Capítulo 2

Narrativas y operaciones de información: una mirada al contexto ciberespacial de la guerra híbrida*

DOI: https://doi.org/10.25062/9789585377882.02

Gabriel Andrés Jiménez Almeira
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo tiene por objeto identificar las particularidades de las operaciones de información en el contexto ciberespacial desde la guerra híbrida, como sitio idóneo para materializar características estratégicas que sobrepasan lo tangible y convencional. Con tal propósito, se emplea un método de investigación analítico-descriptivo a fin de desentrañar desde la teoría de la estructuración, la particularidad de las amenazas y retos que se producen por la manipulación de la información, la confusión, el engaño y la tergiversación tendientes a perpetuar la incertidumbre social recurrente. Se concluye que en el escenario ciberespacial, la comisión de delitos y la dificultad de atender sus desafíos aumentan cada vez más en razón del anonimato, la interconexión e incluso la censura.

Palabras clave: amenazas; ciberespacio; conflicto; guerra híbrida; operaciones de información.

* Este capítulo presenta los resultados del proyecto de investigación "La guerra asimétrica, híbrida e irrestricta: Retos, amenazas y desafíos para los Estados, la seguridad y defensa regional", del grupo de investigación "Masa Crítica", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como A1 por MinCiencias y con código de registro COL0123247. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Gabriel Andrés Jiménez Almeira
Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Internacionalista, Universidad del Rosario, Colombia. Orcid: https://orcid.org/0000-0003-4867-0073 – Contacto: jimenez@esdeg.edu.co

Citación APA: Jiménez A., G. A. (2022). Narrativas y operaciones de información: una mirada al contexto ciberespacial de la guerra híbrida. En T. L. Fonseca-Ortiz & P. A. Sierra-Zamora (Eds.), *Guerras irrestricta e híbrida en los desafíos a la seguridad y defensa nacionales* (pp. 23-40). Sello Editorial ESDEG. https://doi.org/10.25062/9789585377882.02

Guerras irrestricta e híbrida en los desafíos a la seguridad y defensa nacionales
ISBN impreso: 978-958-53778-7-5
ISBN digital: 978-958-53778-8-2
DOI: https://doi.org/10.25062/9789585377882

Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2022

Introducción

El actual avance tecnológico obliga una rápida adaptabilidad de las organizaciones criminales internacionales que comienzan a utilizar los nuevos espacios de comunicación como el ciberespacio para llevar a cabo sus actos. Los Estados y otros actores del sistema internacional (SI) deben adaptarse también al ciberespacio, como un nuevo territorio por proteger, y prepararse ante la posibilidad de que las herramientas del Estado, tales como páginas o inteligencia guardada por medio de nueva tecnología, sean amenazadas por estos actores. Si estos se hallan más especializados que los actores legales del SI y cuentan con mejores estrategias, esto puede significar una situación de peligro para el Estado que se vea enfrentado a tales actores en cuanto a sus alcances en seguridad y defensa.

La guerra híbrida (GH) ha sido una de estas situaciones que se ha visto transformada por el avance y el crecimiento de la influencia de ciberespacio. En la actualidad, la mayoría de los conflictos no se lleva a cabo en el ambiente físico, debido a que por muchos años la especialización se ha dado en este terreno, mientras que el ciberespacio es un territorio mucho más inexplorado y con mayor alcance en cuanto a la facilidad que presenta para atacar estructuras de manera rápida sin encontrarse en el territorio de esta estructura. La información se ha convertido en un arma que puede ser manipulada, analizada y utilizada en ataques en el ciberespacio, para socavar las estructuras construidas alrededor de estos conocimientos y lograr un combate completo entre las especialidades tecnológicas de diversos países, en el cual el actor con menos especialización sería el más perjudicado al momento de entrar en la batalla y, a su vez, perdería posicionamiento en el SI (Schmidt, 2014).

Debido a la rápida evolución del ciberespacio, el SI no ha sido lo suficientemente ágil para legislar frente a lo que allí sucede. La falta de conocimiento y de

reglamentación frente a lo que ocurre en el ciberespacio hace que los actores criminales internacionales obren en este sin mayores consecuencias, ya que la facilidad de encriptar la información y la comunicación y la de eludir el mapeo de la ubicación de los servidores ayudan a engañar a las estructuras que buscan evitar el crecimiento de estos grupos, al hacerles triangular la ubicación de la comunidad en zonas comúnmente alejadas de las reales. El conocimiento del ciberespacio y de sus niveles permite que haya comunidades enteras llevando a cabo acciones al margen de la ley, de manera completamente anónima y segura, debido a la protección que se ofrece en estos espacios y a la falta de legislación de los Estados frente a los mismos (Reguera, 2015).

Al ser el ciberespacio un lugar tan poco reglado, no son solo el crimen organizado transnacional (COT) o los grupos de jáqueres mundiales quienes presentan un peligro para los Estados y para la ciudadanía misma; también grandes empresas mundiales de tecnología han sido descubiertas llevando a cabo acciones al margen de la ley con la información que obtienen de las personas que usan sus servicios. Situaciones como la de Cambridge Analytica —que ofreció la información de sus usuarios para la creación de un algoritmo dirigido a informar a las personas con noticias y artículos específicos según sus posiciones y que llevó al crecimiento de comunidades como la antivacuna y la terraplanista y que incluso llegó a influir en situaciones de política internacional como las elecciones presidenciales estadounidenses de 2016 y el referendo Brexit del mismo año— señala la importancia de la información y de la seguridad de la misma en el entorno internacional actual (Isaak & Hanna, 2018; Lykhova, et al., 2022).

En el escenario de la guerra híbrida

El desarrollo y la conducción de la guerra (Fonseca-Ortiz, et al., 2022) son dos escenarios que se han articulado en los planeamientos estratégicos del Estado como un sumario unificado para la acción (que puede tener como final la victoria o la derrota). Sin embargo, son varios los procesos y procedimientos que aqueja llevar a cabo la guerra *per se*. En ese contexto, se han contemplado diferentes variables que condicionan el desenlace de una confrontación o la evolución de esta (que para la pertinencia del presente texto será tomada como referencia).

Los nuevos escenarios donde se desarrollan las guerras y los conflictos han estado marcados por los distintos campos de lucha: político, militar, cultural, económico y social. Esto ha permitido avanzar en distintos paradigmas en el

abordaje de los estudios de la guerra, abriendo así la visión de recrear diferentes escenarios donde los Estados deben atacar las dinámicas desestabilizadoras. Por esto, en los estudios sobre la *evolución de la guerra* se ha podido avanzar hacia la construcción de lo que la academia en los últimos cinco años ha llamado las *tipologías generacionales de la guerra*. En estas tipologías, se destacan tres ejes. El eje A: donde se encuentran los nuevos escenarios de la guerra; el eje B: donde se analiza la naturaleza cambiante del adversario, y el eje C: donde se establecen y priorizan los objetivos de las guerras. Estas tipologías han permitido entender cómo evolucionan las guerras en un campo de batalla o teatro de operación cada vez más cambiante por las nuevas dinámicas criminales de los grupos armados organizados y grupos delincuenciales organizados.

Otra forma de analizar las tipologías generacionales de la guerra es lo que Artelli y Deckro (2008) llaman *los instrumentos y las dimensiones*, los cuales han categorizado las confrontaciones armadas de carácter internacional y no internacional en diferentes generaciones en que el SI ha incurrido.

Por un lado, han recreado las guerras de primera y segunda generación que se distinguen por "la tecnología y la capacidad económica afrontando un espacio unidimensional" (Álvarez et al., 2018, p. 180). La de tercera generación se da por la inclusión de otras dimensiones armonizando un entorno tridimensional que abarca tierra, aire, mar y cibernético. La de cuarta generación "expande la guerra más allá del campo de batalla tridimensional, de carácter físico, hacia el escenario político" (Álvarez et al., 2018, p. 192). Estos autores señalan que durante los últimos cinco años se ha moldeado el camino para empezar a dimensionar las guerras de quinta generación, pues ha podido verse cómo los componentes del espacio exterior, la información cibernética y los dominios políticos constriñen el comportamiento de los nuevos actores del SI (Álvarez et al., 2018).

En la cuarta generación de la guerra y la propuesta de quinta puede establecerse lo que hoy se conoce como *guerra híbrida* (GH). Entre las características de la de cuarta generación logra verse cómo los grupos armados organizados (GAO) y grupos delincuenciales organizados (GDO) transforman sus métodos de lucha y combate, articulándolos con acciones tecnológicas, razón por la cual han obtenido una mayor incidencia dentro de los conflictos armados no internacionales (CANI).

A parte de la experiencia de esta generación se ha abierto el espacio para hablar de las guerras de quinta generación (como se nombró anteriormente), donde las dimensiones cognitiva e informática, enlazando los dominios políticos,

han traído como resultado la formación de nuevos combatientes y estrategias de lucha irregular (Miron, 2019). La era de la información, los datos, las redes sociales y las interacciones del ciberespacio han profundizado aún más el teatro de operación o el campo de batalla.

Por esta razón, se ha configurado un nuevo concepto dentro de las tipologías de la guerra: la guerra híbrida. Este concepto ha puesto sobre los estudios de seguridad y defensa aspectos relevantes que antes no se contemplaban. Las situaciones de peligro o amenaza son un factor determinante dentro de este nuevo contexto de la guerra.

Para el Departamento de Defensa de los Estados Unidos de América (United States Department of Defense [USDOD], 2005) "la guerra híbrida es la combinación de dos o más amenazas de tipo tradicional (convencional), irregular, catastrófico o disruptivo" enfatizando en que los problemas del futuro estarán determinados por los procesos disruptivos en los Estados. Asimismo, Hoffman (2007, p. 29) establece que "la guerra híbrida mezcla la letalidad del conflicto estatal con el fanatismo y fervor prolongado de las guerras irregulares" y también que "la guerra híbrida incorpora un rango de diferentes modos de combatir incluyendo capacidades convencionales, formaciones y tácticas irregulares, actos terroristas, incluyendo violencia indiscriminada, coerción y desorden criminal", situación presentada con mayor claridad desde el desenlace de la Primavera Árabe con la proliferación de nuevos actores (o agentes) armados ilegales que combinan tácticas irregulares de lucha y que, por su carácter *spill over,* ha permitido vincular (o conectar) métodos y tácticas terroristas a un espacio latinoamericano influenciado por movimientos revolucionarios guerrilleros en varios países de la región.

Nuevos actores o agentes de la guerra híbrida

Las guerras híbridas son un fenómeno relativamente nuevo en el contexto de las confrontaciones internacionales. Aunque en los últimos años los conflictos entre Estados han disminuido de manera significativa, los medios de comunicación y la sociedad en general parecen renuentes a identificar dichos conflictos entre Estados y con otros actores ilegales como *guerras*, ya que estas parecen requerir un nivel de especialización y reconocimiento que no se alcanza con facilidad. Es ahí donde el dominio del ciberespacio entra en juego de manera definitiva, pues aunque un actor criminal carece del alcance, armamento y entrenamiento que en cambio sí tienen los Estados al momento de enfrentarse, el ciberespacio

no solo parece ser un terreno más fácilmente transitable para estos grupos, sino que también permite que los enfrentamientos en las GH sean, si no entre iguales, sí lo suficientemente estratégicos y cercanos como para que tales conflictos no puedan ser terminados con rapidez.

Uno de los mayores desafíos que tienen los Estados hoy son los riesgos residuales desprendidos de los conflictos armados no internacionales, donde la variedad de delitos trasnacionales comienza a tomar un rol desestabilizador para las instituciones y pone en jaque las estructuras sociales del Estado. Los principales riesgos son: el crimen organizado trasnacional, el tráfico de armas, el tráfico de flora y fauna, la trata de personas, el narcotráfico, la minería ilegal, la explotación de recursos estratégicos de manera ilegal, el contrabando y los delitos financieros que se encuentran en el sector bancario; es allí donde el ciberdelito toma relevancia para las estructuras ilegales y sus procesos de financiación del terrorismo. Estos riesgos han hecho que los países tengan que priorizar sus amenazas dentro de la estrategia nacional de seguridad y defensa, permitiendo que se establezcan parámetros para la anticipación de escenarios de vulneración o amenaza a la seguridad nacional (Nizovtsev, et al., 2022).

Con el avance de la tecnología y el aumento de la interconexión mundial propia de la globalización, el alcance de los grupos ilegales y la amenaza que representaban para otros actores del SI crecieron de manera inusitada. Así, el ciberespacio se convierte en el principal ámbito en que se lleva a cabo la financiación de estos grupos, y aunque en un momento dado no se esté utilizando para realizar las acciones ilegales, los fondos tienden a ser encriptados y movilizados en dicho ámbito hasta llegar al grupo al que pertenecen. El desconocimiento de este espacio y de las maneras como la información puede viajar allí se ha vuelto una debilidad de los Estados, así que complejizar el proceso para asegurar el continuo flujo de fondos se ha convertido a su vez en parte de la estrategia para desarrollar los conflictos híbridos de la actualidad, por lo cual enfrentarse a estos y crear estructuras y estrategias efectivas para llevar a cabo el conflicto se han convertido en claras debilidades en este tipo de guerras (Reichborn-Kjennerud & Cullen, 2016).

Una de las acciones desarrolladas por los Estados para garantizar su seguridad y mantener controlados a los grupos criminales que consideran una amenaza ha sido monitorear el ciberespacio y mantener filtros de diversos tipos, cuyo objetivo es disminuir o evitar de manera completa el ingreso de personas con cierto perfil, haciendo uso de códigos y *firewalls* para proteger de mejor manera

sus estructuras virtuales e identificar y localizar a los atacantes. Aun así, cada vez es más difícil descubrir exactamente en qué lugar del mundo se encuentra un jáquer, ya que mientras la población civil ha comenzado a usar VPN (*Virtual Private Network*, red privada virtual) para esconder su localización y tener acceso a páginas o contenido en otros lugares del mundo, los jáqueres han llegado a ser capaces de saltar de servidor en servidor, haciendo imposible triangular su ubicación exacta, o de hacer uso de un dispositivo remotamente para no dejar rastros de su presencia en el lugar de origen de la señal para los sistemas de seguridad (Bahari & Azar, 2018).

En un principio, la facilidad de conectar con diferentes regiones del mundo, junto con el relativo anonimato del ciberespacio, hizo que este se convirtiera en un lugar para reclutar nuevos miembros para las organizaciones ilegales. Con el pasar del tiempo, se fueron creando espacios virtuales, como blogs y chats dentro de los cuales se probaría a los posibles candidatos y, eventualmente, se llevarían estas conversaciones a lugares del ciberespacio más privados para hablar de temas más específicos de la organización y planear acciones para demostrar la presencia del grupo en diferentes regiones del mundo. Esto normalmente ocurría una vez el grupo ya era más conocido por los esquemas de seguridad de los Estados, pero su alcance aún no era tan claro; el ciberespacio ha permitido que muchos grupos ilegales lleguen a regiones donde antes no habrían tenido influencia. La creación de comunidades en internet y el darles un sentido de pertenencia a sus miembros, incluso mediante una pantalla, aseguraron el éxito del aspecto visual de estos grupos armados (Payá & Delgado, 2016).

Otra manera en que las amenazas híbridas hacen uso del ciberespacio para llevar a cabo sus movimientos dentro de las GH son las llamadas *guerras psicológicas*. En estas se usan las comunidades virtuales para reclutar a los nuevos miembros de la organización, y aun si no se logra reclutar a todos los individuos en la comunidad, se utilizan propagandas y discursos para ganar los corazones de estas personas y convencerlas de estar a favor de la organización, aunque no hagan parte de ella.

Aunque la guerra psicológica ha sido parte importante en toda las guerras de la historia, en la actualidad, con la interconexión y el poder que cada individuo posee debido a la posibilidad de crear una opinión propia haciendo uso de las herramientas de información dadas por la globalización, dicha guerra psicológica no es más que otro matiz de las GH actuales en que se hace uso de herramientas

sociales, políticas y económicas para ganar apoyo y tener un mejor posicionamiento frente a la población civil al momento de llevar a cabo un ataque a una estructura del SI (Sánchez, 2014).

No todas las acciones de grupos ilegales en el ciberespacio se llevan a cabo en zonas protegidas o secretas tales como la *Deep Web* (internet profunda, invisible u oculta). Algunos de estos grupos toman acciones en redes sociales como Twitter, Facebook o Reddit, lugares donde las personas tienden a compartir sus opiniones de manera indiscriminada. Los grupos ilegales internacionales hacen uso de estos espacios, y del mismo algoritmo de estas redes sociales, para incentivar ciertos pensamientos en las personas más fácilmente influenciables y cuyo *feed* (flujo de contenido) ya se encuentra de alguna manera contaminado por este tipo de ideas, así que el algoritmo queda establecido para enviar este tipo de información.

Los algoritmos de estas plataformas están diseñados para proveer a sus usuarios el contenido más similar a lo que por búsquedas previas les interesa, lo que permite que estos grupos puedan perseguir a estas personas sin llamar la atención de otras comunidades de internet, ya que el algoritmo también se encarga de ocultar la información que no considera importante para el usuario específico. Esta forma de usar el ciberespacio legal para avanzar en sus objetivos demuestra la especialización que estos poseen y cómo la falta de legislación y control sobre la parte legal del ciberespacio también puede contribuir en el avance de los ideales de los grupos ilegales internacionales en las comunidades virtuales (Cetina & Ramírez, 2019).

Tabla 1. *Actores (o agentes) de la Guerra Híbrida*

Actores estatales	Actores no estatales
Fuerzas Militares (FF. MM.)	Grupos armados organizados ilegales
Fuerzas policiales	Grupos delincuenciales organizados ilegales
Agencias de Inteligencia	Pandillas
Multinacionales	Grupos terroristas
Movimientos sociales	Mafias
Individuo	Carteles

Fuente: elaboración propia

Un aspecto crucial de las GH es que los actores no gubernamentales carecen de las mismas capacidades de sus contrapartes en el conflicto, por lo cual se ven obligados a buscar otras maneras de enfrentarse a los Estados o a las estructuras que quieren cambiar, sin exponerse a grandes pérdidas cada vez. Por esta razón, los actores presentan una amplia adaptabilidad y buscan estrategias con las cuales atacar las estructuras de su enemigo, sin tener que enfrentarse directamente con ellos. Es entonces cuando el ciberespacio toma un papel importante en las dinámicas de este tipo de guerras, ya que por medio de este los actores evitan muchos de los posibles enfrentamientos directos, además de generar una dinámica de poder dentro de la cual los actores legales deben evolucionar de manera rápida para protegerse de estos ataques. Acerca del ciberespacio y de las nuevas tecnologías, los actores ilegales del sistema tienden a ser más eficientes al momento de adaptarse y crear estrategias para usarlos en sus propósitos y ganar terreno en el conflicto (Bartolomé, 2019).

En consecuencia, es posible entender las razones por las cuales los grupos ilegales del SI tienden a acumular mayor especialización y control en cuanto al ciberespacio, contando incluso con la participación de personas con mayor conocimiento acerca de este sistema en el mundo, logrando así avanzar en sus objetivos y llevando a cabo demostraciones significativas para llamar la atención de la población y ganar apoyo, lo cual se relaciona con el nivel de poder por alcanzar, lo que de alguna manera permitirá una ventaja en cuanto al contexto de la GH y la manera en que esta funciona frente al SI.

Tabla 2. *Métodos y tácticas de acción de los actores de la guerra híbrida*

Método	Acción
Blurring	Difuminación de los marcos entre los que se desarrolla la guerra, hasta el punto de que estos desaparecen.
Alineación de los niveles de la guerra	Sincronización hacia un fin estratégico de amplio alcance.
Objetivo sociopolítico	El objetivo ya no es forzosamente el territorio nacional o las fuerzas armadas, sino el núcleo del sistema sociopolítico del adversario.
Ruptura de la cohesión social	Desconexión entre el liderazgo político, el ciudadano y las fuerzas de seguridad.

Método	Acción
Revolución molecular disipada	La acción militar es subsidiaria de las acciones en otros ámbitos o dominios. Ya no será el elemento fundamental de decisión y se desvanece la utilidad práctica del concepto *batalla decisiva*.

Fuente: elaboración propia con base en Quiñones (2020)

Narrativas y la teoría de la estructuración

El concepto de *narrativa* se refiere a una historia sobre un evento o eventos que tienen una trama con un punto de partida y un punto final claros, proporcionando coherencia secuencial y causal sobre el mundo o la experiencia de un grupo. Algunos eruditos sugieren que este concepto representa una metáfora de raíz ideal para la psicología en su capacidad para tender puentes entre los niveles de análisis. Dado este marco, las narrativas son analizadas en dos niveles. A nivel individual, son historias de vida que proporcionan significado, coherencia y propósito para el curso de la vida de una persona. En el nivel colectivo, las narrativas son conceptos sociales, estructuras que interrelacionan coherentemente una secuencia de eventos teóricos y actuales, cuentan experiencias colectivas de la comunidad, encarnadas en su sistema de creencias, y representan el simbolismo del colectivo, la identidad compartida construida (Banasik, 2015).

Agente-estructura

La consecuencia de la modernidad, de Antony Giddens (1993), ayuda a entender la implicación e incidencia que tenían los "canjeables" dentro de las relaciones sociales del Estado, mostrando una construcción entre agentes y estructura. El concepto de *agente* se entiende como actores sociales que se movilizan dentro de una estructura social determinada por los recursos y las reglas. Y la estructura es una conformación dada por el establecimiento de una administración política de un Estado, quien ejerce las reglas y constriñe el comportamiento de los agentes (Giddens, 1993).

La visión *agente-estructura* se afianza en el constreñimiento que brinda la fuerza de negociación del Estado ante un grupo insurgente (Plakoudas, 2019) y la facilidad que tiene el agente de poder transformar sus métodos y metodologías de lucha ante dicho constreñimiento en búsqueda de una afectación al desarrollo del Estado.

Esta idea da a entender que la utilización de la estrategia de los "canjeables" hacía evidente un deseo por cambiar la estructura del Estado, al poder aprovechar un cambio de las reglas de juego en búsqueda de poner en un estado de desequilibrio las diferentes políticas públicas de seguridad y defensa (Sierra-Zamora et al., 2020).

Relación estructural

La teoría constructivista dentro de las relaciones internacionales ha podido consolidar aspectos que otras teorías como la realista y liberal no han podido. Mientras que estas se enfocan en conceptos como poder, seguridad, cooperación, estructuras unipolares, bipolares y multipolares, el constructivismo, desde su nivel de análisis, interpreta las interacciones de la arena internacional a partir de las acciones sociales que allí se presenten. Por esta razón, dentro de los axiomas principales podemos encontrar conceptos como ideas, identidad, valores, reglas, procesos, procedimientos, agentes y estructuras.

Estos conceptos, que terminan siendo variables de la teoría constructivista, permiten entender los cambiantes escenarios del SI y su estructura *per se*. Las interacciones sociales que allí se presentan entre agentes (Estados, organizaciones, empresas e individuos) y estructuras (regiones, comunidades, grupos o asociaciones) están caracterizados por el resultado social que se desprende de la relación que se presente. Por ello, la construcción social de individuos, grupos o Estados estará dada por los procesos y procedimientos que se derivan de una relación constante entre actores.

Narrativas y operaciones de información

Una de las armas más utilizadas en el contexto de las GH en el sistema internacional es la información. Con el avance de la tecnología, mucha información pasó a ser protegida en el ciberespacio mediante una multitud de estrategias de defensa y protección. Toda la información que la población civil somete a las diferentes plataformas de internet para acceder a muchos de los servicios cuenta, a su vez, con cierto nivel de protección, demandado por una de las pocas legislaciones existentes acerca de la protección de la información y las estructuras de seguridad necesarias. Sin embargo, en muchas ocasiones, la información no se encuentra completamente protegida, debido a la falta de especialización de las personas que construyen los sistemas de seguridad o de conocimiento por parte de las estructuras que buscan la

protección de esta información al no comprender de manera completa cómo estos sistemas de protección funcionan o decodifican la información para asegurarla.

Cada empresa con presencia en el ciberespacio hace uso de información para llevar a cabo sus objetivos, sea información corporativa o información personal de sus empleados y usuarios. La información se vuelve, de alguna manera, moneda de cambio por medio de la cual se busca extender el alcance de las empresas en el ambiente legal. La venta de información se ha normalizado de tal manera que es de conocimiento público que una red social vende su algoritmo y la información que este consigue para enfocar los comerciales que le aparecen a cada persona tomando en cuenta sus intereses o cómo de una red social a otra pueden aparecen tiendas o comercios de los cuales se buscó. La falta de legislación al respecto ha permitido que estas situaciones ocurran, ya que en industrias que manejan información comúnmente conocida como *sensible*, como la financiera, la legislación es mucho más fuerte que la utilizada para las empresas de comunicación, ya que en un principio no se consideraba que los perfiles de una persona en una red social pudieran ser utilizados de alguna manera. Cosa que unos años después causó uno de los desastres por venta de información más importantes de la historia, donde la falta de legislación permite la manipulación de la información y las noticias de las personas (Lanier, 2018).

Tabla 3. *Tácticas defensivas de la guerra de redes sociales*

Autovalidación	Asegurar al mundo la validez y legitimidad de una posición.
Influencia en entidades alineadas	Convencer a los aliados de la validez y legitimidad de una posición o una acción.
Reforzamiento de alianzas	Mostrar apoyo de la posición o acción de un aliado.
Persuasión de entidades no alineadas	Convencer a los no aliados de la validez y legitimidad de una posición o acción.
Reclutamiento y adoctrinamiento	Atraer a las personas hacia una causa y enseñar la causa o doctrina relacionada.
Creación de relaciones	Establecer esfuerzos cooperativos con personas y organizaciones.
Anulación de oponentes	Realizar esfuerzos para desacreditar a los oponentes.

Fuente: elaboración propia con base en Erbschloe (2017)

Tabla 4. *Tácticas ofensivas de la guerra de redes sociales*

Engaño	Falsas promesas e información inválida.
Confusión	Crear y perpetuar la incertidumbre.
División	Instigando el odio y la sospecha.
Exposición	Liberación no autorizada de información.
Trolling	Publicar mensajes opuestos a los mensajes existentes.
Creación de relaciones	Establecer esfuerzos cooperativos con personas u organizaciones con ideas similares.
Anular a los oponentes	Esfuerzos para desacreditar a los oponentes.
Amenazas combinadas	Actividades combinadas para lograr objetivos ofensivos.

Fuente: Erbschloe (2017)

La rapidez con que viaja la información en la red y la manera en que las redes sociales permiten que cada persona presente un hecho y dé su opinión y perspectiva acerca del mismo, creando su propia percepción de lo sucedido, propician que una parte u otra gane más apoyo frente a dicha situación. Por esto, el control de la información, junto con la propaganda establecida y popularizada frente a diferentes situaciones, se ha convertido en una parte esencial de cualquier conflicto actual. Aun si estos no se llevan a cabo de ninguna manera en el ciberespacio, con estas situaciones se ha visto un aumento en la censura de la información, dentro de la cual, incluso sin legislación presente, se esconden o eliminan historias, videos, fotos o perfiles que no concuerdan con la narrativa popular del actor con más poderío sobre la situación, normalmente el Estado. Aun con esto, la globalización y la existencia de redes sociales permiten la comunicación rápida lo que hace que las acciones dentro de las GH tiendan a tener una audiencia continua y una percepción creada (Cano, 2007).

En la actualidad, muchos países han pasado de considerar innecesarios los sistemas de ciberseguridad y de ciberdefensa (Cujabante et al., 2020) a considerarlos unos de los elementos más importantes en cuanto a las estrategias de seguridad y defensa de un país, ya que la amenaza ya no solo se

encuentra en que las páginas gubernamentales dejen de funcionar, sino que ahora, con el avance y la especialización de las amenazas híbridas, la información confidencial de los Estados, las estructuras virtuales e incluso los bienes financieros virtuales que un espacio pueda poseer se encuentran en peligro. Con la tecnología avanzando y la vida entera de una persona dejando marca en el ciberespacio es fácil para las amenazas híbridas estudiar cómo un sistema gubernamental funciona, sus horarios y estructuras y atacarlos de una manera lo suficiente efectiva como para crear un efecto longevo dentro del esquema de la institución. Estos ataques en muchas ocasiones no son llevados a cabo con el fin único de atacar la institución, sino como parte de una estrategia más grande para controlar la manera en que la información es trasladada entre herramientas del Estado para llevar a cabo una acción más grande (Jang-Jaccard & Nepal, 2014).

Lo anterior se refiere a estrategias de recolección de información y movimientos, mediante las cuales se van traspasando poco a poco los esquemas de seguridad de un Estado o de una institución, identificando los lugares en que la información más importante es almacenada y los movimientos que esta institución tiene, con el objetivo de proteger esta seguridad. Después de un tiempo, la organización ilegal ya es parte de este sistema y tiene el suficiente conocimiento y experiencia para pasar los esquemas de seguridad y acceder a la información sin mayor problema. En algunas ocasiones, se ha visto cómo la información es almacenada, estudiada y analizada con el fin de llevar a cabo acciones decisivas para el conflicto, mientras que en otras, la información es dejada al público, con lo cual se crea un escándalo mediático, ya que la información normalmente publicada tiende a ser sobre escándalos políticos o financieros en que figuras importantes del SI se encuentran involucradas (Ghernetti-Hélie, 2010).

Los actos anteriores son normalmente utilizados a manera de distracción, haciendo que los medios de comunicación se enfoquen en los hechos escandalosos de la información publicada, en vez de en alguna acción, menos importante, que el grupo ilegal está llevando a cabo. También existen las situaciones en que estos escándalos tienen un matiz mucho más geopolítico con los que se busca romper de alguna manera relaciones entre actores del SI o generar desconfianza entre estos para evitar posibles uniones que podrían amenazar la existencia y la subsistencia del grupo ilegal. El ciberespacio puede, como se ha visto, ser el terreno por el cual un conflicto híbrido se lleva a cabo en su totalidad y permite, a su vez, una mayor participación de otros entes del sistema que

aun si no hacen parte del conflicto, se encuentran presentes para presenciarlo (Obermaier & Obermayer, 2016).

Otro factor que causa que algunos conflictos híbridos se lleven a cabo casi totalmente en el ciberespacio aparece en los actores ilegales que no cuentan con presencia en el mundo físico, a quienes el anonimato del ciberespacio, junto con la organización y la especialización de los espacios dentro del mismo y la forma en que este funciona les permite llevar a cabo acciones en contra de múltiples actores del SI, sin enfrentarse a consecuencias. Grupos como Anonymous, una comunidad virtual de jáqueres alrededor del mundo, cuyo único punto de referencia es su mayor propaganda, la máscara y la voz virtualizada como símbolos, sus integrantes hacen uso del ciberespacio para mantener su completo anonimato y volverse una amenaza sin rostro para los actores a quienes la organización decida enfrentarse. Este tipo de conflicto solo es posible gracias a lo que es el ciberespacio intrínsecamente y a cómo, a pesar del avance y de los intentos por legislar, se mantiene un espacio libre de barreras y al que todos tienen acceso (Olson, 2013).

Conclusiones

Las guerras híbridas han ganado alcance global y se han posicionado como una amenaza real para los actores del sistema internacional en gran parte gracias a la existencia del ciberespacio y a la facilidad para los actores ilegales de ganar especialidad en este y de crear comunidades cerradas y anónimas dentro del mismo. La corrupción del ciberespacio, con la existencia de espacios como la *Deep Web*, ha permitido a su vez que el financiamiento de estos grupos ilegales pueda ser llevado a cabo sin llamar la atención de los entes financieros, ya que estos fondos son encriptados y depositados en diferentes cuentas alrededor del mundo, ubicadas en países comúnmente conocidos como *paraísos fiscales*, donde la entrada de grandes sumas de dinero no es cuestionada y puede después ser sacada y trasladada a la ubicación real del grupo ilegal, para continuar su financiamiento y seguir con sus acciones. Sin la existencia del ciberespacio, los grupos híbridos ilegales y los conflictos híbridos que llevan a cabo no serían tan eficientes o conocidos mundialmente, lo que hace del ciberespacio intrínsecamente el terreno en que las guerras híbridas se llevan a cabo.

Referencias

Álvarez, C., Santafé, J., & Urbano, O. (2018). *Metamorphosis Bellum:* ¿mutando a guerras de quinta generación? En C. Álvarez (Ed.). *Escenarios y desafíos de la seguridad multidimensional en Colombia*. (pp. 145-247). Libros Escuela Superior de Guerra. https://n9.cl/c7dlh

Artelli, M., & Deckro, R. (2008). Fourth generation operations: Principles for the 'Long War'. *SmallWars&Insurgencies,19*,221-237.https://doi.org/10.1080/09592310802061372

Bahari, R., & Azar, D. (2018). Operation of Monitoring the Cyberspace of the Army of the Islamic Republic of Iran in Hybrid Warfare. *Military Science and Tactics, 14*(45), 53-74. https://n9.cl/c7dlh

Banasik, M. (2015). How to understand the Hybrid War. *Securitologia, 1*(21), 19-34. https://doi.org/10.5604/18984509.1184214

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (25), 8-23. https://doi.org/10.17141/urvio.25.2019.4249

Cano, J. L. (2007). *Business Intelligence: competir con información*. Banesto, Fundación Cultural.

Cetina, R., & Martínez, J. (2019). Algoritmos y noticias: Redes sociales como editores y distribuidores de noticias. *Revista de Comunicación, 18*(2), 261-285. https://doi.org/10.26441/RC18.2-2019-A13

Cujabante, X. A., Bahamón, M. L., Prieto, J. C., & Quiroga, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. https://doi.org/10.21830/19006586.588

Erbschloe, M. (2017). *Social media warfare: Equal weapons for all*. Auerbach Publications. https://doi.org/10.4324/9781315232072

Fonseca-Ortiz, T. L., Cortés Castillo, D. E., & Cardona Orozco, A. F. (2022). La guerra híbrida e irrestricta en un ámbito de seguridad multidimensional en el posacuerdo en Colombia. *Revista Logos Ciencia & Tecnología, 14*(2), 158–171. https://doi.org/10.22335/rlct.v14i2.1607

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. In *2010 International Conference on Availability, Reliability and Security* (pp. 370-373). IEEE.

Giddens, A. (1993). *Las consecuencias de la modernidad*. Alianza, Universidad.

Hoffman, F. (2007). *Conflict in the 21st Century:* 72. Potomac Institute for Policy Studies. https://n9.cl/c7dlh

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56-59.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Lanier, J. (2018). *Diez razones para borrar tus redes sociales de inmediato*. Debate.

Lykhova, S., Servatiuk, L., Shamsutdinov, O., Sysoieva, V., & Hurina, D. (2022). International and national standards on societal information security. *Revista Científica General José María Córdova, 20*(38), 247-264. https://dx.doi.org/10.21830/19006586.898

Miron, M. (2019). La guerra irregular, insurgencias y cómo contrarrestarlas: Una perspectiva comparativa entre los enfoques centrados en el enemigo y en la población. *Revista Científica General José María Córdova, 17*(27), 457-480. https://doi.org/10.21830/19006586.497

Nizovtsev, Y. Y., Lyseiuk, A. M., & Kelman, M. (2022). From self-affirmation to national security threat: analyzing the Ukraine's foreign expe-rience in countering cyberattacks. *Revista Científica General José María Córdova, 20*(38), 355-370. http://dx.doi.org/10.21830/19006586.655

Obermaier, F., & Obermayer, B. (2016). *The Panama Papers: Breaking the story of how the rich and powerful hide their money*. Simon and Schuster.

Olson, P. (2013). *We are anonymous*. Random House.

Payá, C., & Delgado, J. (2016). El uso del ciberespacio para infringir el terror. *Estudios en Seguridad y Defensa, 11*(22), 91-108. https://doi.org/10.25062/1900-8325.211

Plakoudas, S. (2019). Cómo terminan las insurgencias: En busca de la victoria del gobierno. *Revista Científica General José María Córdova, 17*(28), 923-938. https://doi.org/10.21830/19006586.523

Quiñones, F. (2020). Una revisión del concepto "guerra híbrida/actor híbrido", *Instituto Español de Estudios Estratégicos*. Documento de opinión. IEEE.ES https://n9.cl/c7dlh

Reguera, J. (2015). *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario*. GESI, Grupo de Estudios de Seguridad Internacional, Universidad de Granada, Granada.

Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is hybrid warfare?* Norwegian Institute for International Affairs (NUPI). https://n9.cl/5sae4

Sánchez, G. (2014). Ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI. *Revista Enfoques, 10*(16), 71-87. https://n9.cl/79loy

Schmidt, N. (2014). Neither conventional war, nor a cyber war, but a long-lasting and silent hybrid war. *Obrana a strategie, 14*(2), 73-86.

Sierra-Zamora, P. A., Fonseca Ortiz, T. L., & Mejía Azuero, J. C. (2020). Modernización y reestructuración de la seguridad y defensa nacional: análisis propositivo para una ley de seguridad y defensa en Colombia. En: Sierra y Bermúdez (Eds.), *Evaluación jurídica de la Seguridad y Defensa nacional como política de Estado*, (pp. 247-268). Planeta.

United States Department of Defense (USDOD) (2005). *National Defense Strategy of the United States of America*. Government Printing Office.