EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270
Página web: https://esdegrevistas.edu.co/index.php/rcit

La ciberseguridad y la ciberdefensa frente a los factores de inestabilidad económicos y sociales

Cybersecurity and cyberdefense against economic and social instability factors

Diego Mauricio Quintero Franco

CITACIÓN APA:

Quintero Franco, D. M. (2022). La ciberseguridad y la ciberdefensa frente a los factores de inestabilidad económicos y sociales. *Ciberespacio, Tecnología e Innovación, 1*(1), 41-66.
https://doi.org/10.25062/2955-0270.4767

Publicado en línea: **Junio 30 de 2022**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 41-66)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

La ciberseguridad y la ciberdefensa frente a los factores de inestabilidad económicos y sociales

Cybersecurity and cyberdefense against economic and social instability factors

DOI: https://doi.org/10.25062/2955-0270.4767

Diego Mauricio Quintero Franco
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Entendiendo que el ciberespacio se abre como una oportunidad para mejorar la calidad de vida de los humanos, pero también como la génesis de numerosos riesgos, se hace imperioso el estudio de las estrategias que prevengan, afronten y disminuyan los riesgos devenidos de esta dimensión. Los conflictos sociales, económicos y políticos cuentan con nuevas herramientas que potencializan sus efectos y resultan más amenazantes, por tanto, no se pueden seguir contemplando las variables, los instrumentos y el nuevo dominio del ciberespacio. Así, el presente artículo establece la correlación entre el narcotráfico, el secuestro, la extorsión y la violencia en las protestas sociales, agrupados como factores de inestabilidad socioeconómicos, y la ciberseguridad y la ciberdefensa. Para ello, se examinan las iniciativas que se deberían emprender a nivel nacional para mitigar la potencialización de los factores de inestabilidad desde la Ciberseguridad y la Ciberdefensa, como un aporte para las Fuerzas Militares del país.

Palabras Clave: ciberseguridad; ciberdefensa; factores de inestabilidad

Abstract

Understanding that cyberspace opens up as an opportunity to improve the quality of life of humans, but also as the genesis of numerous risks, it is imperative to study strategies that prevent, confront and reduce the risks arising from this dimension. Social, economic and political conflicts have new tools that potentiate their effects and are more threatening, therefore, the variables, instruments and the new domain of cyberspace cannot continue to be considered. Thus, this article establishes the correlation between drug trafficking, kidnapping, extortion and violence in social protests, grouped as factors of socioeconomic instability, and cybersecurity and cyberdefense. To this end, the initiatives that should be undertaken at the national level to mitigate the potentialization of instability factors from Cybersecurity and Cyberdefense are examined, as a contribution to the country's Military Forces.

Key words: cybersecurity; cyber defense; instability factors

Artículo de reflexión
Recibido: 16 de enero de 2022 • **Aceptado:** 20 de mayo de 2022
Contacto: Diego Mauricio Quintero Franco quinterod@esdeg.edu.co

Introducción

Desde las formas más primitivas de la organización de la humanidad, la preocupación esencial ha sido la supervivencia, como individuos y como grupos. Sin embargo, lo que ayer era considerado como algo amenazante, hoy puede verse como algo menos peligroso o, incluso, con el avance de la humanidad, en especial en su dimensión tecnológica, puede que algún temor particular, ya sea solo parte de la historia *La inseguridad en el ciberespacio es inevitable.* Es peligroso que esta afirmación se convierta en un mantra que consolide la creencia de que la inversión en ciberseguridad es un gasto superfluo (Santamans, 2018)

Así, con el paso del tiempo se ha ido transformando lo que se concibe como amenaza y lo que no y, con ello, se ha transformado el concepto de seguridad, incluyendo en este todos aquellos escenarios que la misma evolución ha abierto como oportunidades, pero que pueden resultar también contraproducentes. En este sentido, desde el surgimiento de la máquina de vapor, hasta el desarrollo de inteligencia artificial, se han modificado las condiciones de vida de los seres humanos, obteniendo resultados tanto positivos como negativos, toda vez que, como se anotaba anteriormente, así como se han abierto un sinnúmero de posibilidades para hacerle más fácil y cómoda la vida a las personas, también se han abierto las puertas para grandes riesgos que hacen pensar en el pesimismo antropológico del que alguna vez habló Thomas Hobbes, entendiendo al hombre como un ser egoísta y malvado (1651).

Desde esta perspectiva de estudio de la naturaleza humana, se ha procurado entender la existencia, proliferación y prolongación de los conflictos sociales, políticos, económicos, étnicos, etc.; empero, es de notarse que el estudio de la conflictividad humana ha de ser multidisciplinar, pues solo integrando los saberes de diversos campos de estudio, se puede entender cuáles son las motivaciones y las agravantes de estos fenómenos sociales, los cuales, indiscutiblemente, ameritan en la actualidad una revisión desde la evolución tecnológica.

Precisamente, ese es uno de los retos de este artículo, exponer la interrelación existente entre los factores que se han hallado como catalizadores de inestabilidad socioeconómica, y la ciberseguridad y la ciberdefensa, entendiendo el impacto que ha tenido la evolución y creciente protagonismo del ciberespacio en problemáticas como el narcotráfico, la extorsión, el secuestro, la violencia en las manifestaciones sociales y las afectaciones a líderes sociales.

En ese contexto de riegos y amenazas, producidos mayormente por la globalización, se sitúá el problema de las Nuevas Amenazas o Amenazas-No Convencionales (Chillier, 2005) Cuando un militar investiga respecto de las implicancias que las nuevas tecnologías (y en particular las tecnologías de la información y las Comunicaciones – TIC-) tienen en las operaciones militares podrá observar que la planificación de operaciones

en el ciberespacio ya no es un tema que se aborda desde un punto de vista teórico (o escolástico), sino que ya hay FFAA que están realizando operaciones en el ciberespacio (Mato, 2018).

Este nuevo escenario apenas comienza a tener un espacio en las preocupaciones del público en general, como efecto de la virtualización de la vida y, aunque ha sido una de las preocupaciones de los expertos en la materia hace unos años, en el país apenas se está integrando esta temática de manera explícita en las políticas públicas, y específicamente en aquellas estrategias de seguridad y defensa nacionales. Así, los escenarios que tradicionalmente se han estudiado, se han limitado a las dimensiones de tierra, mar, aire y espacio.

De esta forma, este nuevo espacio, que se contempla como una herramienta con un doble impacto: positivo y negativo, es la génesis de la construcción de saberes que logran maximizar la potencia de estos tecnificados sistemas de información cuyo uso, infortunadamente, no está restringido para actores violentos e ilegales.

> Finalmente, y en relación al ciberespacio, entendido como el dominio global y dinámico compuestos por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de información (EULATE, 2013, p.16).

En este sentido, es posible entender la *ciberseguridad* como la seguridad de la información en el ciberespacio, en otras palabras, cuando se busca *proteger* la información contenida en el *hardware,* redes, *software*, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o *ciberseguridad* (Medina, 2009)

Este doble impacto se ha materializado como parte del enlace que se genera en un mundo cada vez más globalizado, interdependiente e interconectado, desarrollando canales de información y servicios novedosos y beneficiosos. No obstante, al tiempo, ello ha abierto la puerta para que se desarrollen técnicas que se valgan de los vacíos existentes en ese ciberespacio para sacar provecho de manera ilegal.

En este sentido y, entendiendo que uno de los intereses básicos de los Estados es la supervivencia de su territorio y sus ciudadanos (Pearson y Rochester, 2001), los Estados deben hacer frente a las amenazas que surgen desde esta nueva dimensión.

Así, Colombia, por ejemplo, no ha sido ajena a estos avances y riesgos y, por ende, se puede apreciar en el documento del Consejo Nacional de Política Económica y Social (CONPES) 3701 del 2011, que se incluye la ciberseguridad y la ciberdefensa como preceptos que deben ser objeto de atención estatal. Este documento resulta esencial para entender la concepción del Estado sobre la ciberseguridad y ciberdefensa.

De esa manera, especifica que la Ciberseguridad es la "capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (Departamento Nacional de Planeación, 2011, p. 2).

Por otro lado, detalla que la Ciberdefensa se refiere a la capacidad preventiva que desarrolla el Estado para contrarrestar las amenazas cibernéticas que pueden llegar a tener implicaciones en la soberanía nacional.

Particularmente para Colombia, establecer nuevas dimensiones de seguridad y defensa en un nuevo escenario, resulta ser retador, teniendo en cuenta el contexto conflictivo que diversifica, profundiza y complejiza, los frentes ante los que se debe responder con prontitud y asertividad.

De hecho, los factores que se asumen como productores de inestabilidad son numerosos, pues muchos han surgido y se han fortalecido gracias al conflicto de larga data. Entre estos factores (el narcotráfico, grupos ilegales que ejecutan la extorsión y el secuestro, las manifestaciones que derivan en violencia, y las afectaciones a líderes sociales), se halla una realidad que en la actualidad debe ser evaluada como un elemento catalizador de la violencia y las afectaciones a la legitimidad y legalidad del Estado.

En la era donde la revolución de la información permite a los individuos y a los estados cometer sabotaje, espionaje y otras acciones a una velocidad y escala sin precedentes, la amenaza cibernética se constituye en un factor de vulnerabilidad y pérdida del control en la sociedad moderna que exige rápidas y contundentes medidas para evitar una catástrofe (Porto, 2015).

Por tanto, el objeto es analizar cómo los factores de inestabilidad económicos y sociales se potencializan con las herramientas cibernéticas e impactan la ciberseguridad y ciberdefensa en Colombia. Para ello, se tendrán tres partes: en la primera el lector podrá encontrar una aproximación teórica y conceptual sobre la ciberseguridad, la ciberdefensa y los factores de inestabilidad, pues solo entendiendo adecuadamente cada categoría podrá hallarse la correlación entre estas, teniendo un marco adecuado dado por la teoría conflictualista de Johan Galtung y los Complejos Conflictuales de Guillem Farrés.

Una vez abordada toda la dimensión conceptual y teórica, la segunda parte se encarga de hacer explícita la relación entre los factores de inestabilidad y la ciberseguridad y ciberdefensa, para, en tercer lugar, poder examinar las iniciativas que se deberían emprender a nivel nacional para mitigar la potencialización de los factores de inestabilidad desde la Ciberseguridad y la Ciberdefensa.

Desde esta perspectiva, se busca contribuir a la comunidad académica del país y la región, así como establecer un precedente para la toma de decisiones asertiva y enfocada en este espacio que requiere expertos multidisciplinares que logren administrar lo que ya hay, y prepararse para lo que posiblemente pueda suceder. Sin lugar a duda, es un tema que resulta no solo interesante, sino que su estudio es imperioso en un país y un mundo que ha encontrado otra manera de estudiar, relacionarse, comerciar, pero también de delinquir y amenazar a los individuos y a la sociedad como un todo (Cano, 2008)

Metodología

El diseño se enfoca en un análisis de orden cualitativo, el cual "utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación" (Hernández et al., 2014, p.7), en el que se pretende el entendimiento de los fenómenos que se derivan de los factores de inestabilidad socioeconómicos asociados al conflicto armado interno y a las falencias estructurales del Estado, de cara a la ciberseguridad y la ciberdefensa.

Para ello se propone un análisis documental y del mismo modo, "se propone un alcance correlacional, el cual finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular" (Hernández et al., 2014, p. 93).

Así, para el primer punto se realizará una descripción correspondiente al encuadre conceptual, así como una exposición de la teoría de los conflictos, para enmarcar los lineamientos que guiarán el análisis.

Para el segundo y tercer apartado, se conectará la información recolectada, ejecutando la correlación de variables, que permitirán esbozar los escenarios de inestabilidad en el ámbito ciber, que debe enfrentar el Estado colombiano.

Marco Teórico y Conceptual: Acercamiento a la Ciberdefensa y la Ciberseguridad

Como ya se mencionó, este escenario que se abre en el ciberespacio, merece no solo un reconocimiento minucioso por parte del Estado y sus Fuerzas Militares, sino que, en términos generales, la ciudadanía debe ser sensibilizada frente a los temas concernientes a este, acercándose a temáticas como la ciberseguridad y la ciberdefensa, entendiendo que la virtualización de las actividades cotidianas, se debe efectuar bajo todos los protocolos establecidos para allanar las vulnerabilidades propias del sistema y del desconocimiento de los ciudadanos en el uso de dispositivos conectados a la red.

Por otra parte, las cibercapacidades en el ámbito criminal, resultan facilitadoras en términos de tiempo, energía y riesgos: hay una percepción de reversibilidad de los efectos, el mantenimiento de la criminalidad es menos costosa, ya que observan únicamente cuestiones de actualización/desarrollo de software y porque cuentan con una vida útil extensa, puesto que pueden utilizarse en múltiples ocasiones (Van Puyvelde, 2019).

Así pues, es de anotar que las formas más comunes de comunicación y socialización en la actualidad son vectores de inseguridad, toda vez que los usuarios desconocen la diversidad de formas en las que los ciberdelincuentes usan para robar datos, suplantar identidades, y maximizar el efecto de actividades criminales que hasta hace muy poco se limitaban a ejecutar sus acciones con herramientas tradicionales.

En este sentido, si bien la ciberseguridad es una responsabilidad de expertos que deben garantizar que cada actividad que se desarrolle por algún medio tecnológico interconectado esté blindada de amenazas, la actividad global no se puede desligar del usuario final, pues desde la responsabilidad conjunta y compartida, se puede disminuir la posibilidad de que los sistemas puedan llegar a ser vulnerados, y tanto la cultura como la educación en este tema, debe ser proporcionada por los agentes garantes en todos los niveles, con el fin de minimizar cualquier tipo de afectación.

En este sentido, es menester volver al concepto de ciberseguridad, que constantemente se redefine de acuerdo con los avances de la tecnología, las medidas emprendidas, y las nuevas respuestas por parte de los ciber atacantes. En su acepción más amplia, la seguridad se refiere a la sensación de que se está libre de peligro, y aquel vocablo se ha aplicado a diversos entornos en donde se completa la definición, acompañándole de las características específicas del entorno en el que se busca aplicar.

Para el caso presente, el ciberespacio, entendido según Joaquín Aguirre (2010), como "un espacio que se genera cuando se producen ciertos tipos de comunicación" (p.10), es el escenario al que se adapta el concepto de seguridad. Probablemente, la definición es descomunalmente amplia, pero desde el proceso epistémico que sigue el autor en mención, se denotan unos aportes de relevancia.

En este sentido, Aguirre (2010), indica que la diferencia entre un medio virtual y uno físico en el acto de comunicación, es esencial para poder comprender de manera clara la naturaleza del ciberespacio. Precisamente, apunta que el medio virtual amplía las capacidades de interacción, es decir, de comunicación. Así, el espacio virtual no puede ser visto meramente como un banco de información, sino como una plataforma en la que se pueden dar tres tipos de relaciones:

a) Las relaciones de intercambio de información entre máquinas
b) Las relaciones de intercambio de información entre seres humanos y máquinas
c) Las relaciones de intercambio de información entre seres humanos a través de las máquinas (Aguirre, 2010).

No obstante, advierte Aguirre, no deben asumirse aisladamente, sino que todas, indiscutiblemente, están medidas por las máquinas que facilitan la interacción. Empero, se hace necesario detallarlas, para entender la multidimensionalidad que reviste al concepto de ciberseguridad, pues este debe verse desde la perspectiva antropológica que reconoce el elemento humano y, por otro lado, desde el lado técnico que se encarga de las máquinas y las redes tejidas entre estas.

Así, habiéndose abordado someramente el ámbito al que se aplica el concepto de seguridad, se esboza una de las definiciones más exactas del término, que es aquella construida por la Unión Internacional de Telecomunicaciones (2010):

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno (p.20).

En términos más escuetos, se refiere a la liberación de los actores y las máquinas, de los peligros que se suscitan en el ámbito cibernético.

Por su parte, la ciberdefensa contempla el "conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición" (CARI, 2013, p. 10).

Sin embargo, hay definiciones que amplifican la connotación del término y asignan la responsabilidad a los Estados, entendiendo que, si bien hay amenazas que tienen implicaciones individuales, en conjunto, toda la población, las organizaciones privadas y públicas, y el Estado como un todo, puede verse afectado en su funcionamiento, soberanía y, en general, pueden verse afectados los pilares que lo sostienen. De esta forma, Vargas et al. (2017), hacen la precisión de ello, referenciándolo como la sumatoria de

> las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa (p. 32).

De este modo, se tiene que, si bien hay una responsabilidad en cabeza del Estado, reconociendo este espacio como un escenario de potencial confrontación con otros Estados y actores no estatales, hay un principio de corresponsabilidad en el que se deben incluir a todos los ciudadanos, de manera que se reduzcan las vulnerabilidades.

Si se generan buenos mecanismos de cultura en todos los niveles de la sociedad, se coadyuvará a disminuir que los actores al margen de la ley, que desean obtener ventaja de estas nuevas capacidades que brindan las tecnologías de la información, no lo logren. En especial, se ha entendido que los actores relacionados con los factores de inestabilidad como los que se estudian en el presente documento: narcotráfico, existencia de grupos ilegales dedicados al secuestro y extorsión y violencia en manifestaciones sociales, se valen de toda la información dispuesta en la red, para maximizar sus capacidades.

Precisamente, en ese primer factor de inestabilidad, se ha evidenciado la manera en la que los narcotraficantes han establecido nexos con hackers profesionales para diversificar sus canales de actuación. Por ejemplo,

> La agencia Magal S3 reportó que los sistemas de seguridad habían sido hackeados por una organización criminal que comenzó a usar el puerto para introducir drogas en cargamentos que supuestamente eran plátanos provenientes de Sudamérica. El puerto reforzó sus sistemas de seguridad, pero los criminales no se dieron por vencidos y lograron instalar puentes inalámbricos para irrumpir los sistemas y abrir un acceso directo al sistema operativo. El hackeo permitió a la organización criminal localizar cada contenedor con droga para introducirlo por la llamada "Puerta de Europa". (Baltazar, 2018, párrafo 6).

Ante ello, son varios los escenarios de vulnerabilidad que se disponen a favor tanto de los hackers que contarían con financiación adicional para abrirse camino en el ciberespacio y, en el mismo sentido, se deberían reestructurar las estrategias de combate del flagelo, entendiendo estos nuevos métodos.

En este mismo sentido, la extorsión que, como delito, data de tiempos remotos ha sido adaptada a las tecnologías de cada época para sacar provecho de las víctimas identificadas cuidadosamente. Así, en la era de la información se abren las posibilidades para delinquir, entendiendo que se puede acceder a información especializada de las víctimas, quienes, a su vez, usan con mayor frecuencia medios tecnológicos que pueden resultar en un mecanismo de sobre exposición aprovechado por los cibercriminales.

> Ahora vemos que las extorsiones se dan a través de internet, lo que las vuelve más anónimas, más difícil de encontrar al agresor y a su vez muchas veces nos encontramos frente a un vacío legal para nuevos delitos que van surgiendo a medida que la tecnología va evolucionando. Hay dos aclaraciones que creo pertinentes la primera es los avances de internet no son los culpables de dicha, extorsión, sino el uso que se le da y las personas extorsionadas, o que lastiman socialmente a través del bullying no siempre son chicos u adolescentes, sino que esto también le ocurre a las personas adultas (Vaisenberg, 2014, p. 23).

En términos generales, la ciberextorsión se ha constituido como un delito con unas características diferenciadas, que evidencian cómo el ciberespacio aumenta exponencialmente las oportunidades y las vulnerabilidades de los ciudadanos, las organizaciones y, en términos generales, los Estados.

> El ciberespacio es una tierra muy fértil para cualquier actividad relacionada con el chantaje, ya que todas tienen como objetivo el bien más preciado de la era digital: los datos. Sin gran complejidad técnica, con relativamente poco riesgo, y sin discriminar demasiado a las víctimas, pueden causar daños irreparables. En la actualidad, las técnicas de extorsión se han adaptado a un nuevo medio extraordinariamente versátil: el ciberespacio. En este entorno, los criminales aprovechan la gran variedad de herramientas y recursos existentes en Internet para dar una nueva dimensión a sus actividades de extorsión. El ciberespacio ha modernizado, automatizado y rentabilizado la extorsión, adaptándola a la era digital. En el pasado, el chantaje era personal; ahora, los criminales y los ***hackers*** que intentan sembrar el caos tienen la capacidad de lanzar docenas de campañas de ciber extorsión simultáneas. (Fulwood, 2016, párrafo)

Desde otra dimensión, se tiene que los Estados y, en especial, los que constitucionalmente albergan las características propias de un Estado de Derecho, enfrentan las

vicisitudes propias de la polarización social y política, que hacen parecer incompatibles derechos como el de la movilización, cuando este se ha prestado para afectar la infraestructura crítica de los países.

Así, se ha visto en otras latitudes, específicamente en el Norte de África y en Medio Oriente, cómo las redes sociales y la sociedad de la información ha tenido una injerencia directa en la construcción de imaginarios colectivos que han movilizado a la población con objetivos claros como la deposición de regímenes, y cambios sustanciales en el ámbito socioeconómico.

Empero, como se ha advertido, ello ha derivado en una oportunidad para desestabilizar a los Estados que, en medio de la protección de derechos colectivos e individuales, quedan a merced de la violencia que se suscita desde las movilizaciones sociales, en las que a menudo se ha podido comprobar la intervención de agitadores que ocultan intereses económicos y políticos particulares.

Asimismo, como todas las formas de expresión de la humanidad están inmersas en la gran telaraña que se teje en la red de redes, no es lejana la idea de efectuar manifestaciones por grupos expertos en sistemas, también llamados ***hacktivistas,*** los cuales existen por todos los rincones del planeta, y se apoyan en la tecnología para efectuar las manifestaciones de sus desacuerdos políticos, religiosos o sociales con el gobierno, de forma digital a través de ataques informáticos. Por tanto, desde esta perspectiva también se deben plantear estrategias claras y asertivas para prevenir y afrontar las consecuencias de esta modalidad.

Como es de notarse, todos los factores de inestabilidad que se han esbozado y su relación con el ciberespacio, suponen individual y globalmente un conflicto. Individualmente, cada factor de inestabilidad, en sí mismo, representa un conflicto en el espacio físico y virtual, y en conjunto conforman un complejo conflictual. Así, con el ánimo de plantear una delimitación teórica para el análisis de la ciberseguridad y la ciberdefensa, se plantean los aspectos básicos de la teoría del conflicto de Johan Galtung y el Complejo Conflictual de Guillem Farrés (2012), bajo la premisa que se debe entender la base conflictual de estos asuntos, para poder hallar la relación explícita de las variables que componen cada factor, su potencialización con las herramientas cibernéticas y, por ende, cómo se debe actuar desde el ámbito de la ciberseguridad y la ciberdefensa.

Así, la teoría del conflicto de Johan Galtung, explica la conjugación de variables que lleva a la explosión y escalada de conflictos de diversa índole, en la que el ciberespacio se plantea como un escenario que potencializa las oportunidades y las amenazas que se enmarcan en los conflictos mencionados.

> Partimos con la constatación de que los conflictos aparecen como una constante en la historia de la humanidad. Son, como afirmará este autor, inherentes a todos los sistemas vivos en cuanto portadores de objetivos. En algunas etapas de la historia fueron como la *force*

> *motrice* que contribuyeron a generar verdaderos cambios en provecho del hombre, pero en otras, trascendiéndose a sí mismos y convirtiéndose en violencia (metaconflicto) condujeron hacia la deshumanización absoluta. De ahí su importancia y sentido para la vida y el destino de las personas. De ahí la imperiosa necesidad de conocerlos en su complejidad práctica, en sus lógicas internas y externas, para poder finalmente teorizarlos y sistematizarlos para devolverlos a la realidad en forma de modelos y conceptos accesibles y manejables por la racionalidad humana y así, en la medida de lo posible, contribuir hacer más llevadero nuestro, a veces duro, peregrinaje por el mundo (Calderón, 2009, p. 63).

En este sentido, el autor plantea la conjugación de diversos tipos de violencia (directa, cultural y estructural), que exhiben manifiestamente la existencia de un conflicto. De esta forma, esta teoría podría adecuarse para sustentar la correlación de los factores de inestabilidad asociados al conflicto armado y a las falencias estructurales del Estado, entendiendo que son parte del modelo que permite entender al ciberespacio como un escenario de conflicto frente al que deben desarrollarse estrategias de ciberseguridad y ciberdefensa.

Para Galtung, existen dos átomos del conflicto: la disputa y el dilema. El primero hace referencia a la situación en que dos personas o actores persiguen un mismo fin que escasea y, el segundo, define la experiencia a la que se enfrenta un actor que persigue dos fines incompatibles entre sí y genera su autodestrucción.

Para el caso presente, el átomo que deberá examinarse será el de la disputa entre actores criminales y el Estado, las organizaciones y los individuos, que deben enfrentarse por fines escasos, llevándolos a tener actitudes, comportamientos y contradicciones que buscan la destrucción del otro.

Precisamente, esas acciones se relacionan con la división que hace Galtung de los tipos de violencia: directa, cultural y estructural. No obstante, sus estudios se restringen a un ámbito físico, psicológico y estructural, en el que no se contempla explícitamente la violencia generada desde el ciberespacio. Por ende, se busca aplicar estos principios a las dinámicas subyacentes a la ciberseguridad y ciberdefensa, bajo la concepción que al haber intereses contrapuestos existe, per se, un conflicto[1].

Al identificar la existencia del conflicto se habla de la explosión de algún tipo de violencia, de hecho, para Galtung (1969), es requisito *sine qua non*, que exista tanto una teoría de la paz como una de la violencia, con el objeto de forjar las bases de la teoría del conflicto. Así, identifica la violencia directa, como aquella visible, que se evidencia en el

1 "Para llegar a un concepto de conflicto, Galtung hace un ejercicio de síntesis conceptual producto del análisis y la interacción de diferentes intentos de respuestas o tendencias, que a largo de la historia de la humanidad se dieron los hombres para poder explicarse este fenómeno: Una primera línea de respuestas se enfocan sobre aspectos interiores al ser humano (como el odio). Una segunda línea se concentraba fundamentalmente en la incompatibilidad de objetivos de las partes. La tercera línea se focaliza en el hecho externo de las contradicciones. Marx se centra en las contradicciones intra-sociales" (Calderón, 2009, p. 71).

daño físico de las personas o los bienes. La segunda es la violencia cultural que se manifiesta a través de símbolos, actitudes desafiantes desde una creencia particular, ideas o leguajes. Por último, está la violencia estructural referida a la precariedad de las condiciones básicas de vida de la sociedad. Esta última ha sido usada como herramienta para legitimar los postulados marxistas, no obstante, Galtung aclara que ello es una falacia, pues se omite la ingeniería social que debe ser tenida en cuenta para hallar la violencia intrínseca en los sistemas económico, social, político (Calderón, 2009) y, para este caso, tecnológicos.

Es menester aclarar que no se concibe al ciberespacio como una estructura violenta, como tampoco lo es la social o la política, pero si hay contradicciones y riesgos que degeneran en violencia y potencializan, como se verá los factores de inestabilidad. Efectivamente, Galtung, asume la violencia como la diferencia entre ***lo que hay*** y lo potencial (Galtung, 1969); es decir, desde esta distancia se genera la frustración que lleva a la manifestación explicita de un acto violento que puede referirse a la "destrucción de cosas como presagio o amenaza de la posible destrucción de personas, y la destrucción de cosas muy queridas por las personas denominadas consumidores o propietarios" (Galtung, 1969, p. 3).

Inexcusablemente, esto último se materializa en la expansión y fortalecimiento de los factores de inestabilidad a través del ciberespacio, pues precisamente expone herramientas adicionales que contribuyen a la perpetuación de la violencia en el país, a la destrucción de cosas, personas y bienes apreciados por los individuos y los consumidores, denotándose una clara amenaza a la infraestructura crítica y productiva del país.

Ello se relaciona, precisamente, con la disertación que hace Guillem Farrés (2012) sobre la definición del conflicto, en la que, desde la sociología del poder, diferencia su concepción del fenómeno, asumiendo que, si bien hay una disputa por un recurso escaso o un objetivo incompatible, debe aclararse que esos recursos están circunscritos al ámbito del poder. Esto, desde la perspectiva que buscan exhibir en su explicación de los conflictos internacionales, pero que, como se aclaraba desde el principio, estructuran elementos que pueden ser susceptibles a la aplicación en el ámbito del ciberespacio.

Así, Guillem Farrés (2012) procede especificando el paso esencial para analizar el complejo conflictual que es la identificación de los actores y los recursos de poder. Estos actores pueden clasificarse como de elite primaria o secundaria, radicando la diferencia en el nivel de dependencia de otros actores y la cantidad de recursos de poder disponibles para cambiar el sistema (Farrés, 2012).

En conjunto, se apela brevemente a estos aspectos teóricos, entendiendo que el análisis de la conflictividad enmarcada en la potencialización de los factores de inestabilidad debe basarse en el escudriñamiento de las interacciones de actores y relaciones variopintas. Como indica Galtung (1969), de la concepción acertada depende la

transformación del conflicto, y ello permitirá hacer una regulación positiva, convirtiendo todas estas situaciones en "experiencias pedagógicas, de concientización, de empoderamiento, de estímulo y desarrollo de la creatividad" (Calderón, 2009, p. 72).

Bajo este precepto, se justifica la mención de estas dos teorías, pues, finalmente, el objetivo de este documento en general es, no solo entender las nuevas dinámicas de inestabilidad a la luz de las herramientas cibernéticas, sino proponer salidas y exhibir vacíos que deben ser asumidos desde la ciberseguridad y ciberdefensa.

Relación entre la Ciberseguridad y Ciberdefensa y los factores de inestabilidad socioeconómicos

En este apartado, se plasma la relación específica entre los factores de inestabilidad socioeconómicos y las herramientas cibernéticas que los potencializan como una amenaza avasallante en contra de la estabilidad de los Estados, las organizaciones y los ciudadanos.

Narcotráfico

La aproximación entre el narcotráfico y el ciberespacio siempre lleva a pensar en la forma sobre cómo este intenta la legalización de todos los bienes que obtiene de este lucrativo negocio.

En esta nueva era digital es necesario familiarizarse con un nuevo término como es el Ciber lavado de activos, modalidad que se está convirtiendo en un medio muy eficaz para los delincuentes que trafican con estupefacientes. Año tras año, alrededor del planeta se incrementa gradualmente la proporción de lavado de todo tipo de activos los cuales se efectúan mediante mecanismos que en su esencia se valen de la naturaleza, características y todo lo que el ciberespacio pueda brindarles. Esto se evidencia en la estructuración de un esquema que se basa en la modalidad de las famosas *apuestas en línea*.

> Así como la Criminalidad Organizada tiene una fuerte presencia a nivel "Off-line", es decir, las operaciones que realiza en el mundo real en término de narcotráfico, trata de personas, venta de armas, etc.; también podemos encontrar expresiones de crimen organizado en el ciberespacio (Musotto & Wall, 2019, p. 17).

Estos criminales, o como se podrían denominar en la actualidad: cibercriminales del narcotráfico, también se están valiendo de la gran red de redes para el comercio de drogas produciendo que, recientemente, este fenómeno se acelerara de una manera exponencial. Las TIC permiten a los ciber narcotraficantes la facilidad de ofrecer bienes y servicios y, a su vez, efectuar todo tipo de movimientos financieros de una forma anónima.

Esto aunado a dos tecnologías que ya hacen carrera desde algunos años como lo son las redes anónimas de Tor[2] y los sistemas de pagos por seudónimo como lo son el Bitcoin, lo cual posibilitó la creación de todo tipo de movimiento de mercancías en la red, con el gran beneficio para los delincuentes que les concede el anonimato, mismo que redunda en la capacidad de vender o comprar dichas sustancias con el menor riesgo posible, ya que se volverían prácticamente invisibles para las autoridades y las entidades financieras de los respectivos países.

> El bitcoin, presentado en 2009 como moneda virtual, no tiene existencia física. Estas transacciones son anónimas y casi imposibles de rastrear, ya que funcionan en un sistema electrónico basado en redes de pares donde los usuarios están directamente conectados, sin pasar por los servidores centrales de un sistema tradicional. (Flores, 2019, p. 32)

A pesar de que esta moneda no cuenta con ningún tipo de reconocimiento oficial de parte de alguna, entidad financiera o gobierno, este no es considerado como una forma ilegal de transacción económica, es más, con este se puede adquirir cualquier tipo de bien desde que la entidad que vende el mismo acepte este canje, pero sirve como base para el intercambio y acumulación de riquezas por parte de actores ilegales.

Aunque este tipo de negocio o venta ilegal reviste más complejidad por Internet que en las mismas calles, para aquellos que su deseo sea zafarse de los ojos de las autoridades es aceptable, y para esto el único requisito que se tiene es poseer una máquina conectada a la red y contar con los suficientes bitcoins para adquirir el producto, seguido a esto y para volverse inrrastreable, debe instalarse Tor y después entrar a un shop y escoger el estupefaciente de su predilección y será llevado a través de algún servicio postal.

Infringir el delito de narcotráfico en la conocida, pero temida Deep Web, trae a los delincuentes algunas ventajas tales como privacidad, anonimato y dificultad para ser apresados por parte de las autoridades. Por lo tanto, se puede visualizar como otra ventaja la comodidad de las partes involucradas en el delito, tanto al realizar la venta, como de efectuar las compras de las drogas.

El tráfico de drogas, en especial, reviste alguna dificultad, ya que los ciberdelincuentes o ciber narcotraficantes tienen la capacidad de adaptar sus prácticas con una velocidad inimaginable con el fin de evitar cualquier tipo de riesgo legal.

Los inconvenientes que se pueden generar de forma penal, en general, con el delito del narcotráfico en la Deep Web acarrearía uno sin número de problemas, los cuales entorpecerían el curso normal de un proceso penal contra aquellas personas que incurran en este tipo de actividades de compra/venta de duchas sustancias.

2 Tor, o The Onion Router, es un programa informático que permite la transmisión de datos a nivel mundial casi sin dejar rastros. Así, los usuarios pueden conectarse a otro punto de la red y mantener su dirección de protocolo de Internet invisible, algo que se conoce como la Red Oscura (Dark Net).

Dichos obstáculos, que se pueden presentar al momento de calificar un crimen como tal, retrasarían al sistema judicial y visualizarían la carencia de regulación del mismo por parte de las ramas judicial y legislativa. Es preponderante decir que los inconvenientes a estudiar que se podrían hallar enmarcados en este tipo penal serían: tipicidad, jurisdicción, territorialidad y competencia de la ley penal, momento exacto de la materialización-configuración del delito y medios probatorios.

> Es preocupante que la Ley Penal no se encuentre cumpliendo su función principal que es la de regular el comportamiento de la sociedad y el ius puniendi del Estado, de igual forma, tampoco estaría cumpliendo su dogmática penal, ya que este no estaría permitiendo que se llegue al objetivo último del Derecho en General; es decir, la realización de la justicia en relación al delito en cuestión en Colombia debido a los indicios de violencia e impunidad de este delito cometido en su mayoría por la Guerrilla. En lo relacionado al delito en cuestión cometido a través de la Deep Web, podemos observar que no existe legislación o una norma que ayude a combatir este ilícito de una manera específica, directa y eficaz. (López, 2019, p. 9).

También se puede identificar que los ciber narcotraficantes pueden estar activamente involucrados en algunos roles muy específicos tales como la protección a ciberdelincuentes, otro es la inversión con altas sumas de capital a determinadas empresas, el tercer rol y el seguramente más usado, es el de utilizar su experiencia en el lavado de dinero, la capacidad que tiene el narcotráfico para efectuar eventuales acuerdos grupales y, el último, es el de actuar como guía de algunas operaciones ilegales como por ejemplo, reclutar a aquellos con habilidades técnicas para llevar a cabo los trabajos de delitos cibernéticos. Las dos últimas actividades son las que más se están llevando a cabo por los ciber narcotraficantes. Y además del uso de mensajes en mantas, cartones y cartulinas al lado de los cadáveres, los grupos armados empezaron a usar portales como YouTube para dar a conocer escenas espeluznantes, asesinatos y todo tipo de mensajes que circularon por la red sin control (Contreras, 2017).

Todo esto evidencia una rápida adaptación por parte de las organizaciones que se valen de este medio para efectuar negociaciones de sustancias psicoactivas, y estas se han valido de esta red *Deep Web,* ya que el reclutamiento de las redes humanas para poder efectuar la comercialización se puede efectuar de una manera mucho más fácil. Por último, el uso de esta red ilegal se da por la intangibilidad de las pruebas debido a que recolectar evidencias de este tipo de sitios web resulta bastante complejo puesto que la información que se maneja en su gran mayoría está en algoritmos encriptados.

Secuestro y Extorsión

Los grupos al margen de la ley, antes que actuar claramente hacia la persecución de un fin político, ejecutan estrategias que les brinda las herramientas económicas necesarias para enriquecerse y garantizar la posibilidad de continuar con las actividades desestabilizadoras del sistema. Así, en Colombia, es bien conocido el delito del secuestro, que

consiste en privar de la libertad de forma ilícita a una persona con fines lucrativos o para el cumplimiento de otras exigencias en perjuicio de terceros. Desde hace décadas el espacio físico ya no es el único ámbito en el que se pueden cometer delitos contra bienes tan relevantes como la intimidad o el patrimonio. El desarrollo de la web 2.0 no solo ha potenciado esto, sino que ha convertido el ciberespacio en un ámbito de intercomunicación social en el que también se cometen delitos contra la libertad e indemnidad sexuales (Llinares, 2012).

Empero, la relación con el ciberespacio supera la dimensión física de la retención de una persona o activo, y encuentra la manera de limitar la libertad de la información estratégica que puede encontrarse en el quinto dominio de la guerra, abriéndose más oportunidades para lucrarse y, al tiempo, desestabilizar a los ciudadanos, diversidad de organizaciones y al Estado mismo.

> Los cibersecuestros siguen siendo noticia. Hace pocos meses, lo era el primer gobierno que pagaba un rescate a un grupo de delincuentes digitales. Se trataba del Gobierno local de Riviera Beach, Florida. El último caso público ha sido la cadena SER y la empresa de servicios informáticos Everis, una de las más grandes de España. Y esos son los casos públicos, porque la mayoría se ocultan por el impacto en la reputación. El impacto de un secuestro digital en una empresa se resume en mandar a casa a los trabajadores hasta que se solucione. Eso puede ser cuestión de días o incluso semanas (SEC, 2019).

La vulnerabilidad de los sistemas en el ciberespacio, ante la tecnificación de los actores ilegales que exploran estos vacíos, se consolida como un factor de inestabilidad que tiene repercusiones multidimensionales, entendiendo que, si bien, el objetivo es económico, el secuestro de información, o inclusive, la consecución de información que puede llevar a facilitar un secuestro físico, puede tener implicaciones políticas y estratégicas para los Estados y las organizaciones tanto públicas y privadas.

Precisamente, la sociedad de la información, en la que se hace preciso que se faciliten los procesos de creación, consulta y utilización de la información, hacen de este tipo de delitos crezcan exponencialmente, y sean más peligrosos para las instituciones que hacen parte del complejo de administración pública, dada la sensibilidad de los procesos que se manejan. Del mismo modo, la seguridad y la defensa nacionales estarían expuestas al acceso a información confidencial que puede generar inestabilidad institucional, de tal modo que afectaría el cumplimiento de los intereses de supervivencia física del Estado y los ciudadanos, el desarrollo económico y la autodeterminación nacional.

Relacionado con este delito se encuentra el de la extorsión, que se consolida como una práctica ilegal casi tan antigua como la misma humanidad. En esta actividad ilegal, se coacciona a un sujeto para realizar una actividad o pagar cierta multa a cambio del desistimiento del delincuente de ejecutar algún hecho en su contra. Esto también se traslada al ámbito cibernético, tipificándose específicamente como la ciber extorsión.

La ciberextorsión o extorsión cibernética es un delito el cual usa la Internet en el cual un individuo desde un equipo informático retiene archivos electrónicos o los datos de su empresa o de una persona natural como rehenes hasta que este efectúe un pago por el rescate.

Esta modalidad es una de las más ejecutadas en la actualidad, en la que la virtualización de la vida cotidiana, como efecto de la pandemia, ha dispuesto al ciberespacio como la plataforma por excelencia para el trabajo, el estudio y la ejecución de cientos de procesos que implican la exposición de información sensible, que puede ser cooptada por los actores ilegales.

Manifestaciones Violentas y Disturbios

Los Estados de derecho están estructurados de manera tal que se protejan los derechos fundamentales de los ciudadanos. Particularmente para Colombia, en la Constitución Política de Colombia el artículo 37 estipula explícitamente la posibilidad de manifestarse pública y pacíficamente. De hecho, para la salud de las democracias, es deseable que los ciudadanos expongan a los mandatarios cuáles son sus preocupaciones, y se modifiquen las prioridades de la agenda política de manera eficaz.

> La Constitución Política garantiza el derecho a reunirse y manifestarse públicamente tanto en una dimensión estática (reunión) como dinámica (movilización), de forma individual como colectiva, y sin discriminación alguna, pues así se deriva de la expresión "toda parte del pueblo". Todo ello, sin otra condición distinta, a que sea pacífico, o sea, sin violencia, armas ni alteraciones graves del orden público. Esto significa que sólo la protesta pacífica goza de protección constitucional (Sentencia T-366, 2013, párrafo 46).

No obstante, la tensión social, y asuntos estructurales como la falta de educación para la democracia, desembocan en manifestaciones violentas que impiden enfocar la atención en las preocupaciones reales que, en primer lugar, llevaron a los ciudadanos a las calles. Estas explosiones violentas obedecen, también, a los fenómenos propios de una era en la que la posverdad y la manipulación mediática se fecalita con el uso de herramientas cibernéticas.

> Per se las implicaciones en relación con el desarrollo de lo social son más que obvias y su incidencia en la vida diaria son fundamentales. No habría que realizar un largo recorrido y manifestar mediante un sinfín ejemplos que la internet es hoy en día parte fundamental de nuestra vida y que configura lo que cada uno es. (Bernal, La opinión pública como forma de participación política en el ciberespacio: análisis de la tendencia #SalvemosNoticiasUno en la red social Twitter, 2020)

La utilización de redes sociales y aplicaciones de comunicación como Whatsapp que permiten la difusión de información masiva, abren el escenario para la masificación de una postura frente a temáticas sensibles. Aquí se abren dos escenarios: por un lado,

la visibilización de comunidades que regularmente no tienen los medios para exponer sus posturas y, por otro lado, plantea el peligroso telón de fondo en el que se construyen posturas radicales a partir de información manipulada que no es verificada por el ciudadano promedio.

> Cada vez son más las actividades que se han desplazado, o se están desplazando, hacia estas plataformas digitales, incluyendo aquellas relacionadas con la participación política, como el consumo de noticias políticas, la fiscalización de las actividades gubernamentales o la organización de protestas. De esta forma, estas tecnologías han creado nuevas dinámicas en la producción, selección, distribución y consumo de contenidos y en la interacción, organización y movilización política. Los medios sociales se articulan como espacios dónde se redefine el ejercicio del poder (Aguilera y Casero-Ripollés, 2018, p.5).

Precisamente, la redefinición de los ejercicios del poder, no necesariamente se remonta a un proceso consensuado, sino que, también con una tradición de política llevada a cabo por medios violentos, como en el caso de Colombia, las tensiones político - sociales, se alimentan de una profunda polarización que termina en estallidos violentos.

Así, en un país con claras necesidades socioeconómicas, en el que, según Forbes (2020), se llegó a un índice de pobreza de 42.5, y una profundización de la brecha de desigualdad, se manifiesta explícitamente lo esbozado por Johan Galtung (1969) como violencia: la diferencia entre lo que es y lo que podría ser. De hecho, si se trae a colación la definición original en inglés, se encontrará que dice: "violence is present when human beings are being influenced so that their actual somatic and mental realizations are below their potential realizations" (p. 168).

En principio, se apela a un proceso de manipulación, que crea la concepción de la diferencia entre lo que es y lo que se podría llegar a ser o tener. Claramente, sin necesidad de influencia o manipulación, millones de colombianos sienten la frustración devenida de la brecha entre estos dos puntos; no obstante, la manipulación viene a ejercerse directamente en la manera en la que se conduce la frustración hacia la ira y la explosión violenta que se encarna en los disturbios y la destrucción de la propiedad pública y privada. De este modo, el uso masificado de herramientas como el computador y el internet invitan a evaluar las consecuencias del avance tecnológico en aspectos relacionados con la democracia (Agudelo, 2010).

Si bien, esta violencia se hace explícita en un plano físico, desde el bombardeo de información y la construcción de una postura particular usando como herramientas la tecnología, se percibe la correlación de los fenómenos. Cabe revisar a otros procesos en otras partes del mundo como la Primavera Árabe. En dichas sociedades cerradas, con una concentración del poder que ameritaba una manifestación genuina que exigiera procesos democratizadores y mejores condiciones de vida, Facebook cumplió un papel fundamental.

Así, Luis Fernando Barón (2015), estudioso del proceso revolucionario en Egipto, concluyó que, "la combinación de acciones en la Web y en las calles amplificaron tanto la movilización de colectividades, como también la reacción del Estado en contra de sus opositores" (p. 21).

Es decir, las herramientas cibernéticas permiten amplificar el efecto de una iniciativa, pero, al mismo tiempo, pueden radicalizar una postura en la que finalmente se materializan hechos violentos que desestiman la protesta en sí misma y cuestionan la capacidad del Estado para proteger el derecho a la protesta y, al mismo tiempo, mantener el orden público.

> El ciberespacio como herramienta de socialización responde a la problemática de la separación del estado civil y el estado. Las plataformas que circulan en el ciberespacio han posibilitado un acercamiento directo a los escenarios y actores de la política, antes tan invisibilizado para la sociedad civil (Bernal, La opinión pública como forma de participación política en el ciberespacio: análisis de la tendencia #SalvemosNoticiasUno en la red social Twitter, 2020)

Ahora bien, la interconexión de la sociedad global, y la capacidad que se desarrolla desde el ciberespacio para exponer ciertas situaciones a nivel nacional y mundial, abren paso a las ciber protestas, entendidas como las manifestaciones en la red; estas pueden ser diseñadas previamente o también se pueden dar de una forma improvisada, en donde un grupo de personas manifiesta a los actores políticos, elites de referencia y a los espectadores en general sus puntos de desacuerdo.

> En el espacio online conviven nuevas comunidades, nuevos sistemas sociales. "Comunidades en el ciberespacio" presenta el análisis de los nuevos sistemas y formas de interacción en diferentes espacios virtuales. (Smith y Kollock, 2003, p. 15)

Estas se pueden encontrar en cualquier tipo de plataforma y para su construcción se encuentran diversos tipos de aplicaciones como pueden ser portales web, blogs, wikis, chats, correos electrónicos, y la diversidad de redes sociales existentes en la actualidad.

Las ciberprotestas, a su vez, tienen diferente sentido y grado de intensidad. A partir de trabajos anteriores (Constanza–Chock 2001) y (Weimann. 2006) Torres Nabel (2007) las clasifica en: a) ciberprotestas convencionales, b) ciberprotestas disruptivas y c) ciberprotestas violentas.

Las ciberportestas convencionales son acciones orientadas a la difusión, la orientación y a la movilización. Estas pueden ser: movilizaciones, consignas, peticiones, cadenas, evaluación de resultados, etc. Por su parte, las ciberprotestas disruptivas se definen como aquellas acciones orientadas a confrontar a los actores políticos o elites de referencia mediante los llamados a boicots, saturación de buzones de correo o de cuentas en redes sociales y teatralización (burlas, sátiras, cartones). Por último, las ciberprotestas violentas se refieren a aquellas actuaciones orientadas a atacar y atemorizar a los actores políticos o elites de referencia mediante: destrucción, robo y secuestro de datos

personales o institucionales (hackeo), ataques de virus informáticos, alteración de sitios web, amenazas, injurias y difusión de atentados.

> Las manifestaciones en la red tienen como función la de extender y amplificar los esfuerzos de comunicación de los movimientos sociales, un muy buen ejemplo es la exitosa estrategia de comunicación llevada a cabo por Internet que desarrolló el Ejercito Zapatista de Liberación Nacional (EZLN) en México. Este grupo lograron movilizar una gran cantidad de apoyos tanto al interior del país como internacionalmente a partir de una serie de estrategias basadas en Internet (Constanza-Chock, 2001; Weimann, 2006).

De esta manera, se deduce que la interacción entre la movilización social y las herramientas tecnológicas tiene una serie de funciones entre las que se encuentran: difusión y el control de la información y el estado del conflicto, recopilación, información sobre sus objetivos (agenda de las instituciones y los actores políticos), recaudación fondos, reclutamiento de activistas, efectuando un estudio de "mercado" sobre los perfiles de los internautas para después contactarlos y hacerles la invitación, interconexión y representación con otros movimientos sociales, divulgación de instrucciones, información, boletines, declaraciones.

Como se indicaba anteriormente, las funciones se pueden encaminar a la construcción de procesos basados en una metodología colaborativa en la que se aporta a la sociedad. No obstante, del estudio de los factores de inestabilidad, se concluye que, en la actualidad, el ciberespacio dota de herramientas que magnifican el impacto de la manifestación violenta que reta la institucionalidad nacional.

De hecho, en España hace algunos años, se buscó penalizar a quienes convocaran a manifestaciones violentas a través de internet o cualquier medio tecnológico, considerándolo como un "delito de integración en organización criminal por alterar gravemente el orden público" (El País, 2012).

> La pedagogía de las ciberprotestas, parte del constante modelado de colocar la crítica abierta como forma política de la verdad, misma que es avalada y diseminada mediante un hashtag, retuit, like o cualquier artilugio técnico de las redes sociales, y que difícilmente puede ser rebatida con argumentos. Esta pedagogía se erige como una nueva forma de "decirlo todo", de hablar con "libertad", con "franqueza", y con esto se gana la credibilidad de muchos o desprestigiar a otros tantos, que salen a las calles a gritar su "verdad" y diseminarla. (Nabel, 2009).

El reto, en la actualidad será la búsqueda de diferenciaciones claras entre el uso asertivo de los medios tecnológicos para la integración, movilización y activismo social, de aquellos llamados violentos, polarizadores y desestabilizadores, sin que desde este último ámbito se manipule la percepción de la ciudadanía que lleve a la concepción de un Estado absolutista que no garantiza derechos básicos como el de la manifestación pacífica.

¿Qué podría hacer el Estado Colombiano?

Propuestas para una estrategia de ciberseguridad y ciberdefensa que mitigue la potencialización de los factores de inestabilidad desde su relación con el ciberespacio

Para poder pensar en iniciativas bien llevadas por parte del Estado para atacar un tema que es tan incierto y cambiante, se deben establecer unas firmes líneas de acción en prevención, refiriéndose a actuar contra el enemigo desde su origen; de protección, minimizando las posibles vulnerabilidades; de persecución, haciendo frente a cualquier actividad terrorista; y de resiliencia, preparando respuestas inmediatas para volver a la normalidad.

Así, dentro de las iniciativas que se deben adelantar para contrarrestar el accionar de los ciberdelincuentes o aquellos grupos e individuos al margen de la ley que se valen del ciberespacio para su actuar, se tiene que se debe incrementar la capacidad de prevención, detección de los hechos, investigación y la debida respuesta a los factores de inestabilidad potencializados desde el ciberespacio, teniendo como base un marco jurídico asertivo, puntual y eficaz.

Precisamente, el marco jurídico referente a la ciberseguridad y ciberdefensa se abre como un tema de amplia discusión actual, entendiendo la necesidad de establecer una reglamentación clara a nivel nacional, que, desde la tipificación de los delitos, permita establecer estrategias acertadas a nivel de ciberseguridad y ciberdefensa.

A nivel de ciberdefensa, no se puede abordar ni estructurar una estrategia que trate efectivamente las cinco dimensiones de actuación, pues precisamente se deben desarrollar capacidades y habilidades que permitan dimensionar y categorizar los riesgos y amenazas para la defensa nacional desde el ámbito cibernético, de manera que se puedan diseñar las estrategias de respuesta y de prevención.

Por ejemplo, desde una perspectiva comparada se pueden rescatar lecciones importantes de las medidas emprendidas en otras latitudes. Por ejemplo, en el marco de la Unión Europea, el Parlamento y el Consejo Europeo establecieron una estrategia nacional de seguridad de las redes y sistemas de información, identificando los ámbitos de actuación, como aquellos relacionados con actividades socioeconómicas vitales e infraestructura crítica.

Si bien los documentos del Consejo Nacional de Política Económica y Social (CONPES), han establecido lineamientos estratégicos en seguridad digital, en especial el último (3395 de 2020), sienta las bases para la creación de una cultura de confianza ciudadana, es decisivo esclarecer los caminos y presupuestos que financien las iniciativas recogidas en este tipo de documentos.

En consonancia con ello se deben, entonces, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados, fortaleciendo la seguridad de los sistemas de información y de las redes de comunicaciones en las cuales se soportan las infraestructuras críticas del país, identificando los posibles escenarios problemáticos y los actores predominantes en ellos, bien sea de naturaleza simétrica o asimétrica, atendiendo la premisa de complejos conflictuales y el triángulo de violencia, que llevan a los tomadores de decisiones a explorar causas profundas para transformar realmente los fenómenos conflictivos.

En este sentido, se hace necesario establecer un sistema de mejora en la seguridad y el fortalecimiento de la resiliencia de las tecnologías de la Información y la comunicación (TIC) en el sector privado a través del uso de las capacidades del poder público. Con ello, se dará un impulso a la colaboración público-privada, contribuyendo a la seguridad y robustez de redes, productos y servicios de las TICs.

Del mismo modo, se debe incentivar la capacitación de los ciudadanos en ciberseguridad, y solidificar la educación en los aspectos relacionados con la seguridad informática, suministrando la información necesaria desde la educación básica primaria, entendiendo que son temas transversales en todos los niveles de educación y en diversas áreas de especialidad, hasta llegar a un nivel de formación de profesionales especializados en el área, que puedan suministrar información especializada que guie las conductas de los Estados y la sociedad en materia de ciberseguridad y ciberdefensa, y con ello podría abordarse aquellas dinámicas enmarcadas en la violencia cultural y estructural definidas por Galtung (1969).

> Como tantas veces se ha dicho, el factor humano es y seguirá siendo un elemento fundamental en cualquier estrategia que pretenda ser exitosa, y las instituciones de educación superior desempeñan un rol esencial en este aspecto. Desde nuestro punto de vista, los desafíos que enfrentamos son múltiples y requieren soluciones complejas y diferenciadas según la realidad política, económica y social de los diversos países que forman parte de América Latina y el Caribe (Banco Interamericano de Desarrollo, 2020).

En este mismo sentido, se generarían las bases necesarias para la construcción de una cultura de ciberseguridad, procurando que los ciudadanos hagan parte de la estrategia de prevención y alerta temprana de riesgos, antes que convirtiéndose en blanco fácil de la ilegalidad. En este sentido, desde los mismos ciudadanos, la cultura organizacional de las empresas y las instituciones estatales, se podrían afrontar los riesgos cibernéticos asociados con factores de inestabilidad como el narcotráfico, las infiltraciones en las manifestaciones sociales, y la reproducción de GAOS y GDO que se solidifican en los escenarios cibernéticos.

Ahora bien, así como el escenario cibernético plantea amenazas y riesgos, también abre posibilidades de actividades constructivas como las propias de la cooperación

internacional. De esta manera, los Estados en la actualidad no solo contemplan estrategias de colaboración con donaciones o intercambios de información o capital, sino que se contemplan acuerdos para estimular el desarrollo de capacidades cibernéticas, así como de tecnificación de las sociedades menos desarrolladas. Con esta tendencia, se podría acceder a la experticia, información especializada e infraestructura desarrollada por parte de las potencias, cerrando las brechas y minimizando los riesgos que enfrentan los ciudadanos y el Estado colombiano como un todo.

Del mismo modo, se abren las oportunidades de cooperación entre los diversos actores que componen el ecosistema de ciberseguridad como las empresas privadas, las entidades estatales y la academia. Ejemplo de ello, son los acuerdos suscritos para garantizar la capacitación de los funcionarios de los sectores más vulnerables del país ante las amenazas cibernéticas.

> Con el propósito de enfrentar los fraudes por canales digitales, delito que en 2020 registró un aumento del 44 % y en el que las alcaldías y gobernaciones presentaron pérdidas por $50.000 millones, el Ministerio de las TIC y Asobancaria firmaron un Memorando de Entendimiento (MOU) para capacitar a 250 alcaldes y gobernadores de todo el país en temas de ciberseguridad. Durante la firma del acuerdo, Germán Rueda, viceministro de Transformación Digital, resaltó la importancia que tiene este tipo de medidas para proteger los recursos públicos y demostrar el compromiso del Gobierno nacional con la ciberseguridad de los colombianos (Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, 2021, p. 26).

Dentro de otras iniciativas que debe adoptar el país con el fin de contrarrestar los efectos de los factores de inestabilidad socioeconómicos apalancados en el ciberespacio, se debe contemplar la de mejorar las capacidades abstractas de las Fuerzas Armadas, como lo son la defensa en las redes y la mejora de la resistencia a los ataques, preparándose para disuadir en el ciberespacio como se podría llegar a hacerlo en el espacio físico, entendiendo la multidimensionalidad del fenómeno, tal y como se plantea desde la corriente teórica de los complejos conflictuales, resaltando que no solo hay una situación puntual que resulta retadora, sino que hay una red de estas que conforman el complejo que debe afrontar el Estado colombiano.

Para ello, la tarea a desarrollar es la de estructurar una doctrina común para la planificación, preparación y ejecución de las operaciones de información, donde se incluyan todas las interpretaciones que se puedan dar de *ius in bello e ius ad bellum* en el ciberespacio, llenando los vacíos normativos del quinto dominio de la guerra.

Así mismo, es perentorio hacerse parte de la discusión internacional con respecto a las regulaciones de la actuación de los Estados en un eventual escenario de ciberguerra, asumiendo que las tensiones geopolíticas y las estrategias de dominio del sistema internacional se desplazan hoy a un espacio cibernético, en el que se requiere de consensos mínimos que eviten el caos y la anarquía total que pueda conducir a la destrucción del modelo de Estado – nación actual.

En términos generales, la mejora continua de las capacidades del Estado, sus instituciones y agentes, será un primer paso para liderar el camino que conlleve a una sociedad cibernética resiliente, capaz de prevenir y afrontar los retos devenidos de actividades tradicionales que actúan su plan de actuación al ciberespacio, tales como el narcotráfico, el secuestro, la extorsión o la búsqueda de la inestabilidad institucional a través de las manifestaciones violentas y la promoción de disturbios.

De base, la estrategia también deberá girar en torno a la capacitación de profesionales especializados y de los ciudadanos en general, entendiendo que a diferentes niveles se puede contribuir a actuar sigilosamente en el ciberespacio, conllevando ello a una actuación responsable y crítica frente a los contenidos y herramientas que se disponen en este dominio.

Conclusiones

Las dinámicas de seguridad actual exigen una revisión constante de las estrategias que buscan afrontar las amenazas variopintas que se potencializan con la evolución misma de la humanidad. Sin lugar a duda, las revoluciones industriales han marcado el inicio y el fin de las eras que han supuesto cambios no solo para los modos de producción y la economía, sino para la vida en si misma de los ciudadanos, las empresas y los Estados.

Precisamente, estos últimos han tenido que volcar su mirada a un escenario volátil, impredecible, complejo y amenazante en el que no solo encuentran como competidores a otros Estados en un escenario de lucha geoestratégica, sino que, tiene que hacer frente a los actores asimétricos que maximizan sus capacidades desde el anonimato del ciberespacio.

En este sentido, el estudio de estos fenómenos en un contexto como el colombiano, requiere remontarse a la multidimensionalidad de estos, que puede ser vista desde la propuesta de Johan Galtung, en combinación con la referencia teórica de Guillem Farrés (2012), entendiendo que hay diversas capas que componen un acto violento, resultando ser la sumatoria de conflictos que se interconectan para formar un complejo conflictual, que no puede ser transformado abordándolo desde una manera tradicional, que, en términos de Galtung (1969), le apuntaría a resolver la violencia directa, sin atender las causas subyacentes de esta.

En este sentido, los factores desestabilizadores como el narcotráfico, la extorsión y las manifestaciones violentas, y su fortalecimiento desde el ciberespacio, no pueden verse desde una perspectiva que solo busque derretir la punta del iceberg, sino que debe enlazar los asuntos que dan pie para el desarrollo de estos fenómenos conflictuales tanto en un plano convencional, como en un plano ciberespacial, con estrategias que se acompasen con la evolución tecnológica.

La ciberseguridad y ciberdefensa de Colombia, se ve avocada a buscar respuestas en la interconexión del ecosistema compuesto por el Estado, las empresas y la academia, de manera tal que se puedan afrontar las amenazas que desestabilizarían a la sociedad en su conjunto. Pero, una vez más, cabe recalcar que no solo basta una estrategia a nivel cibernético, sino que, precisamente, la reflexión del complejo conflictual lleva a evidenciar que las falencias en la educación, los vacíos estatales, la falta de tecnificación y la miopía institucional, alimentan los conflictos que protagonizan la agenda de seguridad y defensa, así como de ciberseguridad y ciberdefensa nacionales.

Así, la exactitud con que se dimensionen estas amenazas será la clave para diseñar soluciones desde la perspectiva de ciberseguridad y ciberdefensa, pues precisamente la delimitación del fenómeno permitirá estructurar el alcance de la respuesta a este. Si la concepción de la amenaza tradicional fracasa en el establecimiento con el nexo con las herramientas cibernéticas, no podrá hacerse un lugar prioritario en la estrategia de ciberseguridad y ciberdefensa nacional.

Asumir en un país como Colombia una visión renovada y diversa del fenómeno de la violencia, aunado a una evolución tecnológica que abre oportunidades, pero al mismo tiempo retos y amenazas, es una tarea que debe afrontarse desde el conjunto de la institucionalidad y la sociedad, coadyuvando todos a generar conciencia sobre los fenómenos en su forma tradicional y su forma más evolucionada en el ciberespacio, para ser contundentes en la lucha contra los factores que desestabilizan la realidad del país.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con este artículo.

Autor

Diego Mauricio Quintero Franco. Oficial de la especialidad de Comunicaciones. Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela de Cadetes José María Córdova, Colombia.

Contacto: quinterod@esdeg.edu.co

Referencias

Agudelo, A. (2010). *Ciberespacio: riesgos y posibilidades republicanas para la democracia* [Tesis de grado]. Universidad de los Andes.

Aguilar, L. J. (2016). *Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0).* Universidad Pontificia de Salamanca.

Aguilera, M., y Casero-Ripollés, A. (2018). Los medios sociales se articulan como espacios dónde se redefine el ejercicio del poder. *Revista de comunicación y tecnologías emergentes*, 16, (1), 1-21.

Aguirre, J. (2010). *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI.* Editorial del Cardo.

Baltazar, E. (04 de 11 de 2018). *Narcos y hackers, cómo funciona esta nueva alianza delictiva que crece en la oscuridad*. Infobae https://www.infobae.com/america/mexico/2018/11/02/narcos-y-hackers-como-funciona-esta-nueva-alianza-delictiva-que-crece-en-la-oscuridad/

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe*. Banco Interamericano de Desarrollo.

Bernal, B. (2020). La opinión pública como forma de participación política en el ciberespacio: análisis de la tendencia #SalvemosNoticiasUno en la red social Twitter [Tweet].

Calderón, P. (2009). Teoría de Conflicto de Johan Galtung. *Revista de Paz y Conflictos* (2), 60-81.

Cano, J (2008). Cibersegurdad. Retos y amenazas a la seguridad nacional en el ciberespacio.

CARI. (Noviembre de 2013). *Ciberdefensa-Ciberseguridad Riesgos y Amenazas*. Obtenido de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Chillier, G. (2005). *The new OAS concept of hemispheric security*. Organization of American States.

Contreras, J. (2017). *La estrategia de comunicación del Narcotrafico*. Editorial: Instituto Chihuahuense de la Cultura.

Corte Suprema de Justicia. Sentencia T-366/13. M.P. Luis Ernesto Vargas Silva; 27 de junio de 2013.

Departamento Nacional de Planeación. (14 de Julio de 2011). Consejo Nacional de Política Económica y Social 3701. República de Colombia.

EULATE, P. M. (2013). *Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*. Boletín Oficial del Ministerio de Defensa.

Farrés, G. (2012). Poder y análisis de conflictos internacionales: el complejo conflictual. *CIDOB d´afers internacional*, (99), 179-199.

Flores, E. D. (2019). *El Delito de Narcotráfico en la Deep Web: Una Visión desde la Legislación Ecuatoriana*. FLACSO Andes.

Fulwood, M. N. (03 de 08 de 2016). *Ciberextorsión: la nueva moda 'hacker'*. Huffpost: https://www.huffingtonpost.es/marina-nogales-fulwood/ciberextorsion-la-nueva-moda_b_7893756.html

Galtung, J. (1969). Violence, Peace, and peace Research. *Journal of Peace Research, 6*(3), 167-191.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6a. ed. --.). McGraw-Hill.

Llinares, F. M. (2012). Fenomenología y criminología de la delincuencia en el ciberespacio. En F. M. Llinares, *Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

López, G. (2019). *El Delito de Narcotráfico en la Deep Web: Una Visión desde la Legislación Ecuatoriana*. Flacso Ecuador.

Mato, R. (jul-2018). *El ciberespacio, un aspecto a tener en cuenta en el planeamiento militar*. CEFA Digital.

Medina, G. E. (2009). *La seguridad en el ciberespacio: un desafío para Colombia*. Sello Editorial ESDEG.

Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. (09 de abril de 2021). *Ante posibles ataques cibernéticos, alcaldías y gobernaciones se capacitarán gracias a convenio entre MinTIC y Asobancaria*. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162457:Ante-posibles-ataques-ciberneticos-alcaldias-y-gobernaciones-se-capacitaran-gracias-a-convenio-entre-MinTIC-y-Asobancaria

Musotto, R., & Wall, D. S. (2019). *The online crime-terror nexus: Using booter services (stressers) to weaponize data?* Routledge.

Nabel, L. C. (2009). *La pedagogía de las ciberprotestas: un análisis psicosocial*. Universidad Autónoma de Madrid.

Pearson, F., y Rochester, J. (2015). Introducción a las relaciones internacionales. Departamento de Derecho Internacional Público y Relaciones Internacionales

Porto, A. (2015). Ciberdefensa. *Centro de Estudios para la defensa nacional*, 12.

Santamans, F. P. (2018). Los avestruces no saben de ciberseguridad. *El farmaceutico*, 26-32. https://www.elfarmaceutico.es/uploads/s1/18/97/ef559-profesion-ciberseguridad.pdf

Smith, M., y Kollock, P. (2003). *Comunidades en el ciberespacio.* Barcelona.

Totalsec News. (21 de 11 de 2019). Cómo evitar el secuestro digital. *Totalsec news*. Totalsec news: https://www.totalsec.com.mx/blog/blog.php?P=como-evitar-el-secuestro-digital

Unión Internacional de Telecomunicaciones. (Noviembre de 2010). *Defi niciones y terminología relativas a la creación de confianza y seguridad en la utilización d etecnologías d ela información y la comunicación*. https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Vaisenberg, V. (21 de 09 de 2014). *Consultas psicológicas*. Consultas psicológicas: http://columnistas.montevideo.com.uy/ucimprimir_301026_1.html

Van Puyvelde, D. &. (2019). *Cybersecurity: politics, governance and conflict in cyberspace.* John Wiley & Sons.

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (20), 31–45.