBC News Mundo*, 2021).

Tabla 1. Análisis publicaciones RT durante el paro nacional colombiano

Hecho	RT	Otros medios
25/05/2021 Migración Colombia negó el ingreso a Colombia del argentino Juan Grabois, miembro de una misión humanitaria de DD. HH., cuyo propósito era verificar las circunstancias de violación de DD. HH. en el marco del paro nacional, por negarse a una verificación de documentación e irrespetar autoridades migratorias (El tiempo, 2021).	Emitió una declaración de dicho ciudadano aseverando que la deportación era un acto de intimidación y que la decisión tomada por los funcionarios era política, lo cual, también se pudo apreciar junto con una publicación en la cuenta de Twitter @JuanGrabois del 25 de mayo acompañado de los hashtags #SOSColombia y #SOSColombiaDDHH (Grabois, 2021).	Junto con el hecho como estaban las declaraciones emitidas por Migración Colombia que, mediante un comunicado describió lo ocurrido resaltando que, de los 20 miembros de la misión, 19 pasaron los controles del país sin ningún problema. Radio Nacional de Colombia (2021), Semana (2021), Wradio (2021), La Nación (2021), (Migración Colombia, 2021).
26/052021 Declaraciones de funcionarios públicos colombianos han de los hechos de violencia que vive Colombia por cuenta del paro nacional.	RT en español publicó declaraciones del representante a la Cámara Inti Raúl Asprilla Reyes, quien manifestó la gravedad de la violación a los DD. HH. Que se vive en Colombia durante el paro, asegurando que los órganos que están llamados a garantizarlos son cooptados por el Gobierno nacional, denunciando la falta de garantías para investigar estas irregularidades y asegurando que se está ocultando la verdad a la comunidad internacional.	No se identificaron declaraciones similares en otros medios.
30/05/2021 Para el 30 de mayo está programada la denominada Marcha del Silencio, marcha pacífica convocando el fin de la violencia desencadenada en el paro nacional por parte de ciudadanos que rechazaban los actos exagerados de intimidación y el ataque contra los bienes públicos y privados.	Entrevista realizada el 26 de mayo por RT en español a la concejal De Cali Ana Erazo Ruiz, quien manifestó que dicha manifestación era integrada por grupos elitistas afines del Gobierno de Colombia y que no se solidarizaba con la expresión de rechazo del pueblo colombiano.	La Marcha del Silencio, en la cual los participantes demostrarán su rechazo ante los actos de violencia y los bloqueos en las vías durante el paro nacional, que han generado graves afectaciones al comercio y a los ciudadanos. Asimismo, la movilización busca apoyar la labor de la institucionalidad y la Fuerza Pública del país, que ha tenido que intervenir en varias alteraciones del orden público en las regiones del país.

Hecho	RT	Otros medios
05/06/2021 Presuntos miembros de dicha comitiva se habrían reunido con organizaciones sindicales y de Derechos Humanos en Colombia haciendo campañas para derrocar al Gobierno de Colombia (Wradio, 2021b).	No se pronunció ante el hecho.	Plataformas de comunicación como Infobae (2021) y Todo Noticias (2021) de Argentina titularon esta noticia en sus medios digitales.

Fuente: elaboración propia, a partir redes sociales.

Masificación de contenidos y narrativas

La masificación de este tipo de mensajes a través de organismos o individuos, como activistas, influenciadores, organizaciones no gubernamentales (ONG) o personalidades famosas, que atraen, convencen o simpatizan con las causas que promovía el paro nacional, agitó los sentimientos de manifestación, lo que en varias ocasiones llegó a los extremos de la destrucción, el vandalismo, la violación de la ley y la desacreditación y el irrespeto en contra de las autoridades.

Tabla 2. Resultados de *hashtags* con mayor tendencia en redes sociales

Hashtags identificados	Hashtags identificados
1.#AhíLesVA 2.#ColombiaAlertaRoja	11. #FuerzaColombia
3. #ColombiansAreDying	12. #Inna
4. #colombiaresisteunida	13. #noalareformatributaria
5. #ColombiaSeRespeta 6. #CORTEDEFRANELA	14. #Nosestánmatando
7. #CrimenesDeEstado	15. #Paronacional
8. #CrimesAgainstHumanity	16. #ParoNacional28J
9. #DondeEstanLosDesaparecidos 10. #ElParoNoPara	17. #ParonacionalterrorenColombia

Hashtags identificados	Hashtags identificados
18. #PoliciaAsesina	22. #SOSColombiaEnDictadura
19. #porunavidadigna	23. #SOSPrimeraLínea
20. #SOSColombia	24. #TerrorismoDeEstado
21. #SOSColombiaDDHH	25. #vivaelparonacional

Fuente: elaboración propia, con base en redes sociales.

Se realizó la búsqueda de *hashtags* que se muestra en la tabla 2, y a raíz de lo cual se identificaron narrativas motivando la continuación de las manifestaciones, el reclamo de exigencias a través de las protestas, la desacreditación de declaraciones hechas por las autoridades y el apoyo de personas o influenciadores que manifestaban su preocupación ante lo que percibían como el atropello del Estado contra la población, así como presuntos excesos de la Fuerza y la violación a los Derechos Humanos (DD. HH.).

De igual forma, se reconocieron conductas que indicarían la articulación de la población como mecanismo de defensa ante las presuntas agresiones o choques con la Policía. Con la evolución del paro, surgieron grupos particulares, activistas y organizaciones de DD. HH. portando indumentaria para proteger su integridad (cascos, máscaras antigases, artefactos explosivos artesanales), y material técnico para registrar fílmicamente los acontecimientos que se generaban durante enfrentamientos con la Fuerza Pública.

Uno de estas agrupaciones fue la *Primera Línea*, un grupo de jóvenes organizado con el objetivo de salvaguardar a los manifestantes de la agresión por parte de la Policía (Deutsche Welle, 2021a), y que recibió apoyo, entre otros, de particulares y figuras públicas como el senador Gustavo Bolívar, quien en su cuenta de Twitter publicó (24/05/2021) la creación de una colecta liderada por la Fundación Manos Limpias Indignados Colombia, con el objeto de dotar a sus integrantes con elementos para proteger sus vidas de la supuesta brutalidad policial.

Al revisar el enlace para aportar con la donación, contenido en el mensaje del senador (https://vaki.co/es/vaki/YGcg5qW7N03Q69mvgy3I?utm_source=twitter&utm_medium=vaker&utm_campaign=v4), en Vaki.co, se pudo identificar el uso de una plataforma de financiamiento colectivo, una colecta en línea para el recaudamiento de fondos (ConnectAmericas, s. f.). El 9 de junio de 2021 se cerró la recaudación para #SOSPrimeralínea con una recepción de 332.000.000 de pesos.

Cabe resaltar que para el estallido social de Chile, en 2019, se organizaron grupos de jóvenes autodenominados Primera Línea y proclamando los mimos objetivos: *la defensa de los manifestantes frente a la violencia policial* (Droguett, 2019). En Colombia se tuvo conocimiento de la vinculación de estos grupos en actividades delincuenciales, fabricación de artefactos explosivos artesanales y vandalismo.

Ciberataques

Dentro del contexto generado por la pandemia y lo que significa 2021 para las elecciones presidenciales de 2022, se demostró el incremento de agresiones cibernéticas, estimadas en más de mil millones de intentos durante el primer trimestre en Colombia, y un total de siete mil millones en América Latina, tal como lo indicó la firma especialista en soluciones de ciberseguridad Fortinet (*El Colombiano*, 2021).

El grupo hacktivista Anonymous se atribuyó el ataque a la página web del Ejército de Colombia, realizado el 4 de mayo de 2021; la publicación en Twitter de contraseñas y correos de 168 funcionarios de la institución, como respaldo a las manifestaciones y rechazo a las víctimas durante el paro, y la alteración del sitio web en Wikipedia (Deutsche Welle, 2021b).

Asimismo, fue atacada la página web de la Presidencia de la República y, presuntamente, se hackearon las comunicaciones de la Policía Nacional; también fueron divulgados datos personales de miembros de las FF. MM. y del partido político Centro Democrático, lo cual generó serias implicaciones de seguridad, por amenazas recibidas a través de WhatsApp, situación que fue denunciada por los senadores Miguel Uribe y Paloma Valencia (@PalomaValencia, 5 de junio 2021).

Dentro de los resultados, se pudo determinar que la información fue obtenida por medio de ataques de *denegación de servicios distribuida* (DDoS), los cuales generaron indisponibilidad de las páginas agredidas por saturación; de igual forma, los datos divulgados de los diferentes funcionarios se obtuvieron a través de campañas de *phishing web*, que se propagaron automáticamente por intermedio de los contactos de mensajería o por las redes sociales, y se complementaron con técnicas de ingeniería social (*Infobae*, 2021).

José Pino, experto en ciberseguridad, planteó en una entrevista a *Canalrcn.com* (2021) que Anonymous no hackeó ninguna información: todo se habría tratado de informes filtrados entre 2012 y 2013, y consignados en Pastebin[5]. Frente al

5 Pastebin.com es una página web donde se comparten datos de cualquier parte del mundo; puede incluir filtraciones.

hackeo de comunicaciones a la Policía Nacional, indicó que pudo ser producto de un radioteléfono perdido durante las protestas, del cual se realizaron grabaciones a las comunicaciones. También aclaró que la caída de páginas web de Presidencia no ocurrió por un hackeo, sino por obra de ataques por DDoS. Finalmente, agregó que las granjas de *bots* representan uno de los mayores riesgos de afectación al desempeño de contenidos en redes, al causar sabotaje y generar narrativas afines.

Estos hechos tienen repercusiones considerables en la apreciación de la sociedad, ya que la cultura nacional respecto a la ciberseguridad es muy débil (inmadura), y ello genera falsas perspectivas, ya que las técnicas utilizadas para afectar a las personas y las instituciones están muy lejos de ser ataques de *hackers* de alto nivel, lo cual no significa que no sean dañinas o no hayan sido escaladas, pero sí demostraron que ante las vulnerabilidades aprovechadas, la intimidación y la desestabilización generadas promueven la desinformación y la imagen negativa, y estimulan, por tanto, la manipulación.

Manipulación y proliferación de información

El uso de *trolls* y *bots* conforman una fórmula perfecta, cuya efectividad ha sido evidenciada a través de diferentes manifestaciones en la región y en el mundo. La circulación de publicaciones falsas en diversos formatos es el común denominador de eventos como los ocurridos en la crisis catalana en 2017, el estallido social de Chile y Ecuador en 2019 y las protestas en EE. UU. por la muerte de George Floyd en 2020.

Los *trolls* son el medio de propagación de contenidos. Son personas (usuarios) que se pueden agrupar por equipos, o hasta ejércitos, que operan las 24 horas del día, de manera anónima, y que provocan deliberadamente, acosan y critican en línea, y de esa forma contribuyen a elevar la polarización, así como a silenciar opiniones y a ahogar la discusión legítima. Estos se apoyan mediante *bots*, o programas computarizados que realizan tareas automáticamente y de forma repetitiva compartiendo contenidos que crean tendencia en las redes sociales, respondiendo preguntas frecuentes (plataformas de atención al cliente), enviando mensajes estructurados en foros, comentando, dando "Me gusta" e implementando ataques cibernéticos (Swedish Civil Contingencies Agency, 2019).

Durante las protestas de 2019 en Colombia, el Laboratorio de Investigación Forense Digital de Atlantic Council (en inglés, DFRLab) identificó cuentas en Twitter, Instagram y WhatsApp que difundieron contenido de presuntos saqueos, al tiempo que sugirió que migrantes y vándalos venezolanos estaban detrás del caos; asimismo, concluyó que usuarios de las redes sociales circularon videos

engañosos durante la primera semana del paro nacional de 2021; al analizarlos, la mayoría se relacionaba, presuntamente, con enfrentamientos entre manifestantes, policías y supuestos infiltrados (Suárez & Ponce, 2021).

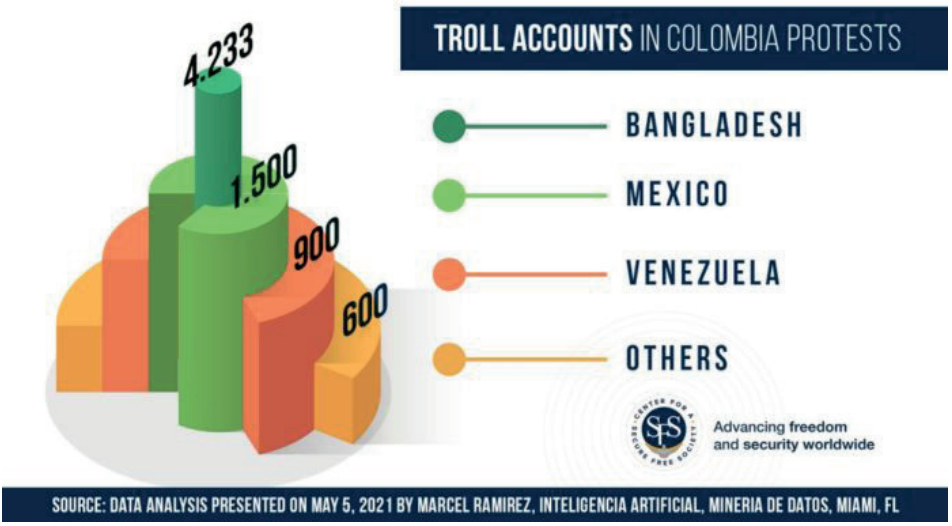
DFRLab también identificó el reciclaje de material fílmico sobre enfrentamientos ocurridos entre manifestantes y la Fuerza Pública, o actuaciones indebidas de la Policía en otros países, que se utilizaron como situaciones o evidencias de lo ocurrido en Colombia. Los ejemplos correspondían a registros en Chile y Ecuador en 2019, los cuales se presentaron como evidencia de presuntos atropellos por parte del Escuadrón Móvil Antidisturbios (Esmad) (*La República*, 2021). El impacto generado fue constante desde el inicio del paro, donde se percibió un efecto muy evidente y perjudicial: la reacción inmediata inicial del receptor, el cual, así obtenga una rectificación posterior sobre algún error o un hecho malintencionado de información falsa o engañosa, asume una posición inicial difícil de controlar o corregir, pese a que la verdad se haya demostrado.

Marcel Ramírez, experto en inteligencia artificial, minería de datos y análisis de redes sociales, manifestó que varias convocatorias y desórdenes en Colombia se organizaron desde diferentes partes del mundo. Mediante un estudio se identificaron más de 7000 cuentas falsas que originaron o replicaron noticias mentirosas. Algunas de estas concentraciones se publicaron mediante redes sociales a partir servidores ubicados en Bangladesh, Corea y China, como se ve en la figura 1. Asimismo, indicó que las granjas de *trolls* son un servicio contratado para tal fin, a costos que pueden oscilar entre 500.000 y 600.000 dólares (La FM, 2021a).

Dicho accionar fue replicado en las protestas de Chile (2019), donde otras investigaciones arrojaron las siguientes revelaciones (ConnectaLabs, 2019/2020):

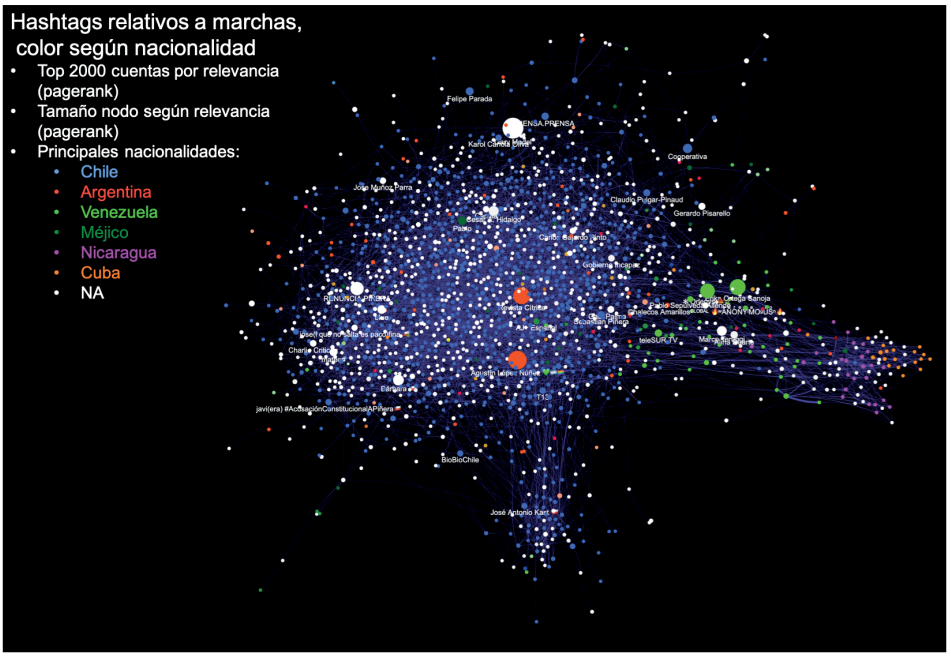
- Estudio de 4,8 millones de Tweets, 638.893 usuarios (entre el 20 de octubre y el 5 de noviembre): origen en Nicaragua, Cuba, Argentina y Venezuela, y que motivó las protestas en Chile, como se muestra en la figura 2.
- Estudio de 7,6 millones de actividades digitales: el 1 % de los usuarios generó aproximadamente el 30 % de los contenidos: origen en Venezuela, tal cual se ve en la figura 3.

Figura 1. Cuentas de trolls identificadas en Colombia durante el paro nacional.



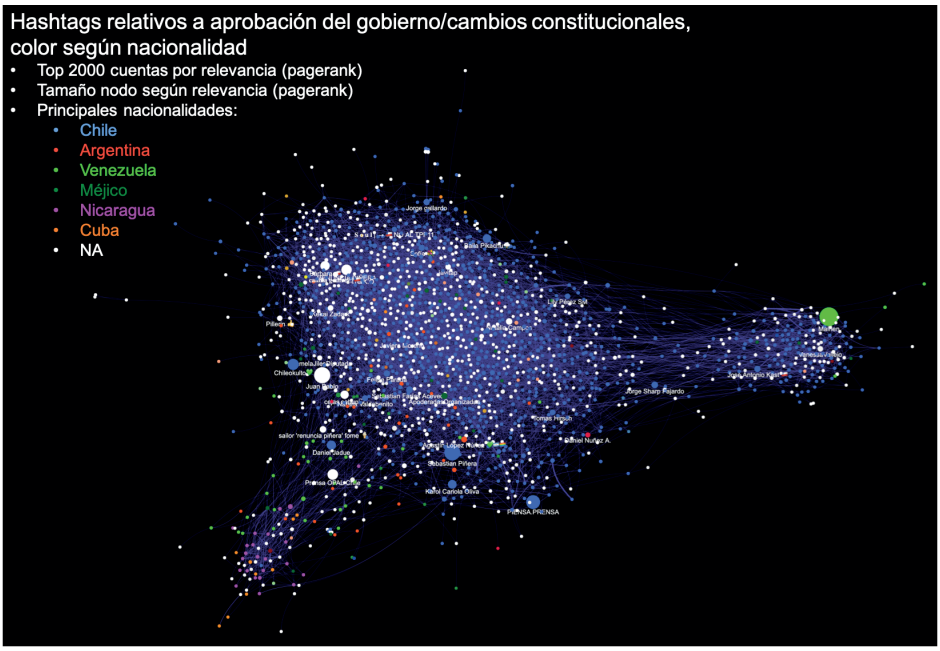
Fuente: adaptado de Asymmetric Assault on Colombia (Joseph M. Humire, 2021).

Figura 2. Análisis de *hashtags* durante las protestas en Chile (2019).



Fuente: tomado de: raw.githubusercontent.com (2020).

Figura 3. Análisis de *hashtags* sobre la aprobación del Gobierno.



Fuente: tomado de: raw.githubusercontent.com (2020).

En 2017, la Universidad George Washington analizó más de cinco millones de mensajes vinculando a los medios RT y Sputnik, y con gran cantidad de cuentas relacionadas con Venezuela, como se ve en la figura 4, para difundir una imagen negativa de España antes y después del referendo del 1 de octubre, por la independencia en Cataluña (Alandete, 2017).

En ambos casos de estudio aparece Venezuela, lo cual podría indicar que cuenta con considerable experiencia en el dominio y la explotación de estas técnicas en Latinoamérica; adicionalmente, el Instituto de Internet de Oxford indicó que dicho gobierno utiliza a menudo tropas de *trolls* y granjas de *bots* para crear y amplificar una sensación artificial de popularidad, impulso o relevancia en su población (Bradshaw & Howard, 2017).

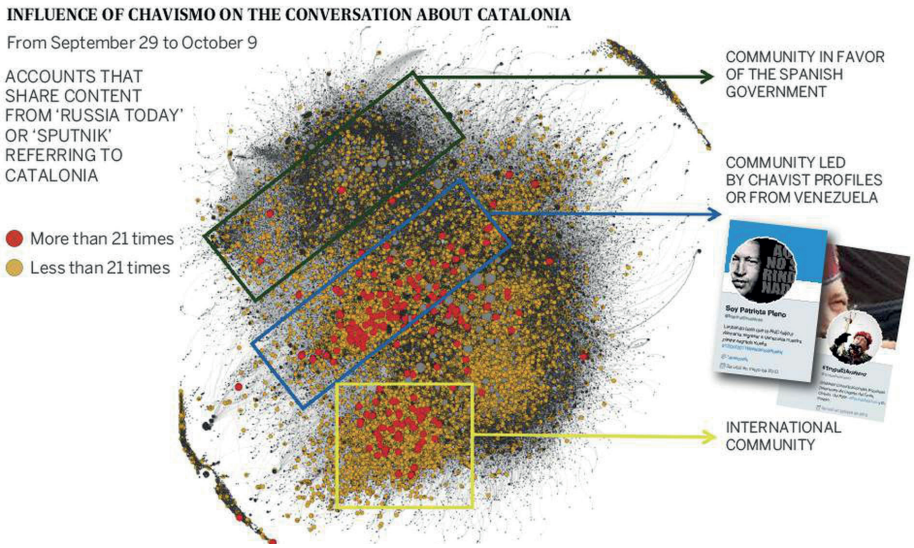
Es evidente que la situación de Colombia en materia política, económica, social e internacional se ve afectada por factores como la inestabilidad, una crisis de legitimidad, los resultados de un escenario lastimado por la pandemia, la carrera electoral para 2022, y algunos reveses del Gobierno nacional, que agotan al Estado y a sus instituciones.

Consecuentemente, pese a la diferencia entre los contextos y las realidades de los casos, hay trazabilidad y coherencia en cuanto al accionar identificado en ellos,

tales como: la influencia, la perspectiva o la intención de los medios de comunicación internacionales; la instrumentalización de las redes sociales para manipular y propagar narrativas; los ataques cibernéticos a sectores y funcionarios del Gobierno, y el uso de ejércitos o grupos de *trolls* y granjas de *bots*, características que evidencian el desarrollo de campañas de MSH.

Por último, se advierte sobre la vulnerabilidad del factor humano ante esta forma de operar. Su falta de experiencia, de conocimientos suficientes y de una regulación apropiada para manejar de manera eficaz este tipo de entornos y amenazas se suma al pobre nivel de madurez respecto a la cultura organizacional en ciberseguridad y el manejo responsable de la información.

Figura 4. Análisis sobre la influencia del chavismo.



Fuente: tomado de: english.elpais.com.

Técnicas y modalidades relacionadas con prácticas o campañas de manipulación social hostil

La simbiosis tipológica enmarcada en el siglo XXI ha fomentado la detonación de guerras de información vinculadas con estallidos sociales; principalmente, en países democráticos de perfil capitalista con altos índices de corrupción, desigualdad y polarización. Todo ello tiende a evolucionar gracias a la diversidad de características presentes en la era de la Cuarta Revolución Industrial, o Revolución Digital (Schwab, 2016).

Dichos elementos convergen armónicamente en la era de la posverdad facilitando la comunicación en un mundo globalizado, dinamizando la infoxicación de la sociedad a través de contenidos falsos o engañosos, donde los individuos carecen de habilidad para tratar, interpretar y determinar, coherente y responsablemente, qué hacer con tal cantidad de datos (Keyes, 2004).

Lo anterior podría considerarse una forma de ataque a la percepción y la opinión de las personas, que busca subvertir las ideas concebidas en un Estado o un grupo social, y da espacio, una vez más, a la connotación de escenarios característicos de las G5G, como lo son el dominio tecnológico y del ciberespacio, con implicaciones en dimensiones organizacionales y psicológicas (Álvarez et al., 2017).

Al abordar esta amenaza se identifican la diversidad de su naturaleza y la multidimensionalidad de su alcance, donde la forma tradicional de entenderla, analizarla y enfrentarla implica la participación de diferentes estamentos estatales, instituciones y sectores, tanto públicos como privados (Oxford Internet Institute, 2021). Dicha apreciación aplicó en Colombia a partir del 28 de abril de 2021, cuando se aprovecharon la crisis económica, la fragmentación de la sociedad y el impacto de la pandemia para socavar la legitimidad del Gobierno buscando efectos propicios ante un panorama electoral, entre otros intereses.

Con base en las prácticas evidenciadas, se relacionaron sus respectivos parámetros o metodologías conexos con acciones de desinformación y manipulación, como se describe a continuación.

Armamentización de las redes sociales

Las redes sociales surgen como una herramienta poderosa para la comunicación, la conexión, la sociedad y el conflicto, ya que son muy eficaces al momento de desinformar, dividir y contribuir con la materialización de violencia en diferentes modalidades. Su impacto en las comunidades es complejo; se desarrolla y se adapta a las necesidades del que pretenda desestabilizar una sociedad, sembrar el terror, derrocar un gobierno o alcanzar de forma agresiva una meta política; fuera de lo que normalmente se consideraría una amenaza, se trata de la preparación y el uso de las redes sociales como un arma, que podría caracterizarse por su hibridez y su asimetría (Robins & Mercy Corps, 2019).

Robbins y Mercy Corps (2019) indica que se hace uso innovador de herramientas y métodos habilitados digitalmente para distorsionar los hechos que ocurren y difundir narrativas o contenidos con objetivos como desorientar la rendición de cuentas, socavar la aceptación de la comunidad, erosionar la cohesión

social o incitar al pánico y el terror, dentro de lo cual el ciudadano se ve envuelto casi inevitablemente, ya sea de forma intencionada o inconsciente, a lo cual se contribuye con acciones *online* y *offline* que socavan sociedades saludables o fomentan la violencia.

Muestra de lo planteado fue la prolongación de actividades relacionadas con el paro nacional, a pesar del riesgo que implicaban las aglomeraciones en un entorno de pandemia en su pico más alto. Para ampliar este concepto, se relacionan dos técnicas o medios utilizados a través de las redes sociales para lograr las MSH.

Discurso de odio digital

Las plataformas sociales pueden amplificar el discurso de odio en contextos frágiles, donde los rumores y la desinformación desempeñan un papel fundamental a la hora de incitar a la violencia intercomunitaria y electoral, entre otras. Las fuentes de información extrafáctica contribuyen a este problema, y a menudo, las redes sociales las amplifican (Robins & Mercy Corps, 2019). El discurso de odio digital ha impulsado el sentimiento de lucha de clases en Colombia, y se puede apreciar la participación abierta de funcionarios públicos y personalidades famosas que lo exacerban.

Operaciones de información

Componente central de la estrategia de guerra de información, y mediante las cuales se amplifican afirmaciones fabricadas y acusaciones falsas contra instituciones del Estado, el gobierno, el sector privado y otros, a los que se atribuyen nexos con organizaciones ilegales, actos de corrupción o inculpaciones estructuradas sobre vínculos con potencias extranjeras, en la búsqueda de desestabilizar y causar división entre la población y sus gobernantes y sus autoridades, entre otros aspectos. Son enfrentamientos sin contacto, no convencionales, utilizando capacidades de precisión dirigidas a los no combatientes (Bakshi, 2018).

Ataques cibernéticos

La información, como activo estratégico en la sociedad y en el ciberespacio, se expone permanentemente a ataques como *phishing*, ingeniería social, DDoS, Fuerza Bruta, MITM, Programas Malignos y *Defacement*, entre otros. A pesar de ello, existe un riesgo mucho mayor: el desconocimiento y la vulnerabilidad de los individuos

ante cada uno de estos. La diversidad de técnicas analizadas implica variedad de riesgos para los que la sociedad no está preparada, pues no cuenta con una cultura organizacional madura para prevenirlas o detectarlas a tiempo, y poder así tomar cursos de acción pertinentes o conducentes a la autoprotección y el bien común (Departamento de Estado de los Estados Unidos, 2020).

Respecto a estas agresiones se deben tener en cuenta dos aspectos. Primero, se observó un profundo nivel de preparación, tecnificación y direccionamiento de blancos al momento de realizarlos (las elecciones en EE. UU. en 2016, el ataque a las FF. MM. de Colombia, al Centro Democrático y a la página presidencial…); segundo, su alto grado de necesidad para el soporte de las campañas de MSH, ya que esta información es requerida para el planeamiento de estrategias y la selección de métodos o herramientas. En ambos estudios de caso se evidenciaron ataques cibernéticos en contra de los sistemas de información de instituciones, organizaciones y personas influyentes o políticamente expuestas.

Caracterización y selección de blancos

A partir de la información obtenida mediante las técnicas citadas, se efectúa una selección de objetivos que puede obedecer al uso de herramientas de análisis y minería de datos, el perfilamiento psicológico o la necesidad de obtener una ventaja frente a algún error del adversario que permita o facilite socavar su legitimidad o su credibilidad. También podría sujetarse a la condición de transmitir narrativas a blancos audiencia que permitan forjar una percepción o una opinión favorable o desfavorable, de acuerdo con factores como la población, la ideología, los grupos afectados por necesidades básicas insatisfechas, las edades, la raza, la cultura, sectores públicos o privados o la Fuerza Pública, entre otros, a los que se direccionan los contenidos preparados para minar su voluntad o fomentar algún juicio o postura (Mazarr, Casey et al., 2019). Para este tipo de actividades existen compañías privadas que ofrecen portafolios de servicios, tal como se evidenció con CA.

Configuración de una sociedad fracturada e inestable

Las operaciones psicológicas se enfocan principalmente en las pasiones y los sentimientos del ser, con el propósito de hacerlo sentir identificado y representado de alguna forma. En este sentido, en los entornos analizados en cada estudio se demostró que previamente al desarrollo de los acontecimientos, los ciudadanos sobrellevaban situaciones como la polarización, la fractura política o ideológica de la sociedad, las carreras electorales, los efectos de la pandemia, el inconformismo general o de minorías, el racismo, los abusos policiales y el feminismo, prácticamente materializados en una crisis política, económica y social, influenciada, a su vez, por un contexto internacional desfavorable.

Estos vacíos se configuraron en vulnerabilidades que, a su vez, fueron oportunidades de acción para las campañas de MSH, las cuales encuentran un nicho de proliferación muy fértil y dominable por la dificultad que representa para el Estado su manejo y su control.

Marketing y propaganda

Esta configuración se produce cuando, en el ecosistema de la información, ciertos sectores resultan favorecidos por los efectos desatados a raíz de la MSH. Dichos sectores permiten posicionar de manera fuerte al individuo o la organización que posee o sobre los que están puestas las necesidades al servicio de la campaña. El mencionado escenario se puede explotar, de acuerdo con su evolución, para sacar más provecho en acciones como operaciones de influencia, que buscan, precisamente, instigar actividades democráticas (Golovchenko et al., 2018).

Es primordial denotar la importancia que repercute para la campaña que medios de comunicación tradicionales o alternativos, con o sin intención, coadyuven generando credibilidad hacia el actor que se esté beneficiando, de la manera vista en los contenidos identificados en cadenas como RT, DW, France 24, BBC Mundo y CNN, entre otros.

Instrumentalización masiva de *trolls* y *bots*

La desinformación y el engaño tienen trazabilidad con los parámetros y las técnicas estudiados; sin embargo, para lograr el efecto deseado, necesitan una forma masiva y permanente de proliferación y acción, lo cual es posible a través de la configuración de ejércitos de *trolls* y granjas de *bots*, donde se busca generar un flujo constante de información que llegue a los blancos audiencia (Mazarr, Bauer et al., 2019). Esto se puede constar en los resultados y los informes obtenidos en los eventos de Cataluña, Ecuador, Colombia y Chile, donde se argumentó la probable participación de cuentas de redes sociales con origen en países como Venezuela, Nicaragua, Cuba y Argentina.

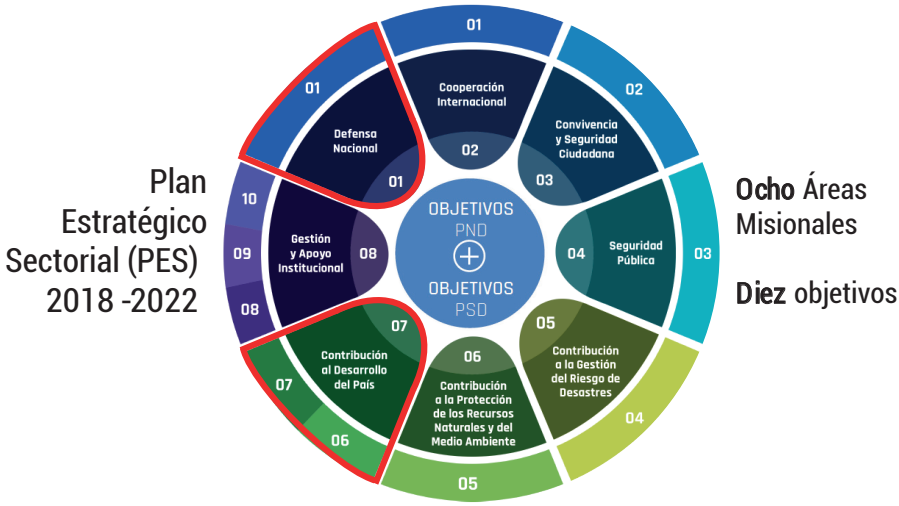
Las campañas de MSH utilizan todos estos métodos en fases y pasos organizados con el propósito de impactar eficaz y ágilmente al ser humano, una institución o una organización establecida como blanco. Los seis parámetros son los más observados en los últimos dos años; los casos de Chile, EE. UU., Colombia y Reino Unido se caracterizaron por completar al menos tres de los mencionados elementos para soportarlas.

Lineamientos para contrarrestar las campañas de manipulación social hostil

La estrategia se enmarca en el Plan Estratégico del Sector Defensa y Seguridad 2018-2022 (PES), donde se determinan los objetivos, las metas y las iniciativas para el cumplimiento y el desarrollo de los lineamientos formulados por el presidente de la República en el Plan Nacional de Desarrollo (PND) 2018-2022, en la Política de Defensa y Seguridad (PDS) y la Política Marco de Convivencia y Seguridad Ciudadana (PCSC), Para la Legalidad, el Emprendimiento y la Equidad. Su estructuración se fundamenta en las áreas misionales del sector y su enfoque multidimensional de la seguridad, y construye así una visión integral para enfrentar los retos y las amenazas a la defensa y seguridad del país para la defensa de los intereses de la nación (Ministerio de Defensa Nacional, 2018).

En consecuencia con lo anterior, se plantea de manera gráfica la estrategia del sector defensa, donde se destaca la importancia de la ciberseguridad y ciberdefensa (Figura 5). A continuación, se evidencian dos objetivos estratégicos fundamentales: el Objetivo 1, que es garantizar la defensa de la soberanía, la independencia y la integridad del territorio nacional, y el cual se encuentra alineado con el Área misional N.º 1 Defensa Nacional; y el Objetivo 7, que es contribuir al desarrollo de los intereses marítimos y fluviales del país, alineado, a su vez, con el Área misional N.º 7 Contribución al desarrollo del país.

Figura 5. Plan Estratégico del Sector Defensa y Seguridad 2018-2022.



Fuente: Ministerio de Defensa Nacional, informe de seguimiento 2020.

Se resalta la importancia del ciberespacio para la protección de los intereses nacionales, los cuales son vulnerables a la MSH debido a que esta repercute contra la estabilidad de un Estado en su naturaleza política, económica, social e internacional, lo que puede impactar en la contribución al desarrollo del país y a la defensa nacional. Sin duda, uno de los principales aspectos en cuanto a la combinación de técnicas y estrategias para materializar campañas de MSH es tener un dominio conformado por la información, la sociedad y el ciberespacio, elementos interconectados que proporcionan la base para las actividades económicas, sociales y políticas de un Estado (Mazarr, Bauer et al., 2019).

Consecuentemente con lo planteado, el aprovechamiento de dicho dominio mediante la explotación de las vulnerabilidades presentes en el sistema es la principal condición para generar resultados que pueden optimizarse al añadir elementos como la tecnología y las redes sociales, los efectos causados por las medidas y los cambios ante la pandemia de la COVID-19, el incremento de la actividad digital, y del flujo de datos y la desinformación, entre otros, que conforman el ambiente o ecosistema de la información. *Este debe asumirse como un escenario de relevancia estratégica*, dentro del cual se busca al máximo la obtención de factores que permitan incrementar su control como principal estrategia para contrarrestar las amenazas, los riesgos y los desafíos que implican para el Estado colombiano las campañas de MSH que se gestan a través del ciberespacio.

Alcanzar este fin requiere la vinculación de múltiples iniciativas y actores, debido a su magnitud; de acuerdo con Digital Future Society (DFS), controlar lo que circula digitalmente no se puede en solitario, ya sea por parte de un gobierno, el sector privado o una entidad particular. Esta precisión implica el planteamiento del primer lineamiento: *priorizar y fomentar la cooperación con visión integral, de modo que esta favorezca los intereses comunes y promueva la generación de estrategias con enfoque multidimensional.*

La cooperación a que se hace referencia no es de naturaleza netamente estatal: implica la necesidad de lograr la integración de capacidades para contrarrestar la amenaza de la MSH partiendo de un liderazgo del sector defensa como actor idóneo y pertinente. De igual forma, el Estado debe buscar una integración más eficiente y cohesionada entre los sectores público y privado; principalmente, en los medios de comunicación, la educación o la academia, la infraestructura crítica y productiva, y organizaciones no estatales, al igual que con otros países, a través de todos los cuales se obtengan la sinergia y el empoderamiento suficientes para generar las estrategias ideales y hacer frente al desafío.

En efecto, esta sinergia debe lograr una armonía entre sus articuladores, ya que de su adecuado funcionamiento dependen la construcción de ideas y capacidades, el sostenimiento y la continuidad de las alianzas o los acuerdos de apoyo

mutuo, el intercambio de información y, principalmente, la recuperación o el fortalecimiento de la confianza en las instituciones. En tal sentido, la propuesta podría impactar en las áreas misionales N.º 2 Cooperación internacional, y N.º 8 Gestión y apoyo institucional, del PES.

Asimismo, es pertinente impulsar, mediante una estrategia diplomática, alianzas enfocadas en contrarrestar la MSH; un ejemplo de aplicación es el esfuerzo multilateral construido mediante la Campaña Naval Orión, liderada por la Armada de la República de Colombia (ARC), donde se integran medios, capacidades e inteligencia para desarrollar operaciones en los escenarios marítimo, fluvial, aéreo y terrestre, coordinadas con los países que comparten el interés en neutralizar el problema mundial de las drogas ilícitas. Dicha iniciativa es el reflejo del cumplimiento de compromisos adquiridos por el Estado colombiano con múltiples instrumentos internacionales, así como una alianza estratégica de cooperación internacional que para 2021 llegó a involucrar a 38 países y 88 instituciones nacionales e internacionales (Armada de Colombia, 2021).

Articulado con lo anterior, el segundo lineamiento plantea el *empoderamiento del ciudadano y la responsabilidad del Estado sobre este*. Cada vez son más las personas con acceso a la información. Su consumo y su producción son variables casi imposibles de controlar o de medir y, a su vez, implican la generación de situaciones como las vistas en los estudios de caso. El consumo de datos puede tener repercusiones en la producción o la replicación de contenidos, según el criterio y las aptitudes con que cuente el individuo (nivel y calidad de educación). Independientemente de lo que se consume, si el contenido está creado con fines dañinos, sobre unas condiciones particulares, es preciso analizar la forma de prevenir y mitigar los escenarios y los factores determinantes de dichas conductas.

Para ilustrar mejor esta idea basta con entender que si el ciudadano conoce bien conceptos como la desinformación o las noticias falsas, entre otros, su identificación y su manera de actuar ante estas, los riesgos y el impacto que pueden generar su replicación o una opinión sesgada, entre otras implicaciones, le servirán de instrumento para manipular el ecosistema de la información.

Si bien el Estado tiene un deber, es imposible aceptar que lo puede cumplir de forma independiente; sin embargo, mientras se forja la cooperación bajo su liderazgo, el empoderamiento de las personas se obtiene desde la capacitación o la alfabetización digital, que le permiten la comprensión cada vez mejor de dicho entorno y su interrelación con el ciberespacio, al involucrar el entendimiento de la dinámica de los flujos de información, de modo que transmita a los individuos el conocimiento de las amenazas y las vulnerabilidades presentes en ese ambiente, lo cual conduce a la mitigación de conductas perjudiciales y a la gestión en ciberseguridad.

La huella de la Cuarta Revolución Industrial no es solo de carácter tecnológico: su rápido desarrollo y su evolución están transformando una sociedad rezagada en aspectos como la falta de acceso y la carencia de habilidades o conocimientos digitales, donde la digitalización de las actividades cotidianas no se detiene, y así empeora la situación con consecuencias como la exclusión social (Fundación Telefónica, 2020). Tales condiciones ya hacen parte de las necesidades básicas, donde dicho rezago focaliza la necesidad de capacitar y alfabetizar para mitigar el impacto negativo en la sociedad.

Esta iniciativa, aparte de abordar temas tecnológicos, también debe derivar en dimensiones sociológicas, tomando en cuenta que la cantidad de información que se transmite y el intercambio deliberado de contenidos son el resultado de estrategias que buscan persuadir y manipular la sociedad humana y la opinión pública. Por consiguiente, estas medidas coadyuvarían con la creación de una conciencia situacional colectiva que, a su vez, fortalecería la cultura organizacional del país respecto a la tecnología y el entorno digital protegiendo a los ciudadanos, evitando la afectación de la sociedad y blindando el sistema democrático. En tal sentido, dicha propuesta podría impactar en el área misional N.º 7 Contribuir al desarrollo del país, alineado con el objetivo estratégico N.º 6 Contribuir al desarrollo económico y social del país, con las capacidades de la Fuerza Pública, y a su vez se puede articular junto con otros campos de acción del Estado para contribuir con la construcción y el direccionamiento de este empoderamiento.

Conforme al objeto de los anteriores lineamientos, donde la cooperación y el empoderamiento cumplen un papel significativo ante la existencia de una potencial gama de tecnologías y técnicas analizadas, las crecientes oportunidades de transformar este entorno propician escenarios favorables para diferentes actores hostiles que los explotan en aspectos como la caracterización y la selección de blancos u objetivos (perfilamiento psicológico).

Durante la pandemia fue evidente la vulnerabilidad de las infraestructuras digitales, donde el incremento porcentual de incidentes tanto cibernéticos como de hostigamiento social digital demostró la necesidad de proveer mayor seguridad en el ciberespacio desde niveles domésticos hasta profesionales, lo cual también se evidenció con el volumen de usuarios afectados (Centro Criptológico Nacional, 2020).

Por lo anterior, se propone como tercer lineamento el *fortalecimiento de las estructuras o las organizaciones encargadas de ciberseguridad y ciberdefensa*. Este debe obedecer a que el entorno o ecosistema digital y de la información, al comprender la mayoría de las actividades y los procesos de la sociedad, dependerá de la ciberseguridad y la ciberdefensa de la nación para tomar medidas activas o pasivas frente a la diversidad de riesgos y amenazas a los que se halla expuesta; no

obstante, la responsabilidad tampoco es exclusiva del sector defensa. Como ya se ha afirmado, este actor es el indicado para liderar las estrategias y las iniciativas, pero es indispensable involucrar y comprometer diferentes ciencias, disciplinas y campos de acción para consolidarlas de manera holística.

Bajo el concepto de la acción unificada (AU) del Estado se puede describir una variada escala de actividades que implican la integración y la coordinación con organismos gubernamentales y ONG, así como con agencias del sector privado, a fin de obtener no solo un compromiso, sino también, coadyuvar con la construcción de capacidades y procesos, y la de un sistema completo a partir del cual se puedan generar y continuar estrategias consecuentes con las necesidades y los requerimientos para mitigar cualquier riesgo proveniente de la MSH, así como de la superior demostración de ataques cada vez más numerosos, avanzados y de mayor impacto (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2020).

La propuesta complementa las realizadas en primera y segunda instancia, toda vez que implica dentro de dicho fortalecimiento la demanda de esfuerzos desde diversos sectores, pero enfocados en la necesidad de tener mejores capacidades en ciberseguridad y ciberdefensa, más allá de los escenarios que se conocen hasta el momento, alineado ello con el objetivo estratégico N.º 1 Garantizar la defensa de la soberanía, la independencia y la integridad del territorio nacional, y buscando ampliar las estrategias en la meta N.º 2 Fortalecer las capacidades de ciberseguridad y ciberdefensa.

En cuarto lugar, inmerso dentro los aspectos mencionados, no se debe perder de vista la variedad de tecnologías e innovaciones digitales disruptivas y emergentes, que es un pilar fundamental que demanda el *fortalecimiento de la vigilancia tecnológica* (VT) *en el ciberespacio.* De acuerdo con el artículo "Vigilancia tecnológica: directriz para el éxito organizacional", la VT reúne una serie de metodologías, herramientas y procedimientos mediante los que se identifican y se integran datos de forma sistemática y organizada, para su respectivo análisis y su transformación en información y conocimiento dominante sobre las condiciones del entorno de la organización, así como de orden interno, y a fin de alcanzar a las personas correspondientes para definir y establecer decisiones estratégicas (Robin et al., 2013).

La VT comprende tres elementos fundamentales: las herramientas, las capacidades tecnológicas y el talento humano idóneo para el desarrollo de esta actividad, los cuales deben estar en la agenda del Estado, y con una adecuada proyección, para que la capacidad se construya hasta obtener una condición ideal o suficiente. Este lineamiento se alinearía con el área misional N.º 08: Gestión y apoyo institucional, y con el objetivo N.º 8: Continuar con el proceso de transformación, modernización y fortalecimiento institucional del sector defensa y seguridad.

En este orden de ideas, durante el análisis y el desarrollo de cada uno de los lineamientos expuestos se identificó la *perenne necesidad de recurrir a los saberes, los conocimientos y las herramientas derivadas de otras ciencias, disciplinas y sectores, para ser integrados al proceso con el fin de obtener resultados aplicables de forma integral y con enfoque multidimensional, y así generar conocimiento para la apropiada toma de decisiones*. Este resultado constituye el planteamiento del quinto lineamiento, en el cual se considera que la estrategia debe estar acompañada e integrada por componentes que aporten con esa construcción de conocimiento, y dentro de los que podemos indicar a la inteligencia en sus diferentes dimensiones, las comunicaciones estratégicas y la vinculación de expertos en sociología, psicología y comunicación social, entre otros.

Consecuentemente, *el impacto será alinear sistemáticamente una amplia gama de capacidades para proteger al Estado, las instituciones y los individuos* afectando la percepción de las personas de manera que promuevan los intereses nacionales, para así favorecer la gestión y la implementación de tecnologías para proteger los sistemas de información, las infraestructuras críticas cibernéticas y el desarrollo del conocimiento en ciberseguridad. Dicho escenario presenta las características suficientes para mantener su alineación con la estrategia del sector defensa, por lo que se enmarca en las áreas misionales y en los objetivos estratégicos ya tratados.

Por último, a partir de las experiencias obtenidas en la lucha contra amenazas como el narcotráfico y el crimen organizado transnacional, se recomienda tomar dichas iniciativas como modelo para articular los lineamientos a través de *grupos u organismos de seguimiento e integración de todo lo concerniente al control del entorno de la información, no solo en el ámbito nacional (público, privado), sino también, en los escenarios regional o internacional, en figuras como Centros de Fusión y Análisis del Ambiente de la Información*.

En consecuencia, al trabajar cada uno de los lineamientos expuestos es significativo apreciar cómo estos abordan los elementos que conforman el terreno que busca la MSH para materializar sus técnicas y sus herramientas, lo cual demuestra que se soportan entre sí al crear las condiciones necesarias para que el Estado sea mucho más efectivo en la prevención, la detección y la neutralización, así como la forma de contrarrestar las amenazas de la MSH, considerando, por supuesto, que se cuenta con limitaciones, desafíos y retos, que pueden ser superados, principalmente, por el avance continuo del control del ambiente de la información.

Conclusiones

Se evidenció el impacto que tiene la MSH no solo en el Estado, sino también, en los individuos, las instituciones y los grupos sociales, al materializarse en los entornos político, social, económico e internacional, donde la búsqueda de la seguridad debe apoyarse mediante el fortalecimiento de la institucionalidad, la protección y el empoderamiento del ciudadano, el resguardo de la democracia y el Estado social de derecho y la materialización de la doctrina sobre este campo que direccione las capacidades del Estado hacia perspectivas y mecanismos nuevos para combatir estas amenazas, con un enfoque holístico que va más allá de lo militar, pero, sin dudas, bajo el direccionamiento de dicho componente.

En consecuencia con lo anterior, el análisis de los casos coadyuvó con la determinación del acierto que hay en la combinación de técnicas y métodos como herramienta clave de la MSH para afectar los intereses de la nación al generar cambios profundos en los individuos, la sociedad, las instituciones —y por ende, el Estado—, a partir de una simbiosis que se apoya en los medios tecnológicos, las redes sociales, las vulnerabilidades y las fortalezas de los diferentes actores, y la ventaja de una estrategia muy bien estructurada de la que poco se sabe y no se ha investigado a profundidad en Colombia, pero que ha tenido resultados contundentes en sistemas democráticos representativos en la región y el mundo.

Los ejemplos, más allá de demostrar la efectividad de la combinación de prácticas de la MSH, son una advertencia de a qué podría verse expuesta Colombia en diversos escenarios por cuenta de lo que implican los intereses de diferentes actores y sectores sobre las elecciones presidenciales y del Congreso en 2022, escenario propicio para preparar y ejecutar de manera oportuna en la población las herramientas y las técnicas analizadas, con el objeto de socavar el orden y la tranquilidad del Estado social de derecho.

La diversidad y la multidimensionalidad de esta amenaza implican para el Estado la integración de diferentes estamentos, sectores e instituciones, ya sean públicos o privados; es indiscutible que no se puede abordar la MSH mediante herramientas y capacidades convencionales, pues los actores a los que se enfrenta son disímiles; la realidad de estos es totalmente distinta, porque sobrepasan los límites de la nación y no tienen una faceta reconocible, por lo cual se hace necesario acompañar este proceso con la investigación continua y detallada que permita introducir estrategias con trazabilidad en todos los aspectos y los escenarios afectados.

Las prácticas y los métodos de MSH no se encuentran contemplados como amenaza o riesgo dentro del Plan Estratégico Sectorial, razón por la que es evidente la necesidad de abordar el tema oportunamente, para que el sector defensa

contemple las necesidades, las capacidades y las herramientas necesarias para mitigar y contrarrestar su accionar en el corto, mediano y largo plazo.

Finalmente, se evidenció que las prácticas vinculadas con la MSH se relacionan con acciones como las operaciones de información, las operaciones psicológicas, la guerra económica y el ciberactivismo, entre otros elementos, que por su naturaleza tienen una connotación con estrategias de guerras modernas de quinta generación, que buscan afectar al individuo trastocando su forma de pensar, minimizando el desarrollo de confrontaciones convencionales mediante la desestabilización de un Estado en aspectos económicos, políticos, sociales e internacionales.

Referencias

Ablon, L., Binnendijk, A., Hodgson, Q., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. A. (2019). *Operationalizing cyberspace as a military domain: Lessons for NATO*. https://www.rand.org/pubs/perspectives/PE329.html

Alandete, D. (2017, 11 de noviembre). Russian network used Venezuelan accounts to deepen Catalan crisis. *El País*. https://english.elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

Álvarez, C., Santafé, J., & Urbano, O. (2017). Metamorphosis bellum: ¿Mutando a guerras de quinta generación? En: *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia*. Escuela Superior de Guerra "General Rafael Reyes Prieto".

Arjona, M. (2020). La información en la era de internet. El caso de las Fake News. *REI - Revista Estudos Institucionais, 6*(2), 376-394. https://doi.org/10.21783/rei.v6i2.445

Armada de Colombia. (2021). *Resumen consolidado VII versión Campaña Naval Orión*. Dirección Contra las Drogas Armada Nacional.

Badillo, Á. (2019). La Sociedad de la desinformación: Propaganda, «fake news» y la nueva geopolítica de la información. *Real Instituto Elcano*, 42. http://www.realinstitutoelcano.org/wps/wcm/connect/fc1e5338-b663-4254-943e-15b1d154e62e/DT8-2019-Badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion.pdf?MOD=AJPERES&CACHEID=fc1e5338-b663-4254-943e-15b1d154e62e

Bakshi, B. (2018). Information warfare: Concepts and components. *International Journal of Research and Analytical Reviews (IJRAR), 5*(4). http://ijrar.com/upload_issue/ijrar_issue_20542533.pdf

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina*

y el Caribe. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Bassets, M. (2016, 26 de julio). El factor Putin irrumpe en la campaña entre Clinton y Trump. *El País*. https://elpais.com/internacional/2016/07/25/actualidad/1469464119_801200.html

BBC News Mundo. (2019, 24 de julio). La multa récord de US$5.000 millones que deberá pagar Facebook en EE.UU. https://www.bbc.com/mundo/noticias-49093124

BBC News Mundo. (2021, 4 de mayo). *Cómo la violencia se tomó las calles de Colombia (y por qué Cali fue el epicentro durante días)*. https://www.bbc.com/mundo/noticias-america-latina-56989232

Bigelow, B. (2019). What are Military Cyberspace Operations Other Than War? *2019 11th International Conference on Cyber Conflict (CyCon), 900*, 1-17. https://doi.org/10.23919/CYCON.2019.8756835

Blanco, M. (2016). *Control del ciberespacio desde el Sector Defensa: Un reto a la seguridad nacional*. Universidad Piloto de Colombia.

Bradshaw, S., & Howard, P. (2017). Troops, trolls and troublemakers: A global inventory of organized social media manipulation. *Computational Propaganda Research Project, 2017.12*. https://demtech.oii.ox.ac.uk/research/posts/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

Cadwalladr, C. (2016, 4 de diciembre). Google, democracy and the truth about internet search. *The Guardian*. http://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook

Canalrcn.com. (2021, 11 de mayo). Anonymous no ha hecho ningún hackeo, afirma experto. https://www.canalrcn.com/supertrending/negocios/anonymus-no-ha-hecho-ningun-hackeo-afirma-experto-378211

Castells, M. (2002). Internet y sociedad. https://www.ucr.ac.cr/medios/documentos/2007/Internet_y_sociedad_Manuel_Castells.pdf

Centro Criptológico Nacional [CCN]. (2020). *Ciberamenazas y tendencias*. Centro Nacional de Inteligencia. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html.

CNN Video. (2017). Russia weaponized Twitter to sway election—CNN Video. https://www.cnn.com/videos/politics/2017/09/20/pro-trump-twitter-accounts-weaponized-russia-us-election-ebof-pkg-griffin.cnn

ConnectaLabs. (2020). Connectalabs/riots_chile_analisis [HTML]. https://github.com/connectalabs/riots_chile_analisis/blob/d457ed7e785a318ac049d4131098ef608489ff77/analisis_tweets_sobre_levantamiento_social.md

ConnectAmericas. (s. f.). *Community for Businesses in Latin America and the Caribbean | ConnectAmericas*. https://connectamericas.com/es/service/vaki-nuevos-mecanismos -de-financiaci%C3%B3n

C-SPAN. (2016). *1996: Hillary Clinton on «superpredators» (C-SPAN)* [video]. https://www.youtube.com/watch?v=j0uCrA7ePno

Departamento de Estado de los Estados Unidos. (2020). *Pillars of Russia's Disinformation and Propaganda Ecosystem*. GEC.

Deutsche Welle. (2021a). Los jóvenes de la Primera Línea en Colombia. https://www.dw.com/es/los-j%C3%B3venes-de-la-primera-l%C3%ADnea-en-colombia/av-57500333

Deutsche Welle. (2021b). Colombia: Anonymous se atribuye «hackeo» de la página del Ejército. https://www.dw.com/es/colombia-anonymous-se-atribuye-hackeo-de-la-p%C3%A1gina-del-ej%C3%A9rcito/a-57436738

Droguett, R. (2019). Chile. Qué es y qué expresa la Primera Línea. *Resumen Latinoamericano*. https://www.resumenlatinoamericano.org/2019/12/20/chile-que-es-y-que-expresa -la-primera-linea/

Eissa, S., Gastaldi, S., & Poczynok, I. (2012). *El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino.* VI Congreso de Relaciones internacionales, Argentina.

El Colombiano. (2021). Colombia ha recibido más de mil millones de intentos de ciberataques en 2021. https://www.elcolombiano.com/colombia/colombia-continua -recibiendo-intentos-de-ciberataque-en-2021-MD15169115

Farinetti, M. (2002). La conflictividad social después del movimiento obrero. *Nueva Sociedad, 182*. https://nuso.org/autor/marina-farinetti/

Fundación Telefónica. (2020). *Sociedad Digital en España 2019*. https://www.fundaciontelefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2019/699/.

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs, 94*(5), 975-994. https://doi.org/10.1093/ia/iiy148

Hernández, R., Fernández, C., Baptista, P., Méndez, S., & Mendoza, C. (2014). *Metodología de la investigación*. McGrawHill.

Instituto Colombiano para la Evaluación de la Educación (ICFES). (1996). *Especialización en teoría, métodos y técnicas de investigación social*. http://biblioteca.udgvirtual.udg.mx:8080/jspui/bitstream/123456789/2815/1/Investigaci%c3%b3n%20cualitativa.pdf

Illing, S. (2018). Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained. *Vox*.

Infobae. (2021). Así es como se realizan los ataques cibernéticos de Anonymus en Colombia. infobae. https://www.infobae.com/america/colombia/2021/06/06/asi-es-como-se-realizan-los-ataques-ciberneticos-de-anonymus-en-colombia/

Keyes, R. (2004). *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*. St. Martin's Press.

La FM. (2021a). ¿Cómo operan cuentas falsas en redes, desde otros países, para agitar el paro en Colombia? https://www.lafm.com.co/colombia/como-operan-cuentas-falsas-en-redes-desde-otros-paises-para-agitar-el-paro-en-colombia

La República. (2021). Agencia internacional reportó alto grado de desinformación en medio de las protestas. https://www.larepublica.co/globoeconomia/agencia-internacional-reporto-alto-grado-de-desinformacion-en-medio-de-las-protestas-3172877

Lindholm, R. (2017). Project Alamo, and how Trumps Fake News & Facebook ads won Donald Trump the Presidency. *Proyecto Alamo*. https://semantiko.com/project-alamo/

Mazarr, M., Bauer, R., Casey, A., Heintz, S., & Matthews, L. (2019). *The emerging risk of virtual societal warfare: Social manipulation in a changing information environment*. https://www.rand.org/pubs/research_reports/RR2714.html

Mazarr, M., Casey, A., Demus, A., Harold, S. W., Matthews, L. J., Beauchamp-Mustafaga, N., & Sladden, J. (2019). *Hostile social manipulation present realities and emerging trends*. Rand National Defense Research Inst Santa Mónica CA, United States.

Mejías, S., & De Sousa, S. (2015). *La multidimensionalidad de la seguridad nacional: Retos y desafíos de la región para su implementación*. Instituto Universitario General Gutierrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa.

Ministerio de Defensa Nacional. (2018). *Plan Estratégico del Sector Defensa y Seguridad 2018-2022*. https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Planes/guia_planeamiento_estrategico_2018-2022.pdf

Oxford Internet Institute. (2021). *Programme on Democracy & Technology*. https://demtech.oii.ox.ac.uk/team/samuel-woolley/

Realpe, M., & Cano, J. (2020). *Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia*. https://doi.org/10.12804/si9789587844337.10

Rivolta, A. (2012). *Las vulnerabilidades de las operaciones militares derivadas de las redes sociales en internet* [trabajo final de grado, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas]. http://www.cefadigital.edu.ar/bitstream/1847939/275/1/TFI%2035-2012%20RIVOLTA.pdf

Robin, J., Rosana H., Celeste Q., & Soledad R. (2013). Vigilancia tecnológica: Directriz para el éxito organizacional. Descripción y contribuciones de una disciplina orientada a la eficiencia de las organizaciones de base tecnológica. *Ciencia y Tecnología, 1*(13). https://doi.org/10.18682/cyt.v1i13.64.

Robbins, C., & Mercy Corps. (2019). *The weaponization of social media*. https://www.mercycorps.org/research-resources/weaponization-social-media

Rodríguez, C. (2019). *No diga fake news, di desinformación: Una revisión sobre el fenómeno de las noticias falsas y sus implicaciones*. https://revistas.upb.edu.co/index.php/comunicacion/article/view/437/311

Rodríguez, I. (2017). El Internet y sus inicios. *Boletín Científico de la Escuela Superior Atotonilco de Tula, 4*(7), Article 7. https://doi.org/10.29057/esat.v4i7.2196

Sánchez, O. (2019). *Donald Trump y las acusaciones de interferencia rusa en las elecciones presidenciales de Estados Unidos de 2016*. 10.

Schwab, K. (2016). The Fourth Industrial Revolution. *World Economic Forum*. https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

Seadle, M. (2020). The great hack (documentary film). Produced and directed by Karim Amer and Jehane Noujaim. Netflix, 2019. 1 hour 54 minutes. *Journal of the Association for Information Science and Technology, 71*(12), 1507-1511.

Semana. (2020). ¿Qué es RT, el medio de comunicación del gobierno ruso? https://www.semana.com/mundo/articulo/que-es-rusia-today/202018/

Suárez, D., & Ponce, E. (2021). Misinformation about Colombia's national strike spreads online and on air. *Medium*. https://medium.com/dfrlab/misinformation-about-colombias-national-strike-spreads-online-and-on-air-9c754666c06

Swedish Civil Contingencies Agency (MSB). (2019). *Countering information influence activities: A handbook for communicators*. https://www.msb.se/RibData/Filer/pdf/28698.pdf

Timberg, C., & Stanley-Becker, I. (2020). Cambridge Analytica database identified Black U.S. voters as ripe for 'deterrence,' British broadcaster says. *The Seattle Times*. https://www.seattletimes.com/nation-world/cambridge-analytica-database-identified-black-voters-as-ripe-for-deterrence-british-broadcaster-says/

Torres, M. (2017). *Hackeando la democracia: Operaciones de influencia en el ciberespacio*. Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO66-2017_Hackeando_democracia_MRTorres.pdf
Winston, J. (2017). How the Trump Campaign Built an Identity Database and Used Facebook Ads to Win the Election. *Medium*. https://medium.com/startup-grind/how-the-trump-campaign-built-an-identity-database-and-used-facebook-ads-to-win-the-election-4ff7d24269ac