1
ISSN: 2955-0270

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Revista Ciberespacio, Tecnología e Innovación

Volumen 1 - Número 1
2022 (enero-junio)
Bogotá., Colombia

Revista **Ciberespacio, Tecnología e Innovación**

Volumen 1, número 1, enero-junio 2022
ISSN: 2955-0270
Bogotá, D.C., Colombia

Indexada en:

Google Scholar

ESCUELA SUPERIOR
DE GUERRA
"General Rafael Reyes Prieto"
Colombia

EDITORIAL **ESDEG**

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 1, enero-junio 2022
ISSN: 2955-0270
Bogotá, D.C, Colombia

La **RCIT** es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la **Escuela Superior de Guerra "General Rafael Reyes Prieto"** (**ESDEG**), principal centro de pensamiento conjunto del **Comando General de las Fuerzas Militares de Colombia**, a través de su **Sello Editorial ESDEG**.

2022, Escuela Superior de Guerra "General Rafael Reyes Prieto"
Vicedirección de Investigación - Sello Editorial ESDEG
Carrera 11 No. 102-50. Bogotá, D. C., Colombia
Página web: https://esdegrevistas.edu.co/index.php/rcit
Correo electrónico: esdegrevistas@esdeg.edu.co

Revista Ciberespacio, Tecnología e Innovación

1. ENFOQUE Y ALCANCE

La **Revista Ciberespacio, Tecnología e Innovación** (RCIT). La RCIT es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), principal centro de pensamiento conjunto de las Fuerzas Militares de Colombia, a través de su Sello Editorial ESDEG.

La **RCIT** es una revista interdisciplinaria, con un enfoque en las Ciencias Sociales (Clase 5I01, OCDE / UNESCO), abierta a la discusión y difusión de trabajos teóricos e investigaciones sobre el ciberespacio identificado como quinto dominio, en donde la ciberseguridad, la ciberdefensa y la innovación son ejes para el análisis de este ámbito. Su finalidad es abordar ejes temáticos sobre la seguridad digital, la información, las tecnologías disruptivas, las ciberamenazas, las guerras cibernéticas, entre otros temas, reconociendo la necesidad de generar desarrollo tecnológico de innovación en relación con un quinto dominio de la guerra que afecta desde lo digital a los dominios físicos como la infraestructura crítica de un Estado.

2. ORGANIZACIÓN TEMÁTICA Y PÚBLICO OBJETIVO

Cada número de la **Revista Ciberespacio, Tecnología e Innovación** cuenta con cuatro secciones:

a) **Debates:** artículos de investigación científica y tecnológica.

b) **Coyuntura:** artículos de reflexión o revisión.

c) **Perspectivas:** entrevistas a académicos o tomadores de decisión.

d) **Enfoques:** reseñas de libros.

La **RCIT** está dirigida a un amplio público que incluye decisores políticos, miembros de las Fuerzas Armadas, servidores públicos, profesionales, docentes, investigadores y estudiantes de ciencias sociales y de otras áreas del conocimiento, interesados en la seguridad y la defensa.

3. TIPOLOGÍA E IDIOMA DE LOS ARTÍCULOS

La **RCIT** publica artículos en español e inglés en tres categorías:

a) **Investigación científica y tecnológica:** documento que presenta de manera detallada los resultados originales derivados de proyectos de investigación y/o desarrollo tecnológico finalizados.

b) **Reflexión:** documento que ofrece resultados de investigación desde una perspectiva analítica, interpretativa y crítica del autor, sobre un tema específico, recurriendo a fuentes originales.

c) **Revisión:** documento que organiza, analiza y se integran los resultados de investigaciones publicadas o no publicadas sobre un campo en ciencia o tecnología, con el fin de dar cuenta de los avances y las tendencias de desarrollo.

4. PERIODICIDAD

La **RCIT** es editada semestralmente (enero-junio y julio-diciembre) en formato impreso (ISSN: 2955-0270). La versión en línea y la versión impresa aparecen publicadas el penúltimo día del último mes del periodo de cada número, esto es, 30 de junio para el número enero-junio y 30 de diciembre para el número julio-diciembre. Cada uno de los artículos de la **RCIT** tiene un DOI (Digital Object Identifier) asignado para su identificación y referenciación.

5. FINANCIAMIENTO

La **Revista Ciberespacio, Tecnología e Innovación** es una publicación académica de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), perteneciente, a su vez, al Comando General de las Fuerzas Militares de Colombia que, como entidad pública, se financia con los recursos asignados por el gobierno nacional. Con el fin de mantener su carácter crítico e independiente, la **RCIT** no acepta financiamiento ajeno a la ESDEG para su funcionamiento. Así las cosas, todo el proceso de publicación de la revista está completamente libre de costo para los autores; tampoco se realizan cobros por el envío, procesamiento y publicación de artículos (*no article submission or processing charge*).

6. ACCESO ABIERTO, DERECHOS DE AUTOR Y LICENCIA PARA PUBLICACIÓN

El Sello Editorial ESDEG es signatario de la Declaración de Budapest y todos sus contenidos publicados son de acceso abierto (open access), con pleno reconocimiento de los derechos morales de los autores sobre su obra. Para su publicación, los autores aceptan ceder los derechos de publicación en favor de la ESDEG y el Sello Editorial ESDEG de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

De esta forma, los autores y los lectores pueden copiar y difundir el artículo en la versión final publicada en línea por la **RCIT**, siempre que se reconozca e identifique al autor (o autores) del artículo, no se haga uso comercial del artículo final publicado, ni se trate de obras derivadas o versiones modificadas.

7. POLÍTICA CROSSMARK

La **RCIT** utiliza Crossmark para mantener informados a sus lectores sobre cualquier cambio que tengan los artículos publicados. CrossMark es una iniciativa de CrossRef para proporcionar una forma normalizada de localizar la versión oficial de un documento. La **RCIT** reconoce la importancia de mantener la integridad de los registros académicos para investigadores y bibliotecas, razón por la cual garantiza que su archivo electrónico siempre cuenta con un contenido confiable.

Al hacer clic en el icono CrossMark se informa al lector sobre el estado actual del documento así como información adicional sobre el historial de publicación de este. Los contenidos que muestran el ícono de CrossMark son aquellos contenidos publicados en la página web de la **RCIT**, actuales o futuros.

8. ARCHIVO DE LOS CONTENIDOS

La **RCIT** utiliza la plataforma Portico para el archivo digital de los contenidos publicados. Así mismo, la **RCIT** permite que los autores puedan autoarchivar en repositorios institucionales, temáticos o páginas webs personales su artículo en la versión final publicada en línea.

9. RESPONSABILIDAD DE CONTENIDOS

La responsabilidad por el contenido de los artículos publicados por la **RCIT** corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Superior de Guerra "General Rafael Reyes Prieto", el Comando General de las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

10. INDEXACIÓN

La **Revista Ciberespacio, Tecnología e Innovación** se encuentra incluida en los siguientes Sistemas de Indexación y Resumen (SIR):

Google Scholar

Tabla de Contenido

Esta página queda intencionalmente en blanco

Editorial

Editorial

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 1-3)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Editorial: El ciberespacio: nuevo dominio de la guerra y el crimen

Editorial: Cyberspace: new domain of war and crime

DOI: https://doi.org/10.25062/2955-0270.4792

Tania Lucia Fonseca Ortiz
Editora en Jefe Revista Ciberespacio, Tecnología e Innovación

La revista Ciberespacio, Tecnología e Innovación, presenta su primera edición titulada *El ciberespacio: nuevo dominio de la guerra y el crimen*, dando la apertura a un espacio de intercambio de conocimientos y experiencias en torno al nuevo dominio de la guerra llamado el ciberespacio, un escenario complejo donde interactúan diferentes actores e individuos, y todos comparten un interés relacionado con la tecnología, innovación e información.

Este espacio digital amplía el horizonte de la forma en que se debe ver el mundo, particularmente desde la dimensión de la seguridad y la defensa, dos campos que se han consolidado como conocimientos especializados en temas relacionados con los cibernéticos y dónde las amenazas y riesgos a la seguridad son un tema de interés estratégico.

Dicho lo anterior, la línea que marca la temática de la presente edición está relacionada con la identificación de los factores de inestabilidad en el campo de la ciberseguridad y la ciberdefensa, relacionando con esto las posibilidades de riesgo a la seguridad económica y social a las que se exponen los individuos y los Estados dado las transformaciones digitales que se están presentando. Al mismo tiempo, se busca analizar las oportunidades de mejora para el empleo de tecnologías y procesos de innovación que permiten garantizar los intereses estratégicos de una nación en un escenario digital. Para tal fin, la revista se encuentra distribuida en cuatro secciones, estas son:

Sección debates, la principal sección que guía el número. Para este caso se presentan tres importantes contribuciones. El artículo *Los Factores Armados de Inestabilidad*

frente a la Ciberseguridad y la Ciberdefensa Nacional, un escrito que realiza una aproximación conceptual sobre el ciberespacio y la ciberdefensa relacionado con el crimen organizado transnacional. En este análisis se establece la importancia de las regulaciones normativas frente a los dilemas de seguridad en torno al ciberespacio, como la ciberdelincuencia. Se evidencian nuevas dinámicas de crimen que están siendo explotadas por los actores del crimen organizado y relacionados con actores armados ilegales.

En el artículo *La ciberseguridad y la ciberdefensa frente a los factores de inestabilidad económicos y sociales*, se realiza una profundización detallada de los factores de inestabilidad que afectan a las instituciones de seguridad. Entre las diferentes modalidades se reconoce el empleo de nuevas estrategias que se acompañan de modalidades de delitos tradicionales y convencionales como el secuestro, la extorsión y la violencia en protestas sociales, todas estas potencializadas por actores ilegales que convergen en el mundo digital. Como consecuencia, se proponen líneas de acción que debe emprender el Estado colombiano y las instituciones de seguridad enmarcadas en normativas CONPES, todo con el objetivo de adaptar los sistemas de información e infraestructura tecnológica institucional para afrontar los nuevos escenarios de un dominio que tiene un impacto en el mundo real.

Para el cierre de esta sección, el artículo *Importancia de una Ley de Ciberseguridad y Ciberdefensa para Colombia*, se reconoce la necesidad de crear una ley de ciberseguridad y ciberdefensa en Colombia con el objetivo de que el estado pueda afrontar de manera eficiente y efectiva las amenazas cibernéticas, se recomienda que se adopten las disposiciones nacionales e internacionales en materia jurídica que puedan servir como documentos bases para recomendar la ley.

Sección coyuntura, enfocada a abordar análisis coyunturales sobre temas relevantes, se presenta el artículo corto titulado *Riesgos Cibernéticos Para la Aviación Regular "El 11 de Septiembre Cibernético"*. En este análisis, el autor hace una reflexión en torno a las amenazas que se pueden presentar en la aviación regular, riesgos y peligros extraídos de experiencias de otros países, con el objetivo de abrir el debate sobre la importancia de contener los riesgos cibernéticos generados en el ciberespacio, un dominio y que se relaciona con el aéreo. Como consecuencia, se concluye que existe una probabilidad de riesgo para que se materialicen escenarios de peligro o crisis desde el ciberespacio que pueden impactar directamente sobre el desarrollo de las operaciones aéreas y su seguridad.

Sección perspectiva, comparte las experiencias profesionales y académicas de investigadores que están analizando el ciberespacio. Para esta sección se contempla entrevistas a líderes en el campo de la ciberseguridad seguridad. Para esta sección se

tiene como tema central *La ciberseguridad en Colombia,* una *entrevista a Marco Emilio Sánchez Acevedo*.

Para el cierre de la edición, se encuentra la *sección enfoques*, un espacio especializado para recomendar literatura académica producto de investigaciones realizadas y que pueden contribuir a la generación de nuevo conocimiento. Se recomienda el *Libro: La seguridad en el ciberespacio: Un desafío para Colombia*, una importante compilación de investigaciones realizadas desde la Escuela Superior de Guerra General "Rafael Reyes Prieto".

Con esta edición se invita a la comunidad científica a que participen compartiendo sus escritos y experiencias en este nuevo espacio, y lo más importante, poder abrir el debate hacia el ciberespacio como un escenario de oportunidad y eje transformador.

Esta página queda intencionalmente en blanco

Debates

Debates

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 7-40)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Los factores armados de inestabilidad frente a la ciberseguridad y la ciberdefensa nacional

The armed factors of instability in the face of cybersecurity and national cyberdefense

DOI: https://doi.org/10.25062/2955-0270.4768

Martin Fernando Rincón Gallón
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Los factores armados de inestabilidad como el narcotráfico, el crimen organizado trasnacional, los Grupos Armados Organizados (GAO) y los Grupos Delincuenciales Organizados (GDO), son hoy una fuente de amenaza creciente para la ciberseguridad y ciberdefensa de la nación colombiana, gracias a la convergencia criminal, fenómeno que les permite aliarse temporalmente para cometer delitos o para el caso específico ciberdelitos en común, aspectos que necesitan enfrentarse eficientemente para minimizar su impacto en la nación colombiana. La seguridad nacional busca mejorar y la evolución de la protección del ciberespacio a medida que los delitos incrementan y evolucionan. Existen instituciones del Estado, empresas privadas y ciudadanos de manera segura, vigilante y alerta ante cualquier amenaza, el COLCERT, el CCOCI, Centro Cibernético Policial y el CAI Virtual, quienes buscan combatir los ciberdelitos y a los ciberdelincuentes.

Palabras Clave: Factores Armados de Inestabilidad; Ciberseguridad; Ciberdefensa; Ciberespacio

Abstract

Armed factors of instability such as drug trafficking, transnational organized crime, Organized Armed Groups (GAO) and Organized Criminal Groups (GDO), are today a source of growing threat to the cybersecurity and cyberdefense of the Colombian nation, thanks to the criminal convergence, a phenomenon that allows them to temporarily ally themselves to commit crimes or, in the specific case, cybercrimes in common, aspects that need to be addressed efficiently to minimize their impact on the Colombian nation. National security seeks to improve and evolve the protection of cyberspace as crimes increase and evolve. There are State institutions, private companies and citizens in a safe, vigilant and alert manner in the face of any threat, the COLCERT, the CCOCI, the Police Cyber Center and the Virtual CAI, who seek to combat cybercrimes and cybercriminals.

Key words: Armed Factors of Instability; Cybersecurity; Cyberdefense, Cyberspace

Artículo de reflexión
Recibido: 6 de enero de 2022 • **Aceptado:** 14 de abril de 2022
Contacto: Martin Fernando Rincón Gallón rinconm@esdeg.edu.co

Introducción

Con la llegada de la internet a finales del siglo XX, la sociedad dio un paso agigantado en su evolución tecnológica para conectar al mundo entero; acciones simples como mensajería instantánea, transacciones bancarias, acceso a información desde portales web, videollamadas, y un sin número de aplicaciones hicieron de este invento un gran aliado para el desarrollo de las comunicaciones, los negocios, y la innovación empresarial, sin embargo, como ha ocurrido con otros grandes inventos, todas esas opciones de desarrollo traen consigo el incremento de riesgos y amenazas a la seguridad.

Para este caso en particular, los delincuentes aprovechan sus ventajas y características particulares para mejorar su actuar delictivo ampliando la gama de acciones criminales y perjudicando de manera indiscriminada a los ciudadanos en general, a las empresas del sector público y privado, entidades de gobierno, Estados y asociaciones internacionales, con objetivos variados como son el lucro personal, a través de estafas o robo electrónico, a nivel comercial como el espionaje corporativo y a nivel estado afectando de manera directa o indirecta la seguridad nacional (Machín & Gazapo, 2016).

La internet se ha convertido en un elemento clave para el crecimiento y desarrollo social y económico de una nación, los sectores económicos y productivos dependen del flujo constante de información, así como los diversos servicios ofrecidos por la red, tales como la consecución de materias primas y la comercialización efectiva de sus productos. El sector bancario y financiero que soporta todas las actividades económicas, nacionales o internacionales, de la misma manera, la infraestructura nacional al servicio de la comunidad como transporte, servicios públicos, servicios de salud, entre otros, basan su operación en servicios en la red, dando mayor dinamismo y asegurando el cumplimiento de los propósitos particulares e integrándose entre sí para beneficio de la nación.

Teniendo en cuenta esta dependencia, un fallo en la red o una afectación sobre la misma podría dejar en evidencia vulnerabilidades y materializar amenazas en materia de seguridad, estableciendo la necesidad de realizar acciones que lleven a una estrategia de seguridad en el ámbito cibernético o ciberseguridad. Tras este cambio, en el panorama y concepción de seguridad, el sistema internacional priorizó el cuidado y protección del ciberespacio, con el fin de cuidar la información que circula diariamente por este sistema (Centro de Estudios de Política y Relaciones Internacionales, 2016).

En relación con lo anterior, se propone la siguiente pregunta de investigación ¿Cuál es el impacto de los factores armados de inestabilidad en la seguridad y defensa nacional en el ámbito cibernético?

A nivel internacional, como principal herramienta para contener los ataques en el ciberespacio, como es conocido ahora el campo integrado a la información y su tránsito en la internet, se ha generado el Convenio de Budapest o el Convenio sobre la ciberdelincuencia del Consejo de Europa firmado y ratificado desde el 2001 por varios países del

mundo, principalmente, por la Unión Europea, Estados Unidos, Canadá y Australia con el cual se desarrolla el uso extendido para desarrollar la legislación de combate al cibercrimen. Un proceso que ha venido desarrollando Colombia desde el 2010 y que solo ratificó por medio de la ley 1928 de 2018. Norma que avala el surgimiento y desarrollo de la lucha contra el cibercrimen en la República de Colombia, también conocida como Seguridad Digital (Ferrando, 2018).

Por tal razón, es importante conocer y diferenciar, de manera breve, los conceptos de ciberespacio, ciberseguridad y ciberdefensa, ciberguerra y ciber-arma, entre otros; que apoyen el buen funcionamiento del proceso de seguridad y defensa del ciberespacio a nivel nacional e internacional hasta llegar a su acogida en países como Colombia, que muestra avances en legislación, instituciones, funciones y operaciones superiores a otros países en Latinoamérica dada las condiciones internas y de potenciales amenazas externas, sin importar el ambiente en que se desarrollen y los métodos o medios que se requieran (La República, 2020).

En consecuencia, a lo anteriormente relacionado, me permito establecer una tesis, respecto a cómo los distintos factores armados de inestabilidad (Grupos Armados Organizados, Grupos Delincuenciales Organizados, el narcotráfico y el crimen organizado trasnacional), son determinantes respecto a la Ciberseguridad y la Ciberdefensa de nuestra Nación y como a través de las distintas acciones preventivas en términos cibernéticos se pueden mitigar estos fenómenos, maximizando las entidades existentes para tal fin.

Metodología

Este artículo sobre *Los factores armados de inestabilidad frente a la Ciberseguridad y la Ciberdefensa Nacionales* se desarrollará bajo la metodología de investigación cualitativa en el cual se desarrollará un proceso inductivo, recurrente, con análisis múltiples de las realidades subjetivas y/ objetivas que se puedan destacar, dentro de la comprensión de los lineamientos legales para desarrollar la Ciberdefensa y la Ciberseguridad en Colombia desde el momento en que se establecen las directivas para la creación a cargo de las Fuerzas Militares y de la Policía Nacional de Entidades destinadas a la protección del ciberespacio (Hernández et al., 2014).

Bajo las características en la búsqueda de información de planteamientos más abiertos que van enfocándose en la búsqueda de funciones, estrategias y acciones para neutralizar los Factores de Inestabilidad, conducido por los ambientes naturales destacados, en este caso, el ciberespacio, la ciberguerra, las ciberarmas usadas por grupos armados organizados y grupos armados residuales entre los más importantes.

Trabajando en conjunto, con el método descriptivo caracterizado por clasificar y caracterizar la evolución creciente de las políticas sobre seguridad y defensa en el

ciberespacio, mostrando, como las amenazas han evolucionado en este ámbito en países con alta capacidad tecnológica hasta llegar a países como Colombia, donde el uso de internet se masificó y tuvo que priorizarse al mismo tiempo el cuidado de los usuarios en la red; refiriendo las causas que dieron origen al Convenio de Budapest, punto de partida para el desarrollo de políticas en ciberseguridad y ciberdefensa en Colombia, por medio del CONPES 3701 de 2011, para luego pasar al CONPES 3854 de 2016 quienes pasaron de ciberseguridad y ciberdefensa en Colombia a establecer una política de seguridad digital en la nación, repartiendo tareas entre las Fuerzas Militares y la Policía Nacional por medio del COLCERT o Grupo de Respuestas a Emergencias Cibernéticas de Colombia, el Comando Conjunto Cibernético CCOCI y el Centro Cibernético Policial con su CAI Virtual, vitales para enfrentar esta amenaza en el territorio nacional (Hernández et al., 2014).

Resultados que se extraen de los datos encontrados por la información cualitativa recopilada de los documentos principales para el desarrollo de políticas de seguridad en el ciberespacio, y una descripción de su evolución con normas internacionales y nacionales en pro de su funcionamiento, con algunas estadísticas garantes del crecimiento de los delitos en el ciberespacio, la entidad que los neutraliza y el tipo de delito ejecutado (Hernández et al., 2014).

Marco teórico y conceptual

Para desarrollar el marco teórico y conceptual en este artículo, se toma como referencia la Teoría de la Información encargada de las condiciones técnicas que permiten la transmisión de mensajes, siendo referente en estas páginas para explicar la evolución y aplicación de la ciberseguridad y ciberdefensa en Colombia, mostrando objetivos, funciones e instituciones encargadas para aplicarla, sustentado por el método aplicado por Weaver, al hacer la descripción de "las fuentes de información encargadas de transmitir el mensaje por medio de señales enviadas de comunicación hacia el receptor" (López, pp.2-3, 1998), es decir, desglosar la información expuesta respecto a ciberseguridad y ciberdefensa tomando textos académicos nacionales, españoles y convenios internacionales respecto a la protección en la red, describiéndole al lector la línea de tiempo, los casos relevantes en su aparición, su consolidación normativa internacional, para aterrizarla en las políticas respectivas en Colombia, otorgando un mensaje, por un medio escrito para que el lector lo analice y construya su propio criterio.

En consecuencia, el cuidado y la protección de los datos y la información que se produce a diario en cada nación, y que circulan en la red, debe llevarse a cabo bajo el respectivo proceso que permita salvaguardar los intereses privados y públicos de las naciones alrededor del mundo, este hecho es ratificado por el Convenio de Budapest quien dio el permiso para que cada país desarrolle su respectiva legislación acerca de la prevención y

contención de dicha amenaza en sus territorios, por lo tanto, se hace necesario conocer algunos de los conceptos fundamentales en este escenario, como método de guerra y preparación en el ataque (Convenio de Budapest, 2001).

Para Colombia, la seguridad digital, encierra actividades tanto de ciberseguridad y ciberdefensa de acuerdo al documento CONPES 3854 de 2016 Política Nacional de Seguridad Digital y posterior el documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital, los cuales buscan promover un ambiente seguro y motivar el desarrollo económico y social del país a través de un entorno confiable para los ciudadanos y las empresas, sin embargo frente a la materialización y potencial afectación a la seguridad nacional es importante entender los siguientes conceptos:

1. **Ciberespacio:** Definido por la Junta Interamericana de Defensa como entorno conceptual en el que se produce la comunicación a través de redes informáticas, este concepto se materializa por la interrelación de elementos específicos como: la infraestructura de tecnologías de información y comunicaciones, el software, la información, los protocolos de transporte, la energía eléctrica y las personas (Junta Interamericana de Defensa, 2020). Además, el concepto del ciberespacio en Colombia es concebida como una red mundial abierta que ha reforzado la educación, la innovación tecnológica y el intercambio de conocimientos e ideas (Becerra, Sánchez, Castañeda, Bohórquez, Páez, Contreras, León, 2019), moldeado por el uso de la electrónica y del espectro electromagnético para crear, modificar, guardar, intercambiar y explotar información a través de sistemas de interconexión e internet (Vera, Prieto y Garzón, p.510, p. 2)
2. **Ciber amenaza:** Definida como una fuente potencial de perjuicio, externa o interna, a algún activo de la organización que se materializa a través del ciberespacio (Junta Interamericana de Defensa, 2020).
3. **Ciber arma:** Definido como aquel software específicamente diseñado para causar daño o efecto perjudicial a un elemento del ciberespacio, buscando tener consecuencias físicas en los ámbitos de operaciones convencionales (Junta Interamericana de Defensa, 2020).
4. **Ciber fuerza:** Concepto que ha sido adoptado con dos orientaciones, la primera referida a la unidad militar especializada en el combate en el ciberespacio, y la segunda enfocada en la capacidad para desarrollar acciones ofensivas en el ciberespacio (Junta Interamericana de Defensa, 2020).
5. **Ciberataque:** Es entendido como el uso deliberado de una ciberarma, por una persona o de manera automática, para causa un daño o efecto perjudicial a un elemento del ciberespacio de un adversario, pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales (Junta Interamericana de Defensa, 2020).

6. **Ciberdefensa:** Esta comprende actividades defensivas, ofensivas y de inteligencia; y es aquella capacidad organizada y preparada para combatir en el ciberespacio (Junta Interamericana de Defensa, 2020).
7. **Ciberseguridad:** Definida como el conjunto organizado de medidas destinadas a prevenir, evitar y minimizar potenciales daños a redes y sistemas de información propios (Junta Interamericana de Defensa, 2020).
8. **Ciber persona:** Es toda aquella identidad que un usuario del ciberespacio establece en comunidades o actividades online (Junta Interamericana de Defensa, 2020).
9. **Ciber operación:** Es el "conjunto de acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones" (Junta Interamericana de Defensa, 2020, p.15).

Cada una de estas definiciones da un enfoque concreto acerca del objetivo en la seguridad y defensa del ciberespacio y todo lo que conlleva su protección, aunque son algunos, de los muchos conceptos, que mantiene en retrospectiva lo esencial para entender el escenario completo de la ciberseguridad y ciberdefensa nacional, enfocados en las acciones que pueda realizar el cibercrimen y con él, estar atento al uso de las ciberarmas para contrarrestar, evitar o contener un ciberataque. Haciendo uso de la teoría de la información, capaz de reunir en un mismo lugar y en un mismo contexto la importancia del análisis en ciberseguridad y ciberdefensa para enfrentar las amenazas nacionales en la red. Con estas bases, se debe hacer un repaso sobre la aparición de la ciberseguridad en el mundo, su objetivo principal y que se ha hecho hasta ahora para enfrentar a los delincuentes en el ciberespacio (La República, 2020).

Historia de la ciberseguridad y ciberdefensa.

La información siempre ha sido un bien valioso que se ha intentado proteger de las amenazas existentes, un ejemplo concreto es la obtención y desarrollo de la máquina de cifrada alemana conocida como Enigma, durante la Segunda Guerra Mundial (1939-1945), en ese entonces el sistema de protección de la información fue atacado y descifrado por los británicos, mostrando la vulnerabilidad para materializar una amenaza y atacar un sistema, además de la precaria protección que recibió el sistema de cifrado para evitar el ataque y su materialización, un efecto que con el paso del tiempo, tomo mayor relevancia, en tanto que los medios para reunir, almacenar y mantener información se volvían más sofisticados, así como los medios y métodos empleados para obtenerla de manera ilícita, degradarla o manipularla de forma indebida (Ferrando, 2018).

Citadas consideraciones no podrían ser ajenas a la seguridad en la red de redes, la internet, un escenario que compila y genera acceso a millones de datos por minuto y que

puede afectar de igual forma millones de usuarios o sistemas, por la cual las autoridades empezaron a tomar medidas al respecto, sobre cómo abordar el ciberespacio, quien lo juzga y como se juzga. Este proceso, se inició en países desarrollados en los cuales la penetración de la tecnología avanzo a pasos agigantados y que debido al abuso de los usuarios se empezaron a generar efectos negativos relevantes en la economía y en la sociedad (Derechos Digitales, 2018). El ciberespacio se convirtió en un campo ambiguo y escurridizo en el cual los delincuentes podían aprovechar su anonimato y difícil detección.

El fraude bancario por medios electrónicos, la intrusión en servidores informáticos o el hurto de bases de datos se volvieron comunes y con poca acción de prevención. Fue hasta 1986 y con una perspectiva local que en Estados Unidos se desarrolló, la Computer Fraud and Abuse Act (CFAA) con los primeros cuerpos legales y mecanismos de respuesta frente a este tipo de amenazas a nivel local, sin embargo, su efectividad fue bastante cuestionada por el incremento del crimen trasfronterizo producto de la masificación de internet y la sofisticación de la tecnología computacional. Tiempo después, en 1995, el Consejo de Europa creo un comité de expertos informáticos con el fin de producir recomendaciones sobre delitos informáticos, siendo la base excepcional para la redacción y aprobación del Convenio sobre Ciberdelincuencia mejor conocido como Convenio de Budapest (Derechos Digitales, 2018).

El convenio de Budapest fue aprobado en 2001, atendiendo las preocupaciones del momento como la necesidad de estandarizar los sistemas penales de justicia y la urgencia de crear mecanismos de cooperación internacional contra la cibercriminalidad, una respuesta activa hoy en día en la mayoría de los países del mundo como respuesta a una continua evolución y aumento de la criminalidad en el ciberespacio (Convenio de Budapest, 2001).

Uno de los primeros casos detectados se presentó a finales de los años de 1980, cuando se volvieron populares los ataques con virus en los ordenadores independientes, inicialmente tomados como bromas, pero a medida que fueron incrementando su número se emplearon como medio destructivo que tenían como propósito interrumpir el flujo de información constante o el buen funcionamiento de los equipos en empresas y a los ciudadanos, como respuesta se desarrolló el antivirus con el fin de detener este tipo de ataques y mantener a salvo los ordenadores; el segundo caso fue reconocido a mediados de los años de 1990, fue la primera vez que se dio a conocer el término los hackers, empleado inicialmente para definir a quienes desarrollaban actividades ilícitas como robos, fraudes, accesos no autorizados a sistemas informáticos extracción de información confidencial, entre otras, dando paso a la creciente industria de seguridad en red con el lanzamiento del primer firewall o corta fuegos, necesario para bloquear los accesos no autorizados en el sistema o red informática (Piper, 1997).

El tercer modelo de ataques en la red fue conocido a principios de la década del 2000, combinando ataques a red, software e infraestructuras dando lugar a lo que se conoce como APT's, amenazas persistentes avanzadas por sus siglas en inglés (Advance Persistent Treats) especializados en detectar y explotar las vulnerabilidades en toda la infraestructura, a su vez la industria de la seguridad impulso la promoción de productos para la prevención de intrusiones IPS o puertas de enlaces seguras de la web y del correo electrónico así como mejores antivirus (Piper, 1997); el cuarto momento, se da en la década de 2010 impulsado por el espionaje internacional, permitiendo el acceso a brechas masivas de información personal y la interrupción de internet a gran escala, como respuesta a esta evolución, se crea el ***sandboxing*** y ***Anti-bot*** conocido por su capacidad de mitigación y prevención de ataques. Y, por último, aproximadamente para el 2017, se generan herramientas de hacking avanzadas con un alto componente militar, lo que a su vez daría paso al desarrollo de herramientas para la prevención de amenazas a través de una arquitectura unificada con soluciones avanzadas en tiempo real (La República, 2020).

De esta forma se puede evidenciar como a mejores condiciones de seguridad se presenta una mayor sofisticación de los ataques y ante esta capacidad de ataques, el esfuerzo por incrementar los niveles de seguridad y respuesta a potenciales ataques; lo que convierte este escenario sin lugar a duda en el de mayor evolución, interacción y exposición a las amenazas.

Ciberseguridad en Colombia.

Para entender el escenario de la ciberseguridad y ciberdefensa en Colombia, se debe enfocar la atención en el esquema de seguridad respecto al ciberespacio por parte de los Estados; al entender que una vulnerabilidad identificada en la red y el conjunto de datos e información que se transporta en ella, es capaz de poner en alto riesgo la seguridad nacional. Por ende, la protección del ciberespacio, o conocida en el sistema internacional como ciberseguridad, debe ser atendida desde el más alto nivel de dirección, e irradiada a cada uno de los usuarios finales (Machín & Gazapo, 2016).

Bajo este concepto, la preocupación de los Estados y organismos internacionales se fundamentó en desarrollar una estrategia en torno al concepto de ciberseguridad para proteger a la sociedad de esta nueva amenaza, preservando las libertades y derechos fundamentales de los ciudadanos, bajo la perspectiva global dada por la ONU mediante el convenio global contra el terrorismo desde 1970, unido con el paso de los años al Convenio de Budapest del 2001, por el cual, se ratifica una vez más el compromiso por asegurar el buen uso de internet y la información contenida en ella (Segura, 2017).

En materia de seguridad internacional, la vulneración de derechos tanto privados como públicos, emergentes de una cuarta revolución industrial, merecen la atención de

todos los gobiernos del mundo no solo por los intereses que puedan tener naciones rivales, sino por la proliferación de grupos criminales y el empleo creciente del uso de las tecnologías con fines ilícitos.

Un escenario que no es ajeno para Colombia y que dada su historia de conflicto y problemas internos de seguridad podría desencadenar en una posible guerra doméstica en el ámbito virtual, siendo necesario desarrollar la capacidad para enfrentar la capacidad tecnológica y militar de los Grupos Armados Organizados (GAO) ilegales, los grupos Armados Residuales (GAOR), y los carteles de narcotráfico que delinquen en el territorio nacional, así como de la mano de organizaciones trasnacionales y adicional a esto sin desconocer su gran capacidad financiera y el apoyo que puedan recibir de Estados que quieran desestabilizar el orden nacional o el de naciones que comparten intereses comunes con Colombia (Vera, Prieto & Garzón, 2020).

De cara a afrontar estas amenazas latentes capaces de afectar cualquier escenario, Colombia, en cabeza del Ministerio de Defensa y el Ministerio de Tecnologías de Información y Telecomunicaciones, estableció los lineamientos de política para Ciberseguridad y Ciberdefensa con el ánimo de desarrollar una estrategia que comprometiera a las diferentes partes interesadas en la prevención, detección y respuesta a las mismas, así como fomentando la formación de una cultura cibernética. Siendo así, el Departamento Nacional de Planeación (DNP) materializa el CONPES 3701 del 14 de julio de 2011, lo que a su vez configuro a Colombia como unos de los países referentes en la región en Temas de Ciberseguridad y Ciberdefensa, prevaleciendo siempre la protección y el respeto por los derechos individuales y colectivos de la sociedad (Cujabante et al., 2020).

Este documento CONPES 3701 de 2011 da vida a la ciberseguridad y la ciberdefensa en Colombia, permitiendo establecer instituciones del orden nacional dedicadas a salvaguardar el ámbito cibernético con la creación de un ambiente y las condiciones necesarias para la protección del ciberespacio, esto soportado en tres pilares fundamentales:

1. Adoptar un marco institucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.
2. La capacitación y formación especializada en seguridad de la información.
3. La cooperación internacional y la legislación nacional fortalecidas en estos temas.

Como lo menciona Cujabante (2020) en su artículo Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares (2020), determina los estamentos y funciones principales establecidas en el CONPES 3701 de 2011, le dieron la facultad al Ministerio de Defensa Nacional de manera esencial el abordaje de los asuntos en ciberseguridad y ciberdefensa por medio de resoluciones posteriores

de órganos técnicos y operativos encargados de coordinar y orientar el entorno de la seguridad digital, estructuradas por una comisión intersectorial encargada de la visión estratégica de la gestión de la información y el establecimiento de los lineamientos de política en relación con la gestión de la infraestructura tecnológica, la información pública, la ciberseguridad y la ciberdefensa en el país (CONPES, 2011).

En cuanto a la estructura planteada, se encuentran actores nacionales, representantes del sector académico, el sector privado, expertos internacionales y otras instituciones del Estado, de carácter estricto, el Presidente de la República, el alto asesor para la Seguridad Nacional, el Ministro de Defensa, el Ministro de las Tecnologías de la Información y las Comunicaciones, el Director de Planeación Nacional y el coordinador del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), esta última entidad "es el organismo coordinador a nivel nacional de aspectos de ciberseguridad y ciberdefensa en las acciones requeridas para la protección de la infraestructura crítica del Estado"(Cujabante et al., 2020, p.370). Él se interrelaciona y presta colaboración al Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOCI) de las Fuerzas Militares (Cujabante et al., 2020, p.370).

Comandos encargados de Ciberseguridad y Ciberdefensa en el sector Defensa Colombiano.

Como responsable de la ciberdefensa se encuentra el CCOCI, unidad del Comando General de las Fuerzas Militares, quien delega funciones dentro de las Fuerzas Militares dependiendo de la especialidad y rol funcional. La función inicial plasmada en el documento CONPES era neutralizar y prevenir ataques de amenazas existentes y provenientes del ciberespacio hacia la infraestructura nacional, intereses o valores del Estado colombiano (CONPES 3701, 2011). Posteriormente evolucionaría de conformidad con el proceso de transformación de las FF.MM, pasando a ejercer la Ciberdefensa Nacional y desarrollar operaciones de carácter estratégico para contribuir en la defensa de la nación; el CCP por su parte, se encarga de ofrecer apoyo, seguimiento y protección frente a aquellos delitos ejercidos en el ciberespacio, con ayuda de la investigación, atención, prevención y judicialización de esos delitos (CONPES 3854, 2016). De esta forma la Policía Nacional atiende de manera directa a los ciudadanos en la gestión de incidentes, la investigación, la prevención del delito a través del Comando de Atención Inmediata Virtual (CAI Virtual), quien además recibe todas las denuncias relacionadas de delitos cibernéticos, así como la clasificación de las conductas delictivas encontradas en dichos casos (Cujabante et al, 2020).

Gracias al CONPES 3701de 2011 se derivan dos grandes logros en la política de Ciberseguridad y Ciberdefensa de Colombia:

1. El liderazgo de Colombia a nivel regional en cuanto a ciberseguridad y ciberdefensa, y 2. La implementación de la institucionalidad en la protección del ciberespacio. Plasmadas estas competencias en el primer documento legislativo acerca de la ciberseguridad a nivel nacional, se deriva el CONPES 3854 de 2016, donde se fortalece el sistema de ciberseguridad, catalogándolo como Política Nacional de Seguridad Digital (Cujabante et al., 2020, p.358) con el fin de fortalecer las capacidades múltiples para identificar, gestionar, tratar y mitigar los riesgos en los escenarios descritos anteriormente, además, plantea en las actividades socioeconómicas un nuevo marco de cooperación, colaboración y asistencia necesarios para hacer crecer la economía digital nacional. Haciendo un cambio en el enfoque constructivo de la seguridad del ciberespacio (Cujabante et al., 2020).

El fundamento principal del CONPES 3854 de 2016 es involucrar la gestión del riesgo como uno de los elementos más importantes para abordar el plan de cambio, adoptando los principios: mitigación, identificación, tratamiento y gestión en la planeación de la política que por fases permitirá en el tiempo organizar y delimitar el cumplimiento por medio de las siguientes actividades: 1. El marco institucional en torno a la seguridad digital; 2. Creación de condiciones para la confianza en la gestión del riesgo por medio de la seguridad digital; 3. fortalecimiento de la seguridad y defensa en el entorno digital por medio de la gestión del riesgo; y 4. Generar mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital nacional e internacional.

Por consiguiente, el CONPES 3854 de 2016 establece la gestión del riesgo como el eje articulador de los organismos, instituciones y actores presentes en el ciberespacio, como contribución a las recomendaciones presentadas por la Organización para la Cooperación y Desarrollo Económico (Organización para la Cooperación y el Desarrollo Económico OCDE, 2015) referente a la seguridad digital para la prosperidad económica y social; este cambio se ajusta para salvaguardar los intereses económicos de la nación y que representan gran atractivo para los ciberdelincuentes.

En consecuencia, el Estado colombiano, después de desarrollar el proyecto de seguridad digital en la nación, se adhiere al Convenio de Budapest, responsable del estándar mundial contra la ciberdelincuencia. Restableciendo, la necesidad de mejorar la coordinación y cooperación entre los Estados, por medio de las siguientes expectativas indispensables para fortalecer las capacidades nacionales en prevención, detección, investigación y juicios condenatorios a la delincuencia organizada trasnacional en el ciberespacio: 1. La legislación nacional debe complementarse y actualizarse bajo los estándares internacionales en la lucha contra la ciberdelincuencia; 2. Con los países miembros del Convenio se deben formalizar y dinamizar los canales de intercambio de información como medio facilitador de investigaciones judiciales en los hechos delictivos trasnacionales establecidos (CONPES 3854, 2016).

3. Acceso a proyectos y programas para la transferencia de conocimientos, soporte tecnológico, apoyo investigativo y acciones conjuntas bilaterales y multilaterales en cuanto a la toma de nuevos conocimientos y mejora de procedimientos por parte de los oficiales encargados de este proceso en las debidas áreas de seguridad digital. 4. Mejorar la cooperación internacional en el aspecto judicial, avanzar en los temas de evidencia digital y participación de estrategias conjuntas en materia de ciberdelincuencia (CONPES 3854, 2016).

Basado en dichos aspectos interesantes para Colombia y por los cuales se ratificó junto a 65 países miembros el Convenio de Budapest, este da origen a cada una de las legislaciones, que, hasta el momento, se siguen estructurando por parte de los Estados Miembros, para aplicar su correcto funcionamiento territorial. Hechos establecidos bajo la ley 1928 de 2018. Cada uno de estos aspectos dará un punto de partida para contrarrestar los ataques y efectos de las ciber amenazas, los ciberdelincuentes y sus diferentes métodos y medios empleados para afectar a la población civil y los intereses del Estado colombiano, en procura de combatir con mayor rigurosidad las estructuras delictivas de los grupos delincuenciales organizados, los grupos armados organizados, el crimen trasnacional, comunes y enfáticos en la historia de conflicto colombiano (Ley 1928, 2018).

Capacidades de reacción en Ciberseguridad y Ciberdefensa frente a los factores armados de inestabilidad.

Bajo la perspectiva de las Fuerzas Militares y la Policía Nacional de Colombia de cara al proceso de transformación, afrontando de manera efectiva las amenazas y oportunidades previstas en estos escenarios esenciales en su misión y cambiantes con el paso de los años, se tuvo en cuenta, tres pilares fundamentales para mejorar su capacidad de acción: el primero, la planeación por capacidades; el segundo, la sostenibilidad; y el tercero, el manejo eficiente del gasto público en conjunto con el fortalecimiento del capital humano. Siendo necesarios para enfrentar tanto tradicionales como nuevos retos presentados por las amenazas existentes que dominan otros escenarios, como lo es el ciberespacio, sobre todo para combatir crimen y delincuencia (Hernández, s.f, p.15). Al encontrar un nuevo espacio, más grande e inexplorado, las FF.MM lograron, en un marco de integración y complementariedad entre las Fuerzas, unir estrategias para enfrentar a los factores armados de inestabilidad, neutralizados con la ayuda de instituciones específicas para ese tipo de espacio de guerra (Cubillos, 2017).

Para crear esas nuevas capacidades y áreas específicas que permitieran enfrentar las amenazas en el ciberespacio, se tuvo en cuenta el paradigma de Likke usado por la Fuerza Pública para planear las capacidades desde el nivel político estratégico hasta los niveles operacional y táctico, en el cual se asegura mantener un equilibrio indispensable

entre fines, medios y los modos necesarios para argumentar la necesidad nacional frente a nuevos espacios usados por el crimen, es decir, si una nación entiende que debe tener coherencia entre los fines (lo que se quiere lograr), con los medios (la forma como se va a desarrollar) y el modo (como lo comunico para llevarlo a cabo), se obtiene un resultado conjunto de la operación, eficaz y eficiente al escuchar todos los frentes y sus necesidades (Hernández, s.f, p.17).

En consecuencia, la implementación de dicho modelo en las FF.MM define áreas misionales, campos de acción, análisis de los diferentes componentes de sus capacidades y el conocimiento de conceptos y enunciados requeridos en la metodología, hechos que permitieron la entrada de la ciberseguridad y ciberdefensa en el país. Esta estructura, a su vez, le permite a las Fuerzas Militares, una organización garante de ventajas estratégicas, administrador eficiente de los recursos, integrando las capacidades desarrolladas que facilitan operaciones conjuntas, coordinadas, combinadas e interagenciales, con una capacidad disuasiva frente a potenciales agresores o amenazas a la integridad territorial, el aire, el espacio y el ciberespacio (Hernández, s.f, p.18).

De acuerdo con lo anterior, las Fuerzas Militares abordan el ciberespacio como ámbito estratégico, operativo y táctico, para organizar, entrenar y equipar a sus hombres capaces de aplicar medidas de prevención, disuasión, contención, protección y reacción, fortaleciendo las capacidades de Ciberdefensa y la lucha frente a las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país y poner en riesgo la seguridad Nacional.

Con ello, las tareas dispuestas para la ciberseguridad y ciberdefensa en Colombia, se redactaron y aprobaron con ayuda del Ministerio de Defensa Nacional, el Congreso de la República y las iniciativas de los planes de desarrollo sostenible de los últimos tres gobiernos para darle vida y activación al Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT como organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa y que tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional, al Comando Conjunto Cibernético (CCOCI) en el Comando General de las Fuerzas Militares con la misión de ejercer la ciberdefensa de la nación y llevar a cabo operaciones cibernéticas de nivel estratégico que contribuyan a garantizar la defensa y seguridad de la nación, y al Centro Cibernético Policial CECIP, responsable de la ciberseguridad ciudadana y la atención y respuesta frente al ciberdelito y cibercrimen, cada una de ellas con unas funciones indispensables para enfrentar las amenazas en el ciberespacio (Realpe & Cano, 2020).

En el 2014 y 2015, se establecieron mesas de trabajo en colaboración con expertos nacionales y extranjeros de Estados como Canadá, España, Estados Unidos, Estonia, Corea del Sur, Israel, Reino Unido, República Dominicana y Uruguay, organismos

internacionales como el Foro Económico Mundial, la OCDE, el Consejo de Europa y la INTERPOL, sin olvidar el apoyo de la OEA para establecer las políticas, la estructura jurídica y funciones requeridas para dar vida al COLCERT, el CCOCI, el CECIP, y las Unidades Cibernéticas en cada una de las Fuerzas, para la gestión efectiva de la ciberseguridad y ciberdefensa del sector público y privado, detallando el enfoque nacional de riesgos, el marco institucional, el proceso sistemático para involucrar a todos los interesados y adoptar una estrategia de protección y defensa de las infraestructuras críticas cibernéticas nacionales al mismo tiempo que fortalecía todas las necesidades operativas, administrativas, humanas, científicas, tecnológicas e infraestructura física de las instituciones (CONPES 3854, 2016).

En este orden de ideas es importante destacar la misionalidad del COLCERT, quien a través del desarrollo de estrategias y como ente articulador facilita la atención y gestión de incidentes de carácter nacional, contribuyendo eficazmente al logro de las políticas de gobierno en materia de seguridad digital (Comando General de las Fuerzas Militares, 2016).

En la actualidad, el COLCERT en coordinación con el CCOCI y el CECIP, reúnen sus capacidades fortaleciendo el sistema de toma de decisiones, entre ellas: 1. Capacidad de análisis y fuga de información, en el cual se condensa la protección, generación, respaldo y apoyo a la información en el escenario requerido; 2. Capacidad de búsqueda y recolección de información: estableciendo método, medio, forma y lugar para neutralizar la amenaza que ha permeado el ciberespacio; 3. Capacidad de planificación, ejecución y mitigación: se desarrolla el proceso de capacitación, sensibilización y prevención de las amenazas en el ciberespacio a la población civil, por medio de campañas, asesorías y demás instrumentos necesarios para cuidar la información que se da en redes; 4. Capacidad de análisis y control: en el cual se redacta y vigila las normas, leyes y reglamentos acerca del buen uso del ciberespacio, así como el establecimiento de funciones estadísticas para comparar la eficiencia de las áreas en el campo de la ciberseguridad y ciberdefensa nacional en un periodo de tiempo determinado (Camacho, 2016).

El Comando Conjunto Cibernético CCOCI, reconocido como el ente rector para el direccionamiento, planeación, integración, coordinación, sincronización y ejecución, de operaciones cibernéticas, se relaciona y mantiene coordinación con las Unidades Cibernéticas del Ejército, Armada y Fuerza Aérea, articulando e integrando capacidades para el desarrollo de operaciones de Ciberseguridad y Ciberdefensa, y consolidando esfuerzos a nivel estratégico para la seguridad y defensa de la nación en el ciberespacio (Ministerio de Defensa Nacional, 2012).

Las Unidades Cibernéticas de las fuerzas militares, cumplen un papel fundamental en el aseguramiento de los medios y recursos propios de su fuerza, propendiendo por la obtención de una ventaja estratégica en el ciberespacio que contribuya en el dominio

propio de su rol tierra, mar, aire y espacio, y que garantice la libertad de acción, en el Ejército Nacional se encuentra el Grupo de Apoyo de Comunicaciones y Ciberdefensa, en la Armada Nacional la Dirección Cibernética Naval, y en la Fuerza Aérea Colombiana la Dirección Cibernética Aérea y Espacial (Realpe & Cano, 2020).

Para ahondar un poco más y resaltar la importancia de las unidades cibernéticas se debe precisar qué; el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional se encarga del planeamiento, ejecución y supervisión de las operaciones militares del Ejército en las áreas C5, por medio de herramientas tecnológicas interoperables para los diferentes niveles de Mando, ejerciendo el desarrollo de operaciones militares respecto de quien lo dirige y el tipo de misión que se desarrolle (Ministerio de Defensa Nacional, 2019). Como complemento, el Departamento de Comunicaciones y Ciberdefensa Cede-6 del Ejército, permite asesorar y recomendar a la jefatura de Estado Mayor de Planeación y Políticas en los temas de ciberdefensa (C5) para facilitar la toma decisiones en el planeamiento estratégico de la fuerza al difundir los lineamientos de planeación y políticas para orientar los procesos y capacidades del Ejército en esta área, en especial con la gestión de información, datos, aplicaciones y capas de tecnología para el mejoramiento del uso de TI (Vera, Prieto & Garzón, 2020).

La Dirección Cibernética Naval ARC: se encarga de desarrollar y proyectar las capacidades humanas, técnicas y operativas para prevenir, detectar, neutralizar y contrarrestar toda amenaza o ataque de naturaleza cibernética al vulnerar los intereses navales y aquellas en conjunto con el CCOCI establecidas como determinantes en la protección de la nación (Ministerio de Defensa Nacional, 2019b).

Así mismo, la Dirección Cibernética Aérea y Espacial de la FAC: se encarga de planear, conducir y ejecutar operaciones de Ciberseguridad y Ciberdefensa para propender la protección de la infraestructura crítica cibernética necesaria para cumplir con el propósito principal: cuidar el ciberespacio nacional en el marco funcional de la Fuerza Aérea Colombiana (Ministerio de Defensa Nacional, 2019).

Cada una de estas unidades ha puesto en marcha los principios de la ciberseguridad y ciberdefensa, útiles para el desarrollo de tareas analíticas en el campo del ciberespacio, en las cuales se aplica la integridad, disponibilidad y confidencialidad, complementarios con los principios de la ciberdefensa que procuran las buenas prácticas de la seguridad informática sin necesidad de generar vulnerabilidades que a largo plazo se transformen en riesgos, haciendo uso de estrategias adecuadas encaminadas a la prevención en el ciberespacio como por ejemplo: las guías de uso para la implementación de protocolos y buenas prácticas, para el fomento de la cultura y sensibilización del cuidado y uso de herramientas fáciles de manejar y adquirir para prevenir riesgos en el ciberespacio. El uso de herramientas para aspectos como prevención, detección y neutralización de software malicioso, y fortalecer las unidades con personal especializado.

Las unidades cibernéticas se convierten en parte esencial en esta cadena jerárquica porque de ellas emana los trabajos interinstitucionales en materia de infraestructuras crítica cibernética, y en el desarrollo de políticas y planes de protección en ciberseguridad para sus activos estratégicos, acciones que se materializan e irradian entre los diferentes sectores del país a través de redes de colaboración para compartir información de amenazas y alertas tempranas como medida preventiva, y de mitigación de posibles afectaciones. Una actividad que se destaca son los ejercicios técnicos, ciber-olimpiadas, ejercicios de gestión de crisis cibernética nacional y reuniones de infraestructura crítica, simulacros, riesgo operacional y ciberdefensa, mediante los cuales se fortalecen los lazos de cooperación y las capacidades individuales desarrolladas (Vera, Prieto & Garzón, 2020). Al mismo tiempo, se propician espacios académicos, para la generación de doctrina, como los tanques de pensamiento, que a su vez ayuda en la diferenciación de roles y la especialización de las unidades (Vera, Prieto & Garzón, 2020).

En cuanto al CECIP o Centro Cibernético Policial , sus capacidades desarrolladas están focalizadas para la detección, prevención, investigación, análisis, respuesta y recuperación ante las Ciberamenazas consolidadas en un eje jurídico y constitucional constituido en la resolución 05839 del 31 de diciembre de 2015, en la cual se sustenta el desarrollado de estrategias, programas y proyectos para la ciberseguridad y ciberdefensa en la protección de información y los datos circulantes de toda la sociedad colombiana en el ciberespacio (p.32). Además, atiende necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática de la institucionalidad policial (Policía Nacional de Colombia, 2010).

Así mismo, el CECIP tiene como funciones de acuerdo con lo establecido por Ministerio de Defensa Nacional (2019):

1. Adelantar los procesos misionales relacionados con detección, prevención, análisis, reacción, investigación, respuesta, judicialización y persecución del ciberterrorismo y la ciberdelincuencia en Colombia.
2. Genera vínculos de cooperación para observar el cibercrimen en compañía de organismos y agencias de cooperación multilateral, al establecer el Centro de Capacidades para la Ciberseguridad en Colombia C4.
3. Por medio de servicios proactivos, toma medidas para proteger y asegurar las plataformas tecnológicas, prever futuros ataques, dificultades o eventos que afectan la disponibilidad, confidencialidad e integridad de la información.
4. Con la ayuda de servicios reactivos actúa de manera eficaz ante incidentes o vulnerabilidades existentes que surgen de requerimientos, eventos o incidentes en la protección del ciberespacio nacional.

Cada una de estas funciones, muestra el compromiso de la Fuerza Pública, en la defensa y seguridad del ciberespacio, reflejando la separación de misiones, tareas y

operaciones, de acuerdo a los roles y funciones de cada una de ellas, pero demostrando en todo momento su complementariedad y capacidad de integración ,logrando con ello continuar en la ardua tarea de ser referentes regionales, en ciberseguridad y ciberdefensa, demostrado a través de los logros alcanzados, la generación de doctrina y la conformación de una estructura operacional, táctica y estratégica que contribuya al logro de los fines del estado (Policía Nacional, 2021).

En el campo operacional de la ciberseguridad y ciberdefensa en Colombia, el trabajo en conjunto facilita la toma de decisiones frente a potenciales amenazas en el ciberespacio; surgen con ellas herramientas y tácticas para neutralizarlas, un ejemplo; para prevenir la fuga y robo de información, se utilizan herramientas y se establecen políticas de prevención a su vez a través del análisis de eventos presentados se establece el modus operandi, permitiendo con ellos generar escenarios de prueba con los que a futuro se pueden neutralizar, reduciendo su probabilidad de afectación o logrando una adecuada mitigación de su impacto. Mejorando la confidencialidad, la integridad de la información y mantener los principios de disponibilidad (Ministerio de Defensa Nacional, 2019b).

Quizás la capacidad que ha tenido mayor evolución a nivel de unidades cibernéticas en el país es la gestión de incidentes de seguridad de la información, implementando herramientas que facilitan el intercambio de información oportuna, así como la integración de información de diversos sectores, favoreciendo la protección de las Infraestructuras Críticas Cibernéticas Nacionales-ICCN con el fin de neutralizar toda actividad maliciosa que pretenda atentar contra su normal funcionamiento, lo anterior sumado a la implementación de medidas activas y pasivas para la prevención y detección de amenazas, aprovechando el uso de nuevas tecnologías, sin desconocer la importancia del talento humano cada día más profesional y especializado (Ministerio de Tecnología, Información y Comunicaciones, 2012).

El enfoque en este caso es prevenir al usuario sobre los posibles ataques que se pueden presentar en sistemas nuevos como antiguos, manteniendo monitoreado el servicio, analizando los patrones sospechosos y adelantar alertas cuando se presenten accesos inusuales.

De igual forma, para neutralización de amenazas, se emplea las técnicas y tácticas especiales como el contra sabotaje, contraespionaje, contra subversión, explotación y proyectos especiales enfocado en el amplio conocimiento de la amenaza real y potencial, estableciendo un ejercicio meticuloso a la hora de desempeñar su papel de detección. En este caso, cada una tiene una tarea fundamental como se describe a continuación: 1. Contra sabotaje: se detectan ataques cibernéticos dirigidos a detener o neutralizar la continuidad de las operaciones y busca irrumpir en los activos de la nación; 2. Contraespionaje: empleado al detectar una amenaza específica, generadora de ataques impulsados para robar información de la infraestructura de la nación, se debe

neutralizar de inmediato y evitar la afectación en nuestros sistemas; 3. La contra subversión cibernética enfocada en campañas de prevención social contra las amenazas en sitios web, evidenciando en los diferentes escenarios en los cuales se puede desarrollar a través del hacktivismo, o el empleo de técnicas y tácticas anti desconfiguración de antipishing y ataques a dispositivos móviles (Camacho, 2016). 4. Explotación: en este espacio no se escatima esfuerzos para conocer a fondo la amenaza existente, observando su composición y capacidades que más adelante funcionaran para estructurar defensas sólidas en la infraestructura tecnológica y los objetivos estratégicos con el apoyo del centro de operaciones de seguridad SOC; 5. Proyectos especiales: encaminados al uso de capacidades enriquecedoras en el campo de la ciberseguridad y ciberdefensa, trayendo consigo nuevas tecnologías, herramientas, acciones y estrategias para enfrentar las amenazas latentes y existentes en el ciberespacio colombiano (Cubillos, 2017).

Al finalizar los esquemas usados en ciberdefensa se complementa su actuar con tres etapas esenciales en el proceso de neutralización de las amenazas; la primera de ellas, la prevención a través de las capacidades, procesos y procedimientos desarrollados en el centro de operaciones de seguridad. La etapa de mitigación requiere de la elaboración clara de protocolos que permitan reducir al máximo el impacto generado por la materialización de las amenazas. La etapa de análisis de riesgos se encarga de la identificación y evaluación permanente de los mismos, contribuyendo con la anticipación y su atención (Centro de Estudios de Política y Relaciones Internacionales, 2016).

En cuanto a la ciberseguridad ciudadana, es importante destacar el papel que desarrolla el Centro Cibernético de la Policía en Colombia, con la implementación y puesta en marcha del CAI Virtual, el cual recibe cientos de denuncias diariamente por parte de los ciudadanos relacionadas con delitos generados desde el ciberespacio, tarea que se acrecienta exponencialmente por el masivo uso de internet. Esta entidad se encarga de atender diversos tipos de crímenes, investigar el modus operandi, y desarrollar acciones, detecciones y arrestos, si es el caso, aspecto respaldado por medio de la capacitación constante de los integrantes de la policía encargados de esta unidad operativa, la debida atención a las alertas tempranas, el análisis de casos en movimientos inusuales del cibercrimen y especialmente la efectividad de las respuestas por medio de la toma de decisiones efectivas (Policía Nacional de Colombia, 2020).

Durante el periodo 2018-2019 se evidenciaron los siguientes resultados en cuanto a la Estrategia Integral de Ciberseguridad: 23 operaciones desarrolladas, 5.560 portales web bloqueados, 549 análisis de malware en celulares, 253 capturas por la ley 1273 de 2009, en el periodo comprendido del 07 de agosto de 2018 al 16 de julio de 2019, inauguración del laboratorio de Análisis de Código Malicioso (malware), creación del equipo

de respuesta ante emergencias informáticas del Estado (CSIRT), 47.206 gigabytes de información digital analizada y la integración del centro de capacidades para la seguridad de Colombia C4 (Ministerio de Defensa Nacional, 2019).

Así mismo, el informe sobre cifras de cibercrimen en el país durante el 2020, de acuerdo a CAI Virtual (2020), destaca lo siguiente:

1. El Centro Cibernético Policial con la ayuda del CAI Virtual ha atendido 11.950 incidentes y 7.862 correos gestionados durante el 2020
2. 640 muestras de malware analizadas
3. 180 charlas preventivas dirigidas a padres de familia y profesores
4. 845 comunicaciones Internacionales Intercambiadas

En cuanto a los resultados operacionales se destacaron los siguientes aspectos: 1. Páginas bloqueadas con material de abuso sexual infantil 5.165; 2. Portales suspendidos con contenido malicioso como spam (9), malware (102), phishing (371), en total 482; 3. Alertas generadas en redes sociales, medios de prensa y canales de cooperación internacional 541; 4. Noticias falsas identificadas y desvirtuadas con las fuentes oficiales y validadores autorizados 151; 5. En capturas, de las cuales 27 son por el delito de pornografía con menor de 18 años 155 (CAI Virtual, 2021). Estas cifras muestran como con el incremento del uso de internet y las tecnologías de la información y comunicación, aumenta la ventana de oportunidades para los ciberdelincuentes que ven en este el escenario propicio para incrementar su actividad delictiva, obtener mayores beneficios y reducir aún más su nivel de exposición ante las autoridades. En ellas también se destaca las ciudades con mayor afectación en esta modalidad de ciberdelitos, Bogotá, por ejemplo, es la ciudad más afectada con 12.981 delitos relacionados con esta práctica, sigue Medellín con 3.442 ataques, luego Cali con 2.363, Barranquilla con 1.809, Bucaramanga con 1.256 delitos en este aspecto y Cartagena con 887 delitos relacionados a ciberseguridad, lo cual va directamente desarrollado con el nivel de acceso a sistemas informáticos y la mayor utilización de dispositivos de acceso de a la red (CAI Virtual, 2021).

Se ha dado un breve vistazo de las capacidades desarrolladas por la Fuerza Pública para identificar, atender y neutralizar el avance de los delitos en el ciberespacio, así como amenazas a la seguridad y defensa de la nación, ciberdelincuentes que están en búsqueda de información necesaria para su accionar delictivo, agentes internos o externos que pretenden desestabilizar la nación, potenciales agresores que buscan reducir la capacidad de respuesta de la fuerza pública. Así mismo, se da un breve vistazo de los factores de inestabilidad presentes en el ciberespacio, cada uno catalogado en manera diferente para que la fuerza correspondiente se haga cargo de este, con la estructura y operación requerida, aspectos que se detallaran en el siguiente apartado.

Líneas de acción para contrarrestar los ataques por parte de los factores armados de inestabilidad en el ciberespacio.

Después de analizar y observar las actividades desarrolladas por el Grupo de Respuestas a Emergencias Cibernéticas de Colombia COLCERT, el Comando Conjunto Cibernético y Centro Cibernético Policial así como vistos datos e información de modus operandi y estadísticas de delitos ejercidos en el ciberespacio, se resalta el esfuerzo desarrollado por establecer marcos jurídicos basados en normativa internacional que parte de la Asamblea General de las Naciones Unidas, la Unión Europea y demás organismos rectores que impulsan el cuidado del ciberespacio y que a la fecha si bien se pueden presentar algunos vacíos a nivel nacional , demuestran el compromiso y avance logrado en relación con otros países de la región, claramente reflejado a través de la implementación de Decretos, normas, y doctrina que enmarcan el accionar de las instituciones tanto dentro de la Fuerza Pública como en los demás estamentos del Estado para combatir el crimen en el ciberespacio, delegando responsabilidades y estableciendo estructuras para enfrentar esas amenazas, mitigar su impacto y en el mejor de los casos lograr su total neutralización (Ospina & Sanabria, 2020).

Sin embargo, la dinámica delictiva y las características evolutivas del accionar en el ciberespacio, pone en riesgo la vigencia y aplicabilidad de las normas, así como la eficiencia de las instituciones establecidas para proteger el ciberespacio, los nuevos escenarios cada vez más inciertos obligan al Estado y sus instituciones a estar en permanente evolución y lograr estar un paso delante de los retos que demanda la ciberseguridad. Hablar de ciberdelincuentes no solo se trata de una persona común que por diferentes circunstancias se refugia en el delito para sobrevivir, también en medio de esta infracción de leyes y seguridad en el espacio, convergen factores armados de inestabilidad como los grupos armados ilegales que con el uso ilegítimo de la fuerza coaccionan a la población civil para lograr sus objetivos, principalmente económicos; los Grupos Armados Organizados (GAO), los Grupos Delictivos Organizados (GDO) junto al narcotráfico y al crimen trasnacional se tornan en una amenaza para la seguridad y defensa del Estado Colombiano en un nuevo ámbito, el ciberespacio. Con un potencial de incursión en el cibercrimen cada vez más alto por las alianzas establecidas entre ellos tras encontrar objetivos comunes y solo bajo un corto período para actuar sin mayores contratiempos y así conseguir el objetivo deseado en medio de una red de información completa y esencial para sus intereses colectivos (Ospina & Sanabria, 2020).

Los hechos generados por estos grupos se fortalecen y logran establecerse en áreas grises de difícil acceso para el estado y sus instituciones, conllevando de manera progresiva al incremento del accionar delictivo y llenando espacios dentro de la población basada en la intimidación o los recursos económicos. De igual forma, el ciberespacio se convierte en un terreno propicio para el desarrollo de actividades delictivas al permitir

escenarios de gran accesibilidad, difícil control y limitaciones de seguridad, convirtiendo al ciberespacio lamentablemente en un aliado para la ilegalidad, al poder llegar a una gran cantidad de personas para estafar, engañar o robar y salir del escenario sin ser detectado (Organización de las Naciones Unidas, 2021). Accionar que sin lugar a dudas enciende las alarmas de la Fuerza Pública, obligándolas a innovar en sus estrategias de neutralización y minimización de crímenes en el ciberespacio, ya que la convergencia criminal no da espera para combatirlos y para hacerlo es importante tener en cuenta aspectos como los factores armados de inestabilidad, la convergencia criminal, el ecosistema criminal entre otros.

En Colombia hay varios factores armados de inestabilidad, entre ellos se destacan: las GAO, GDO, narcotráfico y crimen trasnacional, cada una con un enfoque diferente, por ejemplo, las GAO son aquellas que poseen un mando determinado, ejercen control sobre una parte del territorio, donde desarrollan operaciones sostenidas y concertadas, enfrentadas de manera violenta contra el Estado Colombiano y por ende a la Fuerza Pública, hostigan a la población civil y se enfrentan contra otros grupos armados, generando niveles de violencia por encima de los presentados por disturbios y tensiones internas (Función Pública, Ley 1908, 2018).

El segundo factor armado de inestabilidad, las GDO conformadas por tres o más personas, coexistiendo por un gran período, con el fin de realizar delitos establecidos por la Convención de Palermo o aquellos clasificados como delitos graves, para obtener grandes ganancias monetarias directa o indirectamente. Este factor armado solo podrá considerarse con el adjetivo de GDO si así lo determina el Consejo de Seguridad Nacional, así como aquellas que ejecuten crímenes establecidos por el Código Penal Colombiano y definidos por la ley 1908 de 2018 en el artículo segundo. Además, el tercer factor armado de inestabilidad es el narcotráfico, establecido como un fenómeno creciente a raíz de la globalización, conocido a nivel internacional como tráfico de drogas y del cual se derivan otras fechorías, ejerciendo un comercio ilícito mundial donde se une el cultivo, fabricación, distribución y ventas de sustancias que no están avaladas por leyes existentes, capaz de causar fenómenos en las naciones productoras principalmente, como la corrupción, ahondar los problemas sociales actuales y dañar la salud de las personas en general (Comunidad de Policías de América, 2013).

Por último, pero no menos importante como factor armado de inestabilidad, se encuentra el crimen trasnacional, similar a la organización de un grupo criminal o delincuencial, con el objetivo de obtener ganancias monetarias, materiales o financieras por medio de delitos punibles con al menos 4 años de encarcelamiento, cometidas desde un Estado, pero que puede afectar a otros al mismo tiempo, es decir, los agravios se vuelven implicaciones internacionales (United Nation Office on Drugs and Crime, 2021). Dentro de esta conceptualización se obtienen algunos ejemplos como el tráfico de drogas, la

trata de personas, el tráfico ilícito de migrantes, el tráfico ilícito de armas de fuego, el tráfico ilícito de recursos naturales, la venta de medicamentos adulterados, el comercio ilegal de flora y fauna y la delincuencia cibernética. Exponiendo el cibercrimen, como el abuso expandido por la red global de información o Internet para robar datos personales y obtener dinero de manera directa, o promocionando otros delitos, hecho que se vuelve cada vez más peligroso al incluir a gran cantidad de personas, de todas las edades y con las cuales se puede generar todo tipo de abusos, engaños y crímenes, por eso el llamado de alerta a la Fuerza Pública para neutralizarlo en el menor tiempo posible (United Nation Office on Drugs and Crime, 2021).

Estos cuatro factores armados de inestabilidad se vuelven una gran amenaza para la ciberseguridad y ciberdefensa nacional, al establecer alianzas momentáneas y así incrementar sus ganancias cuando coinciden sus intereses a corto y mediano plazo, escenario conocido como Convergencia Criminal, efectuados en territorios baldíos donde la jurisdicción del Estado no ejerce soberanía, permitiendo la instauración de ***reglas*** propias y desarrollar ***acciones*** delictivas y violentas que vulneran a miles de personas en la nación y que repercute en otros escenarios. Reportando otro elemento para encontrar la complexión de esta amenaza al ciberespacio nacional, la convergencia criminal (Ospina, Riveros & Barrera, 2018).

La convergencia criminal, se origina del concepto *ecosistema criminal* donde se une, funciona y opera el mundo criminal al interactuar con el mundo físico, es como en ciencias naturales se le conoce al conjunto de animales, plantas, y cuerpos inertes, agua y demás elementos ambientales conviviendo en un mismo espacio, cada uno ayuda y coopera entre ellos para poder mantenerse, hechos semejantes a la convivencia y aceptación de los criminales en un mismo espacio, que en este caso se conoce como terrenos o espacios baldíos, aquellos donde el Estado no ejerce jurisdicción, dejando a merced de los criminales *la ley y el orden* y como fuente de trabajo las actividades ilícitas desplegadas a gran escala con la ayuda de la globalización donde se permite la interconexión de mercados en todo el mundo, rutas de comunicación que llevan información, dinero, mercancías, materias primas y demás para el crecimiento económico de las naciones y que los criminales aprovechan para ejercer sus actividades al margen de la ley, afectando no solo a un país sino a varios al mismo tiempo (Álvarez & Rodríguez, 2018, pp.9-20).

Esta unión de eventos desafortunados, origina la convergencia criminal, como aquel escenario donde se reúne el crimen organizado trasnacional, el terrorismo y la insurgencia como amenazas vinculadas en una red de conflicto actual y futuro que no se pueden identificar con claridad para catalogarlas como crimen o guerra. Al incluir en el mismo aspecto nuevos actores políticos y económicos, tendencias del crimen trasnacional que se vinculan en puntos o nodos comunes, tan sutiles y eficientes que pueden infiltrarse en cualquier escenario y desarrollar con facilidad cualquier actividad delictiva

sin la intervención de las fuerzas del Estado encargadas de la protección de la nación. Mostrando la rapidez de las acciones establecidas y los socios, ascendentes estratégicos capaces de otorgar distracciones en los momentos en que se lleva a cabo el delito (Álvarez & Rodríguez, 2018, p.11).

Este espacio alberga un ecosistema criminal en el cual interactúan forajidos y población civil principalmente, en medio de un territorio geoestratégico fundamental para la entrada y salida de material, herramientas y productos delictivos, así como productos esenciales, alimento, agua y transporte. En este mismo territorio, donde la convergencia criminal actúa, se organiza en medio de jerarquías y relaciones de interdependencia con actores u organismos de diferentes tamaños e importancia que afectan directa o indirectamente las ganancias de los grupos delictivos, y en sí mismo la estabilidad de la alianza a la hora de realizar actividades al margen de la ley concretadas con anticipación. Generando en estos ecosistemas criminales o convergencia criminal un alto grado de amenaza y peligrosidad para la seguridad y defensa nacional, tras albergar Crimen organizado trasnacional (COT), terrorismo, narcotráfico e insurgencia en una especie de red operativa y enlaces comunicacionales capaces de aumentar la fuerza de trabajo y poder al interconectar a diversos criminales en puntos estratégicos del territorio en los cuales decidirán qué operación realizar, dónde, cuándo y a quién se desarrollará el ilícito con los menores riesgos posibles (Ospina, Riveros & Barrera, 2018).

Dicha red de convergencia criminal tiene 6 características principales, pero en el caso de su interacción con ciberseguridad solo se destacarán cuatro. La primera característica se encarga de laborar por medio de centros de actividad o red de nodos dispersos e interconectados; la segunda característica, los centros de actividad serán liderados por cada uno de los factores armados de inestabilidad, pueden ser grandes o pequeños, estrecha o ligeramente integrados, inclusivos y exclusivos en membresía, es decir, la interacción de cada grupo es en espacios diferentes; la tercera característica, se halla en la toma de decisiones y operaciones las cuales se llevaran a cabo a través de consensos para descentralizar la iniciativa y la autonomía del crimen, es decir, cada grupo se hará cargo de una actividad específica para el éxito del delito; y la cuarta característica, permite con la ayuda de la Internet y del mismo territorio donde se refugian, definir el crimen y el alcance del mismo, hacia quien va dirigido y con qué fin, para así terminar de desarrollar la estrategia y conseguir el resultado material o económico decidido, sin necesidad de salir de su territorio y poner en riesgo su anonimato frente a la Fuerza Pública, de alguna manera se vuelven invisibles en el terreno conocido (Álvarez & Rodríguez, 2018).

Estas acciones criminales pueden asociarse a la red tipo malla, especialista en colaboración en todos los nodos o centros de información para interconectarse entre sí, es decir, la red tipo malla es capaz de involucrarse en cualquier acto criminal tras conocer la información correspondiente al delito en el cual van a incurrir los diferentes grupos

delictivos, hechos que en el ciberespacio pueden generar tantas fuentes de ataques que no se detecta con facilidad el origen del mismo, tampoco, se puede definir cuál fue el grupo que lo causo al borrar los puntos de entrada y salida en el ciberespacio. Generando una capacidad de acción criminal en un mismo espacio, donde las Fuerzas Militares y la Policía Nacional deben ejecutar acciones de respuesta necesarias para hallar el punto donde se originó el delito y así seguir el rastro del cibercriminal. Innovando por medio de estrategias y operaciones para neutralizar el ciberdelito y por ende al cibercriminal (TOCA, 2018). El ciberespacio se vuelve una realidad líquida de fronteras donde ellas desaparecen, permitiendo la acción de innumerables delitos amparados por la omnipresencia y anonimato generados por el mismo escenario, y donde la regulación nacional o internacional aún no encuentra el efecto, el medio, la herramienta o la operación consistente y eficiente para actuar contra el delito y los criminales dentro de la red de redes del mundo (Zúñiga, 2016).

Bajo esta perspectiva, los delincuentes que trabajan en red, como el tipo malla, les permiten ejercer a los cibercriminales delitos como la pornografía infantil y el blanqueo de las ganancias ilícitas, pues un simple movimiento de capitales vía web permite limpiar o hacer lícito el dinero con un par de clics, estableciendo los delitos más populares bajo esta perspectiva criminal en el ciberespacio, como lo son el blanqueo de capitales y el fraude tributario, en los cuales se unen las diferentes formas de criminalidad trasnacional (Zúñiga, 2016). En consecuencia, el lavado de activos se volvió uno de los delitos más realizados a nivel trasnacional vía web, ejecutadas por las llamadas ***empresas de servicios,*** las cuales les permiten a los narcos, funcionarios corruptos y traficantes ilegales de armas concentrarse en lo que saben hacer y contratar o delegar el proceso de blanquear su dinero con una persona o ***empresa*** que conozca muy bien el proceso delictivo, con ayuda de un par de transferencias en línea. Efectos que también se han visto reflejadas en las apuestas en línea como alternativa preferida por el Crimen Organizado Trasnacional (COT) (Uzal et al., 2015).

Con la ayuda de estos ciberdelitos, también se pueden detectar ciber agresiones presentadas en el marco de la ciberseguridad como el ciberterrorismo, la ciberguerra, cibercrimen organizado trasnacional, ciberespionaje, delitos y crímenes vía internet que les permite a los cibercriminales vulnerar la administración gubernamental de los Estados nación, la gestión de defensa, la gestión de economía, de salud, de agua potable, en distribución de alimentos, comunicaciones, transporte, educación, negocios, cultura y muchos más que forman parte de la infraestructura crítica del país, en donde las modalidades delictivas más graves, encuentran el escenario perfecto en el ciberespacio para aparecer, expandirse y perfeccionarse, donde la ley aun no aparece y las ventanas son diversas para operar, eventos que le han permitido al Lavado Trasnacional de Activos su influencia en el ciberespacio. Eventualidades donde Policía, Ejército, Fuerza Aérea y

Armada Nacional deben encontrar el método, la forma, el medio y la operación concreta para minimizar los impactos de estos delitos que afectan al Estado colombiano como a otras naciones por medio de la cooperación militar y policial (Uzal et al., 2015).

Al encontrar nuevos espacios convergentes para generar delitos que interfieren en varios lugares al mismo tiempo, en mayor proporción en la población civil, con el fin de incrementar ganancias a los ciberdelincuentes, se debe visualizar los aspectos en los cuales la Fuerza Pública debe trabajar para disminuir el crecimiento de los cibercrímenes en la proporción en que se vienen ejecutando, enfocando la presión en las operaciones y acciones de respuestas sobre las Fuerzas Militares y la Policía Nacional, buscando los puntos de origen de los delitos caracterizados por la convergencia criminal en el ciberespacio. Bajo esta perspectiva, proteger los puntos ciegos generados por el escenario virtual, con la ayuda de estrategias de cooperación con otros Estados en este mismo campo y contrarrestar el cibercrimen por medio de propuestas que apoyen el crecimiento en la ciberseguridad y ciberdefensa en Colombia (Moreno, 2017).

Bajo esta perspectiva, toda política y organización puede ser mejorada para ir ajustando puntos esenciales en la lucha contra los ciberdelitos y el cibercrimen, por medio de operaciones especializadas de acuerdo al tipo de ataque presente o latente en el ciberespacio, es decir, opciones de respuesta eficaces en contra de los delitos cibernéticos, monitoreando ataques comunes para establecer protocolos efectivos, análisis y neutralización de los factores armados de inestabilidad enfocados hacia quienes van dirigidos y cuál es el patrón de ataque, y en consecuencia responder con operaciones, tácticas y armas necesarias capaces de evitar el ataque, rastreó del punto de origen y protección hacia otras infraestructuras vulnerables tanto públicas como privadas, con nuevas herramientas y estrategias en el ciberespacio (La República, 2019).

Es decir, incentivar el desarrollo en i + D + I junto a los vínculos internacionales para capacitar al personal encargado de la ciberseguridad y ciberdefensa a nivel nacional en la Policía Nacional, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana, por medio de centros especializados como el COLCERT, el Comando Conjunto Cibernético, el Centro Cibernético Policial, las Unidades Mayores y Menores en Ciberseguridad y Ciberdefensa y finalmente la especificación de quién combate a quién, en este amplio escenario de guerra cibernética. Por lo tanto, ¿cómo se puede desarrollar cada uno de estos elementos? Teniendo en cuenta los aspectos relevantes referentes a líneas de acción y regulación interna en cada continente, cuyo objetivo promueve la minimización de los factores armados de inestabilidad en el ciberespacio, sin olvidar, que los ciberdelincuentes en cada país son diferentes, con intereses distintos y objetivos diversos, evaluando y haciendo seguimiento a posibles amenazas externas (Castañeda, 2019) desarrollando una propuesta capaz de apoyar la eficacia del cuidado cibernético nacional.

De acuerdo a la Directiva del Parlamento Europeo y del Consejo de la Unión Europea, organismo que garantiza un alto nivel de seguridad en redes y sistemas de información en la protección de la navegación de los usuarios, se tomó como punto de partida para proyectar propuestas acerca del mejoramiento en el sistema de ciberseguridad en Colombia y enfrentar las amenazas latentes, por medio de: El "establecimiento de requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales" (Castañeda, 2019, p.42). Además, "determinar las obligaciones para todos los Estados de adoptar una estrategia nacional de seguridad de las redes y sistemas de información" (Castañeda, 2019, p.42). El primero de ellos hace referencia a exigir e implementar en las empresas de servicios esenciales o servicios públicos, herramientas para la protección de sus sistemas de navegación e internet, así como de comunicación y abastecimiento, y el segundo enfocado en la implementación y desarrollo de una política de ciberseguridad y ciberdefensa en cada Estado, aspecto que Colombia ya tiene en vigencia con su política de seguridad digital (Parlamento Europeo, Consejo de la Unión Europea, Directiva 1148, 2016).

En ese mismo camino, la Ley nacional de seguridad cibernética ejecutada por el parlamento chino desde el 2017, se tomó como ejemplo el trabajo conjunto entre las entidades públicas con las privadas, para efectos de cooperación entre empresas privadas e instituciones representantes del Estado y así establecer comunicación y alertas tempranas sobre amenazas en la red que puedan afectar el funcionamiento continuo de sus empresas, con lo cual, las instituciones de seguridad encargadas deben estar listas y actuar frente a estos anuncios, hechos que en Colombia están presentes en la ley de seguridad digital, pero que deben reforzarse en tiempos donde los ataques son frecuentes y necesitan respuesta inmediata en ambos sectores con una buena comunicación entre entidades del Estado y las empresas de servicios públicos tanto privadas como públicas por ejemplo (Instituto Español de Estudios Estratégicos IEEE, 2017).

Así mismo, las políticas y programas de Seguridad Cibernética, publicadas por la Organización de Estados Americanos (OEA), a través del Comité Interamericano contra el Terrorismo (CICTE), promueve el fortalecimiento y la capacidad técnica sobre seguridad cibernética donde las políticas destinadas al uso seguro del ciberespacio, fortalecen los procesos de capacitación técnica del personal vinculados a cada una de las entidades encargadas de seguridad y defensa del ciberespacio, además, apoya la creación de nuevos protocolos para la neutralización del riesgo, conocido también como gestión del riesgo en las empresas pero esta vez en el uso y aplicación del ciberespacio, características que pueden impulsar la capacitación constante en este escenario en cada una de las instituciones encargadas de la ciberseguridad, así como de las empresas que quieren y puedan proteger a sus colaboradores de los riesgos cibernéticos, apuntados también como medios para encontrar patrones en los ataques ejercidos desde cualquier

escenario y así encontrar mejores respuestas frente a estas amenazas (Organización de Estados Americanos, 2020).

Con la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas (ONU), se puede poner en funcionamiento la Estrategia para la Cooperación y la Colaboración, tomando como puntos de referencia tres medidas importantes para ejecutar nuevas tácticas operacionales en la estrategia de ciberseguridad y ciberdefensa en Colombia y enfrentar a los factores armados de inestabilidad: 1. Medidas técnicas referidas a capacitación y procedimentales referidas a formas de operaciones; 2. Medidas técnicas y procedimentales enfocadas a mejorar las habilidades de los encargados de investigar y neutralizar las amenazas en el ciberespacio y nuevos procedimientos diseñados por el ingenio colombiano, establecidos desde la misma Fuerza Pública; 3. Desarrollo de capacidades determinadas con el apoyo i + D + I esencial para el crecimiento y efectividad de operaciones cibernéticas, tan eficaces como aquellas desarrolladas en países pioneros en tecnología, rectificadas por el Índice de Ciberseguridad Global (Castañeda, 2019, pp.45-46).

Es decir, por medio de la innovación y la medición en los programas a desplegar para la ciberseguridad y ciberdefensa, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) enfocado en la construcción colectiva sobre la adopción de Gestión de Riesgos se caracteriza por tres puntos esenciales a tener en cuenta para su aplicación en el país: 1. "Medidas de seguridad apropiadas y acordes con el riesgo y la actividad económica y social en juego" (Castañeda, 2019, p.45), orientadas a la creación de nuevas operaciones para neutralizar y eliminar el riesgo del delito para que no se pueda efectuar en el momento preciso hacia la entidad, empresa o persona elegida como víctima; 2. Derechos humanos y valores fundamentales, como en toda actividad dirigida por la Fuerza Pública, debe esclarecerse el alcance, manejo y reglamentación en cada tarea, función y operación a realizar para seguir protegiendo la vida privada de cada persona en el país; 3. Evaluación del riesgo y ciclo de tratamiento, mostrando los efectos negativos y positivos de la puesta en marcha de las operaciones y tareas de los encargados de la seguridad y defensa hacia las personas afectadas, evaluando las acciones y estableciendo estrategias al inicio y al final de cada operación para minimizar los efectos negativos en la siguiente operación cibernética (Organización para la Cooperación y el Desarrollo Económico, 2016).

Otro aspecto a tener en cuenta es el Modelo de Madurez de Capacidad de Seguridad Cibernética de Oxford desde el 2016, vislumbra dos elementos importantes dentro de la seguridad cibernética como lo son la educación y habilidades enfocadas en el factor humano establecidas como fuentes de efectividad en la ejecución de las operaciones en el ciberespacio, así como el incremento de políticas públicas enfocadas en la concientización de la protección en red por parte de toda la comunidad en el territorio nacional,

buscando la reducción de los delitos hacia los civiles, blancos comunes de estos crímenes (Organización de Estados Americanos OEA, 2016).

Por último, las líneas base para mejorar la capacidad de acción y efectividad correspondiente a la ciberseguridad y ciberdefensa en Colombia culmina, con el Índice Nacional de Seguridad Cibernética establecida por la Academia de Gobierno Electrónico en Estonia, teniendo en cuenta lo siguiente: 1. Capacidad para analizar las ciberamenazas a nivel nacional, debido a que cada una actúa de manera distinta, con patrones e intereses distintos y se debe responder de acuerdo a la misma estructura del ciberataque; 2. Capacidad para gestionar una crisis cibernética a gran escala, mostrando la capacidad operativa para enfrentar en dado caso este tipo de eventualidades en Colombia; 3. Capacidad para llevar a cabo operaciones militares de defensa cibernética bajo protocolos y estructuras dadas por las Fuerzas Militares innatas de la institución al identificar los movimientos, intereses y objetivos de los ciberdelincuentes enfocados en su jurisdicción (OEA, 2016).

Cada una de ellas establece un punto contundente para mejorar y fortalecer las actividades realizadas por la Fuerza Pública colombiana, resaltando aspectos en los cuales enfocar su atención para seguir siendo pionero en ciberseguridad y ciberdefensa en la región, implementando aspectos como la gestión y evaluación del riesgo, innovación y desarrollo en las operaciones cibernéticas nacionales, la capacidad de respuesta frente a eventos masivos que puedan poner en jaque la ciberseguridad y ciberdefensa nacional; al tiempo que fortalece el análisis y seguimiento de las operaciones del enemigo por la institución correspondiente, clasificando el riesgo de las amenazas y las acciones inéditas (si es posible) para desmantelar al enemigo; volver constante la capacitación del personal en diferentes aspectos, e incrementar las políticas públicas enfocadas en acción y prevención de los ataques cibernéticos en entidades privadas, públicas y sociedad civil, actores para quienes se ha aplicado la política de seguridad digital en Colombia (Castañeda, 2019).

Recapitulando, los factores armados de inestabilidad pueden actuar bajo el fenómeno de convergencia criminal para ejercer alianzas momentáneas entre grupos delincuenciales organizados, narcotráfico o crimen trasnacional para afectar la seguridad en la red bajo un objetivo común, ganar dinero a costa de los datos personales y esenciales de la sociedad como de las entidades públicas y empresas privadas de la nación, en medio de territorios geoestratégicos que les permiten delinquir sin el menor riesgo posible, pues la ley recae en ellos mismos, esos lugares donde la Fuerza Pública no puede actuar, pero si puede monitorear para hacer caer a los ciberdelincuentes de una manera astuta, nueva y eficaz para impedir el delito correspondiente, así como garantizar la navegación en la red de manera segura. Recordando que la convergencia criminal se vuelve una amenaza latente para el ciberespacio cuando esta no tiene jurisdicción y los cibercriminales la

ejecutan desde lugares donde la ley nacional no existe y para los cuales hay que encontrar la solución respectiva y reducir el riesgo (Toca, 2018).

Ese riesgo se puede superar por medio de nuevas estrategias desarrolladas en Colombia teniendo en cuenta algunos ejemplos de éxito establecidos en organismos y naciones del mundo, en las cuales adoptan la innovación de operaciones, capacitación de personal, seguimiento y evaluación del riesgo de ciberdelitos, de igual forma es esencial el fortalecimiento de los mecanismos de cooperación entre entidades públicas y privadas así como las relaciones internacionales, enfocadas en cerrar los canales de acceso de los ciberdelincuentes para cometer sus crímenes, efectuando un control efectivo del tráfico de red, de los puertos de salida y rastreo de los centros de operación criminal que vulneran la seguridad de la sociedad colombiana.

El trabajo ha sido arduo, pero no se puede bajar la guardia y requiere de un proceso constante de adaptación, desarrollo y fortalecimiento de las instituciones, mecanismos y métodos empleados en la protección, seguridad y defensa cibernética del País.

Conclusiones

En el marco del primer objetivo, la ciberseguridad muestra su historia, evolución y legislación creciente con el paso de los años al incrementar las acciones ilegales o delitos ejercidos desde la web, algunos de ellos iniciaron como bromas o incidentes menores, pero su evolución determinó la importancia, severidad y consecuencias extremas que la manipulación de la internet podía causar en la vida de una persona en cualquier parte del mundo. Pues se ha dejado en evidencia como desde un simple virus en una computadora tuvo tanto impacto en los delincuentes que mejoraron el acceso ilegal a datos personales para su beneficio por medio de hackers, APT's y el hacking para lucrarse sin el más mínimo esfuerzo. Acciones que impulsaron el desarrollo de soluciones en el ciberespacio y navegar de manera segura como los antivirus, las IPS, el firewall, sandboxing, antibot y soluciones avanzadas en tiempo real para minimizar el impacto de los cibercrímenes hacia sus víctimas.

Cada una de las herramientas usadas por los ciberdelincuentes para cometer los crímenes correspondientes establecieron el crecimiento de normas internacionales y nacionales para mitigar el impacto de las violaciones a la seguridad vía web, conocidas actualmente como medidas para la ciberseguridad y ciberdefensa de las naciones, nacidas bajo la mirada internacional del Convenio de Budapest ratificado en 2001, donde se permite la creación de normas internas en cada uno de los Estados para enfrentar los cibercrímenes y ciberdelitos que en muchos casos afecta con mayor frecuencia a los ciudadanos comunes, ley que permitió en Colombia la creación de varios CONPES como el 3854 de 2016, donde se impulsa la política Nacional de Seguridad Digital, en la cual se

unifica, se mejora y especifica las acciones establecidas para ciberseguridad y ciberdefensa en Colombia, al percibir el auge de factores armados de inestabilidad en el ciberespacio causante de una reacción Estatal para crear instituciones encargadas y enfocadas a investigar, clasificar, neutralizar y minimizar las acciones de los ciberdelincuentes en el espacio colombiano.

Bajo estos hechos, el segundo objetivo se encarga de determinar cada una de las entidades desarrolladas para enfrentar las amenazas en el aspecto de ciberseguridad y ciberdefensa al mando de las Fuerzas Militares y de la Policía Nacional, distribuyendo tareas, objetivos, operaciones, ejerciendo cooperación cuando es necesario en las decisiones y operaciones correspondientes, por medio de Entidades como el COLCERT, el CCOCI, la CCP el CAI Virtual entre las más destacadas en el proceso de seguimiento y control de la navegación en el territorio nacional, avaladas desde el CONPES 3701 de 2011 quien aporto con liderazgo en términos de ciberseguridad y ciberdefensa así como la implementación de la institucionalidad encargada de perseguir y eliminar prácticas ilegales en el ciberespacio, protegiendo la infraestructura crítica del Estado y la seguridad de los ciudadanos.

Al clasificar responsabilidades, factores armados a investigar y la división de operaciones que luego se concentraran en una sola institución para analizar y establecer estadísticas para la toma de decisiones presentes y futuras en el marco de la seguridad digital, las normas vigentes como las instituciones encargadas de la ciberseguridad y ciberdefensa muestran los aspectos puntuales a mejorar para consolidar la protección de los ciudadanos, instituciones representantes del Estado y las empresas privadas durante su estadía, navegación, transacción y envío de información por la web, evitando que los ciberdelincuentes encuentren espacios para suplir sus intereses, acciones que ha desarrollado muy bien la Fuerza Pública, pero que debe mejorar para ser más efectivo y práctico a la hora de encontrar el origen del ciberataque y hallar una solución para evitar su reincidencia.

Respecto al tercer objetivo, la Fuerza Pública se dio cuenta de que los factores armados de inestabilidad como las GAO, las GDO, el narcotráfico, el crimen organizado trasnacional, con modalidades distintas pero con objetivos comunes pueden reunir en sitios estratégicos y desarrollar alianzas para alcanzar objetivos comunes temporales, a través del ejercicio conocido como Convergencia Criminal, en donde se reúne diferentes factores armados para cometer delitos, entre ellos ciberdelitos, ciberataques, por ejemplo, que ponen en riesgo la estabilidad económica de la nación en medio de espacios baldíos donde la jurisdicción estatal no tiene cabida y donde se permite el control en la ilegalidad, escenarios y actores que ejercen alarma por su creciente participación en el desarrollo de delitos como el lavado de activos en el ciberespacio, o el incremento de pornografía infantil o trata de personas y demás crímenes desarrollados con mayor facilidad en medio de este escenario que no tiene jurisdicción.

Para evitar el crecimiento de las acciones criminales en el ciberespacio en manos de GAO, GDO, narcotráfico o crimen organizado trasnacional, se desarrollaron varias propuestas que robustecen el actuar de la política nacional de seguridad digital vigente en la nación colombiana, por medio de gestión del riesgo en el ciberespacio, la creación de políticas públicas para concientizar a las personas sobre estos escenarios y los tipos de delitos que se pueden generar, el impulso de cooperación entre instituciones colombianas como de otros países que quieran incursionar en la protección del ciberespacio en sus naciones como en las regiones fronterizas, donde estos crímenes pueden desarrollarse con mayor facilidad, así como el fortalecimiento de las instituciones, operaciones y capacitaciones que al día de hoy han generado grandes resultados, a las cuales solo les falta una inyección de innovación para fomentar propios procesos de investigación, de rastreo, neutralización y mitigación de ciberdelitos provenientes de estos grupos o de cualquier otro actor amenazante a la seguridad nacional colombiana.

Declaración de divulgación

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

Autor

Martin Fernando Rincón Gallón . Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Oficial Fuerza Aérea, Administrador Aeronáutico, Escuela Militar de Aviación, Colombia.

ORCID: https://orcid.org/0009-0007-1725-6888

Contacto: rinconm@esdeg.edu.co

Referencias

Álvarez, C. E. & Rodríguez, C. A. (2018). Ecosistemas criminales: hábitats para la convergencia y la globalización desviada. *Revista Científica General José María Córdova.* 16 (24) 1-30. DOI: http://dx.doi.org/10.21830/19006586.352

Becerra, J, A et al. (2019). La seguridad en el ciberespacio, un desafío para Colombia. Maestría en Ciberseguridad y Ciberdefensa. Sello Editorial ESDEG.

CAI Virtual (2021). Balance Cibercrimen 2020. Centro Cibernético Policial. *Policía Nacional de Colombia.*

Camacho, J.D. (2016). *Evolución de la Ciberdefensa y la seguridad de la información en Colombia.* Especialización de la Administración de la Seguridad. Universidad Militar Nueva Granada.

Castañeda, C. (2019). *La ciberseguridad, gestión del riesgo y la resiliencia, perspectiva de la evolución de la política pública colombiana. La seguridad en el ciberespacio, un desafío para Colombia.* Maestría en Ciberseguridad y ciberdefensa. Repositorio Escuela Superior de Guerra.

Centro de Estudios de Política y Relaciones Internacionales. (2016). *Reseña: sobre la ciberseguridad y la ciberguerra. Centro de Estudios de Política y Relaciones Internacionales.* Oxford University Press. Nueva York. Estados Unidos. https://cepri.upb.edu.co/index.php/transicion-militar-y-policial-en-colombia/ciberseguridad-ciberguerra

Comando General de las Fuerzas Militares. (2016). *Directiva Permanente 010 de 2016 del COGFM*. Emite las órdenes para el fortalecimiento de la ciberdefensa y ciberseguridad para las Fuerzas Militares, con el propósito de unificar criterios, emitir ordenes e instrucciones, establecer u difundir políticas, definir lineamientos y directrices, y fijar criterios operacionales que permitan el empleo adecuado del poder militar en el ciberespacio con temas relacionados con ciberseguridad y ciberdefensa. Comando General de las Fuerzas Militares.

Comunidad de Policías de América. (2013). Análisis Situacional del narcotráfico "una perspectiva policial". pp.51-74, 127-128. Comunidad de Policías de América.

Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia. Council of Europe*. Serie de Tratados Europeos. No. 185. Budapest. 23.XI.2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cubillos Ramos, J, A. (2017). *Gestión de riesgos para seguridad digital en Colombia*. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00004751.pdf

Cujabante Villamil, X. A. Bahamón Jara, M. L. Prieto Venegas, J. C. & Quiroga Aguilar, 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. http://dx.doi.org/10.21830/19006586.588

Derechos Digitales. (2018). Una breve historia de la ciberseguridad importada. *Derechos Humanos y tecnología en América Latina*. https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/

Ferrando Guillem, A, L. (2018). La ciberseguridad como reto internacional: la protección frente a las ciberamenazas. *Universitat Oberta de Catalunya* [Trabajo de Grado]. Master Interuniversitario de Seguridad en las Tecnologías de la Información y las Comunicaciones.

Hernández Sampieri, R. (2014). *Metodología de la investigación*. Sexta edición. McGraw Hill. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Hernández, Bernal. J.F. (s.f). *Ciberseguridad y ciberdefensa en la Fuerza Aérea Colombiana en el marco de la planeación por capacidades*. Fuerza Aérea Colombiana. Fuerzas Militares de Colombia.

Instituto Español de Estudios Estratégicos IEEE. (2017). Ciberseguridad en China. David Ramírez Morán. Documento Informativo. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=http%3A%2F%2Fwww.ieee.es%2FGalerias%2Ffichero%2Fdocs_informativos%2F2017%2FDIEEEI01-2017_CyberChina_DRM.pdf&clen=579294&chunk=true

Junta Interamericana de Defensa. (2020). *Guía de Ciberdefensa, orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* Néstor Ganuza. Canadá.

La República. (2019). *Colombia fue uno de los países con más ataques cibernéticos el año pasado.* https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

La República. (2020). *Ciberseguridad*. https://imgcdn.larepublica.co/cms/2020/05/20104429/100519-CIBERSEGURIDAD-La-Republica.pdf

Ley 1908 de 2018. [Const]. Por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87301

Ley 1928 de 2018 [Const]. Por medio de la cual se aprueba el "convenio sobre la ciberdelincuencia", adoptado el 23 de noviembre de 2001 en Budapest. Secretaria del Senado http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

López, R. (1998). Crítica de la teoría de la información. ***Cinta de Moebio***, 3, pp.2-3. Universidad de Chile.

Machín, N. & Gazapo, M. (2016). *La ciberseguridad como factor crítico en la seguridad de la Unión Europea. Revista UNISCI,* 42, pp. 47-68. http://dx.doi.org/10.5209/RUNI.53786

Medina Páez, O, J. (2016). *Análisis de la Directiva Ministerial Permanente 015 de 2016*. Especialización en Derechos Humanos y Defensa ante Sistemas Internacionales de Protección. Facultad de Derechos. Universidad Militar Nueva Granada.

Ministerio de Defensa Nacional. (2009b). *Ciberseguridad y Ciberdefensa Una primera aproximación.* Ministerio de Defensa Nacional.

Ministerio de Defensa Nacional. (2012). *Resolución 7436 de 2012.* como ente rector para el direccionamiento, planeación, coordinación, integración, ejecución y sincronización de operaciones cibernéticas conjuntas. Ministerio de Defensa Nacional.

Ministerio de Defensa Nacional. (2019). *Memorias al Congreso 2018-2019*. Guillermo Botero Nieto. Ministro de Defensa Nacional.

Ministerio de Tecnología, Información y Comunicaciones MINTIC. (2012). *Documento de Plan de Acción nodo de innovación en ciberseguridad.* Vive Digital. Derechos Reservados.

Moreno Peláez, J, E. (2017). *El fenómeno de la convergencia en la seguridad y defensa nacional.* https://sistemas.uniandes.edu.co/images/forosisis/foros/fsi2017/el_fenomeno_de_la_convergencIa_en_la_seguridad_y_defensa_nacionales.pdf

Organización de Estados Americanos OEA y Banco Interamericano de Desarrollo BID. (2016). *Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe? Informe de seguridad 2016.* https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Organización de Estados Americanos OEA y Banco Interamericano de Desarrollo BID. (2020). *Colombia. Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad.* https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Organización de Estados Americanos. (2021). *Programa de Ciberseguridad.* http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Organización de las Naciones Unidas. (2021). *Tráfico de drogas. La ONU y el Estado de Derecho.* Organización de las Naciones Unidas.

Organización para la Cooperación y el Desarrollo Económico. (2016). *Gestión de riesgos de seguridad digital. Capítulo 14. Un manual para la economía digital.* Organización de las Naciones Unidas.

Ospina Díaz, M, R. & Sanabria Rangel, P, E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad,* 62, (2). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&nrm=iso&tlng=es

Ospina Rubiano, J, D., Riveros Cruz, A. & Barrera Herrera, F. (2018). *Capitulo IX Convergencia de la Seguridad en Colombia: Terrorismo y Delincuencia Organizada*. Sello Editorial ESDEG.

Parlamento Europeo, Consejo de la Unión Europea. (2016, 07,19). *Directiva 1148 2016. Diario Oficial de la Unión Europea*. Parlamento Europeo.

Piper, D. (1997). Authentic teaching and learning in cyberspace: a Heideggerian perspective. *Westminster Studies in Education, 20* (1), 75-87.

Policía Nacional de Colombia (2020). *Ciberseguridad.* Ministerio de Defensa de Colombia. https://www.policia.gov.co/ciberseguridad

Policía Nacional de Colombia (2021). *Centro cibernético de la Policía.* CAI Virtual. https://caivirtual.policia.gov.co/

Policía Nacional de Colombia. (2010). *Resolución 319 de 2010,* Rol de la policía nacional de Colombia frente a la ciberseguridad y ciberdefensa del país en el ciberespacio. Policía Nacional de Colombia.

Realpe, M., & Cano, J. (2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia*. X Congreso Iberoamericano.

Segura Serrano, A. (2017). Ciberseguridad y Derecho Internacional. University of Granada. *Revista Española de Derecho Internacional*, 69 (2), 291-299. Julio-diciembre. Madrid. http://dx.doi.org/10.17103/redi.69.2.2017.2.02

Toca, A. (2018). Terrorismo Global y Crimen Organizado en Colombia: el fenómeno mutante. *Revista Nova ET Vetera,* 4 (39). https://www.urosario.edu.co/Revista-Nova-Et-Vetera/Omnia/Terrorismo-Global-y-Crimen-Organizado-en-Colom/

United Nation Office on Drugs and Crime. (2021). Crimen Organizado Trasnacional. United Nation Office on Drugs and Crime. https://www.unodc.org/ropan/es/organized-crime.html

United Nation Office on Drugs and Crime. (2021). *Delincuencia organizada trasnacional: la economía ilegal mundializada*. United Nation Office on Drugs and Crime. https://www.unodc.org/toc/es/crimes/organized-crime.html

Uzal, R. Riesco, D. Montejano, G. Agüero, W & Baieli, C. (2015). *Lavado Trasnacional de Activos en el Ciberespacio. Presentación del contexto, planteo del problema y formulación de propuestas. Simposio de Informática en el Estado.* Universidad Nacional de San Luis.

Vera Piñeros, D. Prieto, P. & Garzón, D. (2020). *La ciberseguridad, la ciberdefensa, la identidad y los intereses nacionales y las Fuerzas Militares de Colombia. Identidad e intereses nacionales de Colombia.* Fundación Konrad Adenauer Stiftung KAS.

Zúñiga Rodríguez, L. (2016). El concepto de criminalidad organizada trasnacional: problemas y propuestas. *Revista Nuevo Foro Penal,* 12, (86). Universidad EAFIT. Medellín. Colombia. ISSN: 0120-8179.

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.

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 67-90)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Importancia de una Ley de Ciberseguridad y Ciberdefensa para Colombia

Importance of a Cybersecurity and Cyberdefense Law for Colombia

DOI: https://doi.org/10.25062/2955-0270.4766

Julián Antonio Guzmán Pacheco
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

El artículo busca reflejar la importancia de la aprobación de una Ley de Ciberseguridad y Ciberdefensa para Colombia a través de un análisis reflexivo, teniendo en cuenta sus características y perspectivas tanto nacionales como internacionales. Este se realizó a partir de una metodología cualitativa, donde a través de la revisión de la literatura existente se logró comprender el fenómeno de investigación. De esta manera, se lograron descubrir los elementos constitutivos que requieren una ley de ciberseguridad y ciberdefensa desde su relevancia y aporte para la inteligencia nacional. Por último, se lograron identificar las dificultades legales con las cuales opera actualmente la Ciberseguridad y Ciberdefensa en Colombia, desde su inadecuada interpretación y ajuste de las leyes existentes, precisamente como factor clave y estratégico del desarrollo que coincide con la aparición del fenómeno web, cuya expansión ha generado la quinta dimensión de las guerras modernas, afectando la cotidianidad de los diferentes actores.

Palabras Clave: Ciberdefensa; Ciberseguridad; Derecho; Leyes; Política Pública

Abstract

The article seeks to reflect the importance of the approval of a Cybersecurity and Cyberdefense Law for Colombia through a reflective analysis, taking into account its characteristics and both national and international perspectives. This was carried out based on a qualitative methodology, where through the review of existing literature it was possible to understand the research phenomenon. In this way, it was possible to discover the constituent elements that require a cybersecurity and cyber defense law from its relevance and contribution to national intelligence. Finally, it was possible to identify the legal difficulties with which Cybersecurity and Cyberdefense currently operates in Colombia, from its inadequate interpretation and adjustment of existing laws, precisely as a key and strategic factor of development that coincides with the appearance of the web phenomenon, whose expansion has generated the fifth dimension of modern wars, affecting the daily lives of different actors.

Key words: Cyber defense; Cybersecurity; Rights; Laws; Public politics

Artículo de reflexión
Recibido: 2 de febrero de 2022 • **Aceptado:** 14 de mayo de 2022
Contacto: Julián Antonio Guzmán Pacheco guzmanja@esdeg.edu.co

Introducción

Aunque resulta difícil realizar un análisis preciso sobre la Ciberseguridad y la Ciberdefensa, lo que es claro, es que las amenazas, según Fernández (2019) no deben subestimarse. En este sentido, a pesar de que la ciberseguridad y ciberdefensa no se visibilizan fácilmente, guardan una estrecha relación, tanto a través del resguardo de la información almacenada o interconectada para la prevención de las amenazas, como de la planificación y las capacidades del Estado para defender los activos estratégicos e intereses nacionales. Precisamente, el avance tecnológico es lo que ha provocado el interés de salvaguardar la información, exigiendo procesos robustos para contrarrestar y controlar las amenazas cibernéticas, tal como lo hace la ciberdefensa, previniendo los ataques de grupos con interés contrarios al estado, y la ciberseguridad, brindando respuestas para resguardar la información que podría colocar en riesgo la infraestructura crítica del estado.

la ciberseguridad termina siendo el complemento a la ciberdefensa y se materializa, según Hannant (2021) en la defensa digital o de la información del Estado que se puede evidenciar mediante las acciones encaminadas para mitigar el Cibercrimen independientemente el grado de incertidumbre tanto interna como externa, cabe mencionar que la complejidad de dichos elementos dificulta encontrar una solución a las problemáticas relacionadas con estos (Hannant, 2021). Así, estos dos elementos se han convertido en un factor fundamental para el fortalecimiento de acciones que previenen ataques contra la institucionalidad o la seguridad de los gobiernos, como los eventos del 11 de septiembre de 2001 en el World Trade Center de Nueva York, o en el caso de Colombia, a partir de las interceptaciones ilegales del Departamento Administrativo de Seguridad (DAS); provocando la eliminación del mencionado organismo.

Las anteriores situaciones evidencian las dificultades para mitigar el riesgo interno, externo y falencias en el tema de la ciberseguridad y ciberdefensa, puesto que se refleja la incapacidad de los países para evaluar la función y desempeño de estas áreas, sin contar las carencias normativas y aplicables en estos escenarios que muestran la insuficiencia del Estado en cuanto a la prevención y mitigación con las herramientas de seguridad y defensa nacional (Lind,2017). Estas circunstancias, aunque preocupan, no sorprenden, debido a que la ciberseguridad carece de mecanismos tecnológicos y personal entrenado para prevenir y la ciberdefensa presenta un enfoque pasivo sin alternativas de defensa que contrarresten el cibercrimen. Todo esto, apunta a la debilidad del Estado colombiano, que no solo demuestra debilidades evidenciadas en la parte técnica o tecnológica, sino también desde la insuficiencia legal para llevar a cabo la prevención, rastreo y procesamiento de los mecanismos necesarios que ayuden a lograr un adecuado andamiaje entre ciberseguridad y la ciberdefensa, como variables que favorezcan al Estado a través del respeto por la ley desde un nuevo escenario que soporta la justicia y su accionar nacional (Guaqueta, 2015).

Este escenario surge por el creciente uso del ciberespacio en el mundo, en donde la globalización ha propiciado la revolución tecnológica del siglo XXI. Un ejemplo de esto se evidencia en el aumento de personas que actualmente usan sistemas conectados al ciberespacio, originando por ejemplo el internet de las cosas. Igualmente, la cantidad de datos que se originan virtualmente ha generado el *big data*, donde a través de un inmenso volumen de información se logra el análisis de patrones y tendencias de comportamiento como un activo de suma importancia para cualquier persona, organización o Estado (La Gaceta Caese, 2016).

Precisamente todo esto ha llevado a convertir la Ciberdefensa y Ciberseguridad en un aspecto fundamental a nivel estratégico, sobre todo por el enorme manejo de la información por la población en general a través de redes, medios, portales webs y su expansión concebida como la nueva dimensión de las guerras modernas. Este hecho convierte este fenómeno en un factor clave de análisis para la conducción político y estratégica en pro de los intereses de las naciones. En Colombia, estos factores ampliamente discutidos se vienen focalizando en análisis pragmáticos, que llevan a la seguridad y la defensa en el ciberespacio a ser pensada desde un modelo local de gobernanza en ciberdefensa a partir de la normativa actual, donde los hallazgos actuales requieren esfuerzos inter agénciales para su institucionalización (Rojas, 2021). En este contexto, se demuestra como el Estado colombiano carece de regulación satisfactoria en aspectos del ciberespacio, que a pesar de la utilización de los medios, no logra preservar completamente los intereses del Estado y menos salvaguardar (Becerra, et al., 2019).

Para complementar, señala Sánchez (2017) no existe actualmente una legislación clara para afrontar este contexto, ni en términos ofensivos ni mucho menos defensivos, que llevan a dificultades legales y en consecuencia a generar riesgos en la práctica cibernética, sobre todo, por la nula aplicabilidad de acuerdos internacionales. Por tal motivo, no basta con generar espacios o acceso al ciberespacio, sino también, propiciar la estructuración y puesta en marcha de políticas serias y una legislación aplicable para garantizar la seguridad del Estado colombiano, apuntándole a estándares internacionales para garantizar el cumplimiento de la ley (Ministerio del Interior y Seguridad Pública, 2018).

Lo anterior, lleva a plantear, como tesis, que tanto la ciberseguridad como la ciberdefensa carecen de una legislación ajustada a las necesidades del Estado colombiano, presentando un alto riesgo que no le permite contrarrestar con efectividad las amenazas cibernéticas, sobre todo en la protección del Estado y sus activos estratégicos (Consejo Nacional de Política Económica y Social República de Colombia, 2016). Esto evidencia la necesidad de medidas claras para ampliar la seguridad y mejorar la confianza en los medios digitales, como un espacio incluyente con capacidades digitales en los sectores públicos y privados, incrementando así, su desarrollo y crecimiento en materia tecnológica,

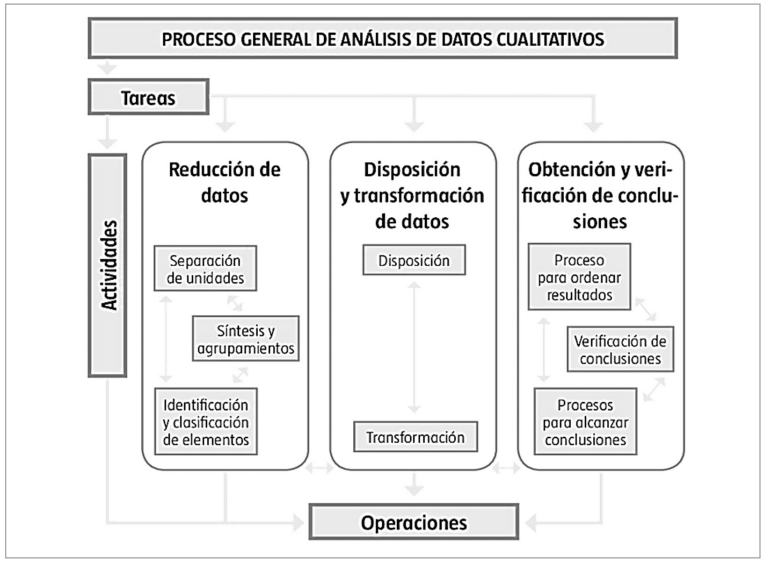
pero desde estándares destacados de seguridad digital (Consejo Nacional de Política Económica y Social República de Colombia, 2020).

Metodología

Se emplea un enfoque cualitativo a partir del análisis de fuentes abiertas y una codificación primer grado, para identificar diferentes categorías y características que no necesariamente llevan a una codificación axial. De esta manera, se agruparán dichas categorías en características asociadas al análisis de la literatura existente, para establecer las condiciones causales que requiere una ley de ciberseguridad y ciberdefensa en Colombia (Lozano, 2003).

El procedimiento se construyó desde una lógica inductiva para pasar de lo particular a lo general y con ello lograr el análisis de la información recopilada sobre la importancia de una ley de ciberseguridad y ciberdefensa para Colombia, sin que esto genere necesariamente un análisis estadístico, pero sí una clasificación e interpretación del fenómeno estudiado.

Figura 1. Proceso de análisis de datos cualitativos



Fuente: Elaboración propia

Etapa I

Inicialmente, mediante la recolección de las fuentes de información se profundizó en la problemática planteada para sintetizar la información (fuentes primarias y secundarias) que para Tamayo (2013) y Hernández et al (2014) llevan a la identificación y clasificación de los elementos relevantes de la muestra documental objeto de análisis.

Etapa II

En esta etapa se fundamentó en la trasformación de la información y la reducción de la misma mediante la separación de unidades de análisis para clasificar los elementos que respalden la importancia de una ley de ciberseguridad y ciberdefensa para Colombia y con ello brindar claridad mediante un muestreo documental (Ariza, 2007).

Etapa III

Por último, se logró la obtención de conclusiones a través de unidades y categorías de estudio por medio del análisis cualitativo proporcionado por el (ATLAS ti 9.0) que apoyan la interpretación y organización de la información de manera lógica, estructural y soportada la significancia otorgada en cada objetivo planteado.

Marco teórico y conceptual

El término de seguridad nace del latín securitas que según la RAE (2018) se define de acuerdo con el contexto, pero generalmente se asocia a la confianza y al mantenerse alejado de los riesgos y/o amenazas latentes. En este sentido, el concepto se trasforma hasta convertirse en un objetivo colectivo con el fin de garantizar la libertad individual (Vargas, 2017). En este orden se destaca también la defensa que se relaciona con las acciones militares que colaboran para mitigar dichos riesgos, amenazas o daños; por lo que sentirse seguro relaciona no solo a la respuesta, sino a la capacidad con que se cuenta.

De este modo, el Estado debe brindar una respuesta efectiva para prevenir, pero también garantizar adecuadas condiciones de vida, seguridad y confianza para satisfacer las necesidades de la sociedad. Esta relación entre la defensa y la seguridad, tal como lo afirma, se presenta intensamente por la influencia, intereses y relaciones de poder, no solo a nivel estratégico, sino del mismo modo en términos geopolíticos y tecnológicos, por el manejo de la información, las comunicaciones y los avances propiciados por la sociedad; entre los cuales se incluye el internet, las telecomunicaciones, los software, los computadores, las redes sociales y la interacción de las poblaciones y los escenarios online, también conocidos como ciberespacio que han llevado a modificar la concepción defensa y la seguridad (Nye & Villanueva, 2013).

Actualmente, el ciberespacio se estima que cuenta con alrededor de 5 mil millones de personas diarias conectadas al internet y se proyecta en los próximos 5 años a 50 mil millones y el acceso a 10 equipos por persona. En este contexto, más de 2 mil personas por minuto se encuentran comunicadas e intercambiando ideas y pensamientos a nivel mundial, generando hasta 41 millones de mensajes en un espacio de 60 segundos. De allí que los Estados basen su información en el uso de computadores, programas y aplicaciones para adaptarse a las condiciones actuales y optimizar sus recursos (Klimburg, 2020).

En este entorno, se puede afirmar que, si las economías mundiales y el bienestar están claramente relacionadas con el mundo online o el uso de la información en el ciberespacio, la seguridad y defensa deben encontrarse de igual manera cada vez más ligada a este mecanismo. Es decir, que las gestiones para defenderse de los riesgos, amenazas y peligros deben orientarse también a brindar la confianza necesaria en el contexto virtual desde la percepción real; y es que desde el ciberespacio no solo se debe buscar la seguridad individual, sino como un asunto de seguridad y soberanía nacional estrechamente ligada a la capacidad para gobernar (Choucri 2014).

Para Der Derian (2009) estos asuntos tecnológicos del ciberespacio han cobrado gran relevancia en las diferentes naciones; sobre todo por los factores asociados a las circunstancias como el resguardo de la información, el seguimiento, la seguridad, la simulación, la vigilancia y velocidad, que llevan a analizar quien tiene acceso a la información y los medios para llegar a ella. Esto lleva a advertir, cómo el uso de la información lleva a una ventana que puede vulnerar la seguridad nacional y generar pérdidas económicas, humanas, sociales y políticas, como las ocurridas en el atentado llevado a cabo en la brigada 30 en Cúcuta o la fuga de información de inteligencia colombiana hacia Venezuela, solo por mencionar algunos casos (Cepik & Brancher 2017).

Todo esto demuestra que los daños al Estado pueden verse generados a través del ciberespacio, que según Feenberg (2019) cuentan con la capacidad para asociar individuos a pesar de la distancia y fraguar planes en contra del Estado como espacio de conflicto. Esta razón precisamente ha llevado a considerar este fenómeno como una prioridad que debe ser abordada a nivel estratégico tanto a nivel nacional como internacional, con el fin de ser preventivos y menos reactivos en temas de defensa y seguridad.

En estas circunstancias emergieron ciertos términos como ciberataque, el cual se refiere a los intentos por atacar, destruir, alterar, saquear o acceder a información no autorizada de un Estado con el fin de causar una afectación gubernamental o poblacional. Esto lleva a generar el término de Ciberseguridad con dos sentidos; el primero, desde un factor estratégico en la que se identifican las condiciones del ciberespacio que se encuentren alejadas de amenazas o riesgos y el segundo, desde un concepto más operativo que busca preservar la reserva, integridad y disponibilidad de la información en el ciberespacio entre otros aspectos (Cepik, 2017).

Finalizando se encuentra el término de ciberdefensa, que resguarda su significancia a través de las acciones del Estado para protegerse y mitigar las amenazas y riesgos cibernéticos, con el objetivo de usar el ciberespacio con normalidad, pero del mismo modo, protegiendo los derechos, las libertades y brindando las garantías a todos los ciudadanos, en virtud de la soberanía y el mantenimiento territorial; pero sin eludir los nuevos escenarios que plantea la hibridez de los conflictos que de alguna manera inciden en el uso del ciberespacio (Virilio 1995). Así, no queda duda que los Estados deben fortalecer su Ciberdefensa desde su capacidad de respuesta a través de la constante evaluación del

enemigo. De esta forma, la ciberseguridad y ciberdefensa han cobrado gran relevancia y evolucionado hasta llegar a ser consideradas como una capacidad estratégica para el direccionamiento de un Estado (Samper 2015).

Dicho esto, una ley de ciberseguridad y ciberdefensa para Colombia cobra valor desde la necesidad por fortalecer al Estado, sino al mismo junto con la ley 1621, brindar herramientas para abordar el dilema jurídico que actualmente se presenta (Congreso de la República, 2013). De esta manera, lo que se busca es proteger al Estado, tal como lo mencionara Cicerón (2014) mediante las leyes se protege a la población y mientras existan, se deben respetar y hacerlas cumplir estratégicamente para aportarle soluciones a factores críticos a nivel nacional.

Regulación de Ciberseguridad y Ciberdefensa en Colombia

En Colombia la regulación en temas de ciberseguridad y ciberdefensa, aunque no presenta grandes antecedentes, si es importante realizar un análisis para reconocerla y al mismo tiempo evidenciar a los factores que apunta, explorar su enfoque y la relación con el entorno actual. En ese orden, inicialmente es relevante relacionar que a nivel nacional existe el Consejo Superior Digital de Protección y Defensa del Ciberespacio; conformado por los Ministros de Justicia, Relaciones Exteriores, Defensa, Tecnologías de la Información y las Comunicaciones (TIC) y el Director Nacional Inteligencia, el de Planeación Nacional, el Comandante de las Fuerzas Militares, el Director General de la Policía Nacional, el Fiscal General de la Nación y el consejero Presidencial de Seguridad que en medio de una crisis, podrá convocar al Presidente de la República o demás organismos para la atención de la misma (PNPICCN, 2017). Desde este consejo, se ponen en marcha las directrices generales para realizar el seguimiento, el análisis y la evaluación de diferentes amenazas que puedan afectar al Estado colombiano. Así, la coordinación y las acciones de los agentes del sistema buscan mitigar una situación crítica a nivel cibernético; buscando con estas acciones propiciar los mecanismos para prevenir afectaciones en contra de la infraestructura desde la planificación y operación del organismo, que para el caso de Colombia también se soportan en una serie de normas que se relacionan a continuación.

Normatividad Nacional

En cuanto a la normatividad nacional, según la Constitución Política de Colombia (1991) en primer lugar, es importante mencionar la existencia varios aspectos constitucionales orientados a la seguridad digital. Uno de ellos es el artículo dos que busca garantizar la efectividad de los principios, derechos y deberes consagrados en la constitución. De la misma manera, en el capítulo II, particularmente en el artículo 15, se reconoce el derecho

a la intimidad y la obligación del Estado a respetarla y hacerla respetar; y en el artículo 20, donde se le debe garantizar a toda persona la libertad de expresión para difundir sus opiniones y pensamientos, al tiempo de poder informar, recibir información veraz e imparcial y también de poder fundar medios masivos de comunicación. De igual modo, la Constitución Política de Colombia establece en su artículo 76 que el espectro electromagnético es un bien público sujeto a la gestión del Estado, donde en el mismo artículo 101 incluye este factor como parte del territorio nacional y junto a ello, señala la responsabilidad y capacidad de las Fuerzas Militares para resguardar y proteger el territorio y soberanía de Colombia (Constitución Política, 1991)

Asimismo, Colombia cuenta con el Código Penal del 2000 y la Ley 1273 del 2009 como parte normativa y procesal para hacer frente a los delitos cibernéticos; reconociendo, a su vez, los tratados internacionales de la INTERPOL Y EUROPOL. De igual modo, la Ley 1581 del 2012 como soporte o marco básico para regular la protección de datos, su divulgación y violaciones de la seguridad. Frente a estos aspectos normativos de carácter ordinario, también se evidencian diferentes herramientas legales para regular la seguridad digital en circunstancias relacionadas con los derechos de autor, la pornografía, el comercio electrónico y la explotación sexual de menores en el ciberespacio, entre otros(Giral-Ramírez et al., 2017)

También se evidencia un avance normativo a nivel nacional que aborda aspectos relacionados con la firma electrónica, el habeas data, herramientas de autenticación y el registro nacional de bases de datos (Sarmiento, 2016). Finalmente, también se pueden divisar en el panorama nacional, otros decretos y actos administrativos que reglamentan diferentes actividades que regulan el ciberespacio, como la circular 052 de 2007 que instaura las pautas de seguridad y calidad para el manejo de la información de medios y canales de distribución de productos y servicios, la Resolución la CRC 3066 y 3067 de 2011 que establece los parámetros integrales de protección de los derechos de los usuarios para el servicio de telecomunicaciones, el Decreto 1704 de 2012 que regula y condiciona las interceptaciones de comunicaciones, la resolución de la Superintendencia de Industria y Comercio Nº. 76434 de 2012, que establece la protección de datos personales y, por último, del Decreto 2573 de 2014, que regula el Gobierno en línea para la utilización y soporte de la ciudadanía; todo esto, sin dejar de lado el Consejo Nacional de Planeación (CONPES) como entidad con capacidades para la generación de políticas y el desarrollo del país (CONPES, 3701).

Consejo Nacional de Planeación (CONPES)

Aunque el CONPES no es reconocida por sí misma como una normatividad, si es la entidad encargada para liderar y presentarle al Gobierno Nacional, los elementos, políticas, planes y programas estratégicos, proyectados al desarrollo económico y social del país.

Esta busca como objetivo fundamental, a través de los documentos CONPES, el fortalecimiento de las capacidades del Estado para el enfrentamiento de las amenazas que puedan atentar contra su seguridad y defensa. De allí que surja como iniciativa fundamental la política para la Ciberseguridad y la Ciberdefensa (CONPES 3701).

CONPES 3701

Inicialmente en Colombia se generó el documento CONPES 3701, que identificó la debilidad del Estado para contrarrestar las amenazas cibernéticas, ya que el sector público no tenía una iniciativa para dicha problemática, por consiguiente, no existía una estrategia nacional, un sistema y un marco legal enfocado a la seguridad cibernética. Asimismo, el documento señalo otros factores que indicaban que Colombia era una nación vulnerable en el tema de la ciberseguridad, tales como el constante incremento de los usuarios de internet, el alto grado de dependencia de las infraestructuras críticas y la alta frecuencia de delitos informáticos

Ante la situación anterior, el documento CONPES 3701 presentó los lineamientos de la política de ciberseguridad y ciberdefensa para contrarrestar las amenazas del ciberespacio. En esta política se destacan la seguridad y defensa digital del Estado como parte primordial, buscando fortalecer las capacidades para hacerle frente a las amenazas que pueden llegar a atentar contra la defensa y seguridad nacional en el contexto cibernético (Consejo Nacional de Política Económica y Social República de Colombia, 3701).

En esta protección se destacan tres objetivos específicos primordiales; el primero de ellos, lograr implementar las capacidades para la prevención, coordinación, atención y control de las emergencias cibernéticas para enfrentar las posibles amenazas y los riesgos que puedan afectar la ciberseguridad y ciberdefensa nacional; el segundo, ampliar las líneas de investigación y capacitación en la seguridad de la información en estos aspectos; y el tercero, fortalecer permanentemente la normatividad y la cooperación internacional con el fin de estar a la vanguardia delos estándares y regulaciones exigidas (López, 2019).

CONPES 3995

El CONPES 3995 formula la política de confianza y seguridad digital que busca instaurar las medidas, generar la confianza y mejorar la seguridad a través del fortalecimiento de las capacidades de la seguridad digital para la población colombiana, el sector público y privado, actualizando constantemente el control y la gobernanza para el desarrollo nacional y con ello, adoptar modelos en materia de seguridad digital enfatizando en nuevas y mejores tecnologías (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020). De igual modo, este CONPES pretende mediante la regulación,

afrontar efectivamente las nuevas amenazas a través de la formulación y actualización de estrategias relacionadas con la seguridad en el ciberespacio (Consejo Nacional de Política Económica y Social República de Colombia, 3995).

Colombia además es miembro de la INTERPOL y de la EUROPOL tal como se mencionó anteriormente, priorizando su cooperación internacional a través de la ley Nº 1928/2018 y la aprobación del convenio de Ciberdelincuencia el 16/03/2020 (Budapest, 2001) adhiriéndose como un instrumento de apoyo a la Ciberseguridad mundial, apoyado también a través de la política digital Nº 1.008/2018 para el uso y aprovechamiento de las TICs buscando consolidar el Estado mediante un entorno de confianza y cumplimiento de la regulación actual.

Dificultades Normativas de Ciberseguridad y Ciberdefensa en Colombia

Según Ceballos (2020) la ciberdefensa y ciberseguridad son elementos críticos para la prosperidad y seguridad de una nación, teniendo en cuenta que las actividades maliciosas ejecutadas por individuos o grupos al margen de la ley ponen en riesgo tanto al Estado como a sus democracias y habitantes. De allí, que la seguridad dependa en gran medida de las capacidades civiles y militares que se tengan para proteger la infraestructura de las amenazas cibernéticas; que mediante herramientas y sistemas seguros podrán prevenir y mitigar de sus impactos. Esta percepción, según Becerra et al. (2019) ha sido reconocida desde la estrategia global y/o política exterior de seguridad de la Unión Europea, considerando este aspecto como una amenaza hibrida que debe de llevar a los Estados a aumentar su capacidad tecnológica y humana para el desarrollo e implementación de un enfoque integral, para el fortalecimiento de la ciberseguridad y ciberdefensa a nivel nacional, regional y mundial (Organización de los Estados Americanos, 2004)

Dicho fortalecimiento requiere un abordaje integral, donde se conjuguen herramientas, mecanismos, estructuras eficientes y una sólida normatividad que permita promover el uso del ciberespacio desde una perspectiva de ciberdefensa y ciberseguridad, para promover el avance tecnológico, la promoción de expertos y el cumplimiento de la ley en general. Aunque para Castañeda (2019) debe ir de la mano de los operadores y proveedores de servicios que en gran medida mantienen la responsabilidad de las redes (Giral-Ramírez et al., 2017) y los sistemas de información, ajustándose a la normatividad y buscando la generación de una cultura de riesgos que permita la implementación de medidas de seguridad y control para mitigar las amenazas que enfrentan el mundo en la actualidad, sobre todo por las sofisticadas tecnologías a las que se tiene acceso (Serrano, et al., 2019)

En este sentido, tal como lo reconoce Moreno (2020) la ciberseguridad y ciberdefensa no solo dependen de un control interno, sino también de la capacidad de disuasión

sobre otras naciones; provocando o no una estabilidad cibernética que aumenta o disminuye la efectividad para contrarrestar las amenazas externas y prevenir los ataques y la afectación de los mismos. En tal sentido, en la naturaleza de la amenaza global se deben contemplar la construcción y preservación de acuerdos esenciales para la prevención y persuasión de ataques cibernéticos; cada vez más críticos para la seguridad y estabilidad de una nación, pero que también pueden mitigarse a través de un marco normativo estratégico que permita la regulación del ciberespacio y sus componentes en cuanto a la seguridad.

De esta forma la Unión Europea (UE) ha promovido la posición que el derecho internacional y particularmente la carta de las Naciones Unidas (2018) se apliquen al ciberespacio complementando el derecho internacional vinculante, alentando de igual forma el incremento de las capacidades para desarrollar e implementar medidas que permitan fomentar la confianza a nivel de la seguridad y también en términos de cooperación regional e internacional; teniendo en cuenta que estas alianzas facilitan el reforzamiento y mantienen la responsabilidad de los Estados en el control y regulación del ciberespacio en general, que para el caso de Colombia se requiere analizar desde los vacíos de la legislación existente y sobre todo desde la aplicabilidad y cumplimiento de la misma (Moreno, 2020).

Debilidades normativas

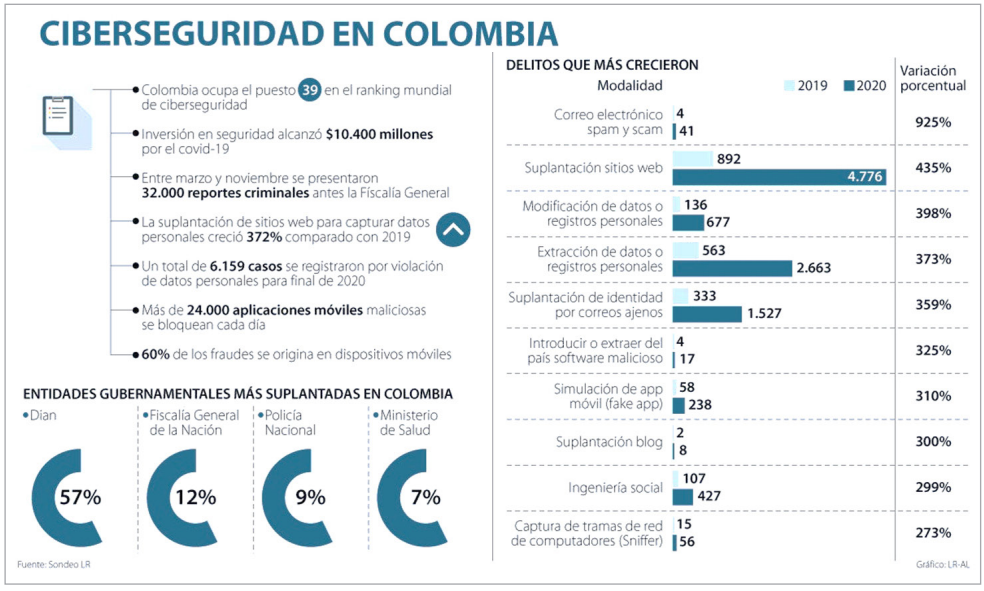
Colombia, según Ruiz (2018) viene adoptando medido y herramientas legales que en términos de ciberseguridad y ciberdefensa comenzarían a fortalecerse a partir de su segunda política en el año 2016, cinco después años de haber salido la primera. Esta buscó fortalecer las capacidades nacionales para responder, reconocer, gestionar y prevenir los riesgos en el ciberespacio, incorporando en ella un coordinador nacional de seguridad digital a cargo de la Presidencia de Colombia. Asimismo, generando un comité de seguridad digital como máximo ente para abordar situaciones intersectoriales de seguridad a cargo del coordinador nacional de seguridad digital e incluyendo, este apartado, aspectos integradores para el desempeño, la operación y seguimiento de entidades públicas y privadas.

De igual manera, el Ministerio de Tecnología y las Comunicaciones (MinTIC) buscó desplegar, a lo largo y ancho del territorio nacional, el modelo de seguridad y privacidad para gestionar e implementar estándares efectivos para salvaguardar los activos críticos de la nación (infraestructura, información y herramientas de comunicaciones); proyectando la mejora continua a nivel nacional e internacional. Además de buscar el desarrollo de un programa para el fortalecimiento de la infraestructura crítica cibernética, apuntándole a la transformación digital, que, junto a la legislación reseñada en el capítulo anterior, buscaría prevenir los ataques y los intereses del Estado (Quintero, 2019).

Después de todo, Colombia ha desplegado medidas para asegurar el ciberespacio y con ello proyectar elementos estratégicos en ciberseguridad y ciberdefensa a nivel nacional, sobre todo en la estructuración de políticas que, a pesar de sus vacíos, han brindado un punto de inicio para prevenir y mantener la estabilidad nacional; pero también generan un ambiente de poca confianza en su aplicación y respaldo jurisprudencial. Esta desconfianza preocupa, no solo por la débil regulación, sino también por su carente divulgación que, a pesar de los organismos responsables, presentan una nula precaria efectividad a nivel nacional y transnacional (Ruiz, 2018).

En este orden, según Salazar (2019) a pesar de los esfuerzos legales, esta normatividad en Colombia se ha convertido en una legislación disuasiva, carente de unas bases político militares que respalden los vacíos jurídicos presentados, sobre todo, pensando que la afectación en la ciberseguridad y ciberdefensa en Colombia, en su mayoría, son delitos cometidos desde otras naciones, dejando la regulación colombiana sin campo de aplicación en otros Estados. Estos crímenes han presentado un crecimiento exponencial, aumentando un 37% entre el 2019 y el 2020, tal como se evidencia en la figura 2, donde paralelamente se asocia al incremento y uso de nuevas tecnologías, provocando que los ciberataques convirtieran esta amenaza en una de las principales economías ilegales en Colombia (Rodrigo, 2021).

Figura 2. Ciberseguridad en Colombia



Fuente: Sondeo LR

Con respecto al documento CONPES 3701, se descuidaron aspectos relevantes dentro del mismo, tales como: la ausencia de protocolos que facilitaran acciones correctas

en relación con la seguridad cibernética (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020). La falta de aplicabilidad en las entidades territoriales, ya que al ser ejecutado en las entidades estatales, el riesgo cibernético se traslada a los territorios, la falta de un órgano regulador de las agencias militares relacionadas con la Ciberdefensa de la nación, falta de equilibrio de la normatividad colombiana con los estándares internacionales promovidos por la Convención de Budapest, ausencia de políticas claras para proteger los derechos humanos de los usuarios del internet, ausencia de personal fiscal idóneo para investigar y sancionar los ciberdelitos (Parra, 2019)

En este lapso entre el 2019 y 2020 de acuerdo con el análisis de Asuntos Legales (2020) se registraron más de 7.000 mil denuncias de cibera taques equivalentes a un 27% de acuerdo con los datos suministrados por la Cámara Colombiana de informática y de telecomunicaciones, mientras los delitos ejecutados a través de medios informáticos pasaron de 21 mil a 36 mil reportando un incremento del 83% entre un año y otro, los delitos financieros presentan la mayor proporción e impacto.

Según la Universidad del Rosario (2019) el 81% de las empresas en Colombia presentan acceso a internet, pero menos del 1% de sus ingresos son destinados a reforzar sus mecanismos de prevención y, el 43, % de estas empresas no están preparadas para enfrentar algún ataque, y las del Estado incluyendo la DIAN, Fiscalía, Registraduría entre otras, no han estado exentas del uso de su nombre para ser suplantadas e incluso a pesar de sus tecnologías ser vulneradas cibernéticamente. Y en materia de Ciberseguridad y Ciberdefensa en Colombia para Vargas (2018), la criminalidad informática ha ido aumentando a partir de la vulnerabilidad de las entidades y empresas, pero también de los vacíos legales; sobre todo por la penalización tan permisiva con la que se cuenta, además de que el principal referente para atacar este tipo de crímenes es el convenio de Budapest del 16 de marzo del 2020, el cual aunque genera confianza entre los Estados, no se ha adoptado ni adaptado para propiciar los elementos e instrumentos jurídicos como un mecanismo de aplicación factible para el Estado colombiano.

Ahora bien, en Colombia la falta de una normatividad estandarizada y carecer de un bloque regional e internacional fuerte y la voluntad política, dificulta la cooperación internacional, sobre todo a nivel regional; donde incluso ni el hacer parte el convenio de Budapest, ha llevado a actualizar ni a construir una legislación procesal que refuerza las políticas existentes y castigue con mayor rigor los crímenes en el ciberespacio. Esto hace más crítico el panorama actual, reflejado en los altos índices de impunidad que, a pesar de los avances normativos, aún carece de elementos contundentes para la identificación, colaboración, definición, penalización y castigo en concordancia con la legislación interna y latinoamericana (Moreno, 2020).

De esta forma, aunque puede adaptarse a un marco normativo de mayor relevancia, entendiendo que su promedio según Ceballos (2020) que de acuerdo con el Capability

Maturity Model CMM se encuentra en 2 (donde 1 significa etapa Inicial y 5 Dinámica o Avanzada), esto demuestra que, a pesar de los avances alcanzados, aún presenta sistemas inmaduros e iniciativas pilotos sin la coordinación de los entes y elementos involucrados.

En consecución, el reto de la Ciberdefensa y la Ciberseguridad radica en la construcción y aprobación de leyes que no solo regulen el uso del ciberespacio, sino que también condenen con mayor rigor a quienes violen el marco normativo. Para ello, se debe contar con la participación de todos los actores que colaboren en el desarrollo de los mecanismos para introducir el respeto por la normatividad, la generación de una cultura del riesgo cibernético y la adquisición de competencias generadas a través de organizaciones como el *Foro para la Gobernanza de Internet* (Ceballos, 2020).

Finalmente, los esfuerzos de Colombia demuestran importantes avances, pero también grandes vulnerabilidades, que hacen necesario promover una ley de Ciberdefensa y Ciberseguridad en Colombia, donde asociadas a políticas sólidas, protejan al Estado, sus organizaciones y los bienes de los colombianos, mediante estándares de seguridad que impidan la evasión de las sanciones penales y económicas, amparándose en la carente instrumentalización de la ley y la ambigua definición técnica de los delitos que deben castigar teniendo en cuenta su gravedad y afectación.

Aspectos relevantes para una ley de Ciberseguridad y Ciberdefensa en Colombia

Los avances tecnológicos y las comunicaciones han sido desarrollos globales para beneficio de la humanidad, que para Arboe (2020) aunque no las convierte en inadecuadas, si pueden ser utilizadas para el accionar ilegal de los grupos al margen de la ley, propiciando gran afectación al Estado, sus organismos y la población en general. Por esta razón, el Estado colombiano ha estructurado una serie de normas para contrarrestar estas amenazas desde el apoyo operacional de Ciberdefensa y Ciberseguridad, pero todas ellas sin el alcance necesario para mitigar el impacto nacional generado por los grupos al margen de la ley.

La preocupación no es para menos, dado que los delitos cibernéticos se han convertido en una forma emergente de la delincuencia nacional y transnacional como uno de los fenómenos de más rápido crecimiento. Para Hernández y Fojón (2016) a medida que el Internet y la tecnología crecen, los delincuentes más se aprovechan de ello, logrando que el delito cibernético crezca a la medida en que avanza la tecnología, logrando evadir la judicialización que se hace cada vez más compleja, y convirtiendo al Estado, las instituciones y las mismas Fuerzas Militares como objetivos de mayor vulnerabilidad para estos grupos ilegales.

A pesar de que las Fuerzas Militares de Colombia cuentan dentro de la organización con unidades tácticas estructuradas y organizadas, y una serie de mandos para cumplir eficazmente la misión relacionada con las operaciones en el ciberespacio; es necesario la generación de una ley que aborde y respalde esta labor sin impedimentos, sobre todo para el abordaje adecuado de la Ciberseguridad y Ciberdefensa en Colombia. Esto debe contar inicialmente con la alineación interinstitucional que permita la planeación, ejecución, seguimiento y mejoramiento continuo desde un objeto misional que favorezca al Estado colombiano y desde allí se logre afrontar el delito Ciberespacial sin alterar las operaciones de Ciberdefensa pasivas y activas a nivel nacional y/o transnacional (Hernández y Fojón, 2016).

Iniciativas o Marco Operacional

La ley en ciberseguridad y ciberdefensa en Colombia requiere pasar de simples iniciativas para consolidar, desde una normatividad, un marco operacional que permita integrar esfuerzos institucionales (tanto privados como públicos) para propiciar organismos a nivel nacional que permitan coordinar y desarrollar operaciones, implementando los mecanismos suficientes para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio, donde a su vez, se ataque la débil difusión, concientización y generación de una cultura de prevención para la acción segura en Ciberdefensa dirigida tanto al sector público como al privado, así como a la sociedad civil (Restrepo, 2014).

De esta forma, según Vargas (2018) se podrán defender intereses nacionales desde un marco normativo de la mano con la política de seguridad nacional, apoyando el Estado desde aspectos trascendentales como la diplomacia, el liderazgo y factores comerciales, así como sus obligaciones internacionales (Convenio de Budapest) y la sociedad global con la (OTAN) desde un entorno cambiante rápido, eficaz y exitosa ante los peligros, pero sin poner en riesgo la soberanía, la integridad del territorio nacional, el derecho y la libertad de los ciudadanos, su seguridad y la del Estado. Prevenir una crisis, conflictos nacionales, regionales o internacionales, entonces, soportan la aprobación de una ley de ciberseguridad y ciberdefensa, sobre todo pensando en las amenazas que envuelve al Estado, junto a la preocupación del acceso al ciberespacio que busca mitigar los ataques y las amenazas cibernéticas del crimen organizado (Sarmiento, 2016).

Normatividad Ciber en las Fuerzas Militares

Es importante que la ley de ciberseguridad y ciberdefensa contemple la normatividad que permita soportar las capacidades e implementación del entorno ***Ciber*** en las Fuerzas Militares y de forma paralela permita el apoyo de las Fuerzas Armadas colombianas de tierra, mar y aire, entendiendo que el ciberespacio es el nuevo campo de batalla y el mundo

continúa cambiando, presentando episodios a nivel nacional e internacional que dan muestra de los alcances y gravedad y abordaje de estas confrontaciones. Lógicamente, este apartado deberá contemplar aspectos importantes como procedimientos, personal capacitado y expertos en Ciberdefensa y Ciberseguridad orientado desde una preparación integral con capacidad para efectuar operaciones militares en el ciberespacio para preservar la integridad del Estado (Rojas, 2021).

Lo anterior, para Quintero (2019) se contrarresta a partir del marco legal que debe contemplar la forma de abordar los riesgos y/o amenazas de los activos estratégicos del Estado, que a través de una unidad de Ciberseguridad y Ciberdefensa y mediante una estructura especializada para los desafíos, implican el dominio ciberespacial. Todo esto bajo la designación de mandos responsables para el desarrollo de operaciones en el ciberespacio que permita mediante unidades fundamentales y especializadas, contar con personal idóneo y aprovechar las capacidades y la experticia en beneficio del Estado colombiano.

Siguiendo a Quintero (2019) deberá estar estandarizado y adaptado al Convenio de Budapest y la OTAN y de esta manera, según Moreno (2020) las políticas, normatividad y directrices actuales podrán reorientarse para promover un cambio pragmático de estandarización como lo exigen los retos del futuro, necesarios para el accionar de la *Ciberinteligencia y la Ciberdefensa* colombiana sin las limitantes en la conducción de la guerra de la información incorporando tácticas internacionales de la OTAN en ambientes complejos donde se respalde el actuar militar a partir de la transformación y conducción de los intereses estratégicos de Colombia, para dotar al cuerpo militar y las agencias de seguridad del gobierno para efectos de neutralizar la fuerza del enemigo, mantener el pie de fuerza propio y evitar la proliferación de los ataques controlados, dirigidos y guiados electrónicamente, para obtener información del estado como parte de una estrategia militar nacional, regional o global, para controlar los tipos de confrontación a que haya lugar.

Aplicabilidad de la normativa sobre las tecnologías militares

Hasta el momento los avances en ciberseguridad y Ciberdefensa se encuentran en la aplicabilidad del documento CONPES 3701. Parra (2019) indica la creación de las siguientes instituciones encargadas de ejecutar la política de ciberseguridad y Ciberdefensa:

Comisión Intersectorial, que se encarga de *establecer los lineamientos de política con relación a las tecnologías de la comunicación y la información y el tema de ciberseguridad y ciber defensa.* Esta comisión se encuentra conformada por el Presidente de la República, los Ministros de Defensa y de las Tecnologías de la Información y las Comunicaciones, los directores de la Policía Nacional, Planeación Nacional y el ColCERT (Parra, 2019).

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, integrado por personal civil, militar y de otras instituciones y tiene a cargo la coordinación de todas las acciones relacionadas con la protección de la infraestructura crítica del gobierno con respecto a los temas de ciberseguridad y ciberdefensa que puedan comprometer la seguridad de la nación (Parra, 2019).

El Comando Conjunto Cibernético de las Fuerzas Militares – CCOC, conformado por el Comando General de las Fuerzas Militares, con la ayuda de las unidades cibernéticas del Ejército, la Armada y la Fuerza Aérea. Previniendo y contrarrestando los ciberataques contra la infraestructura crítica del gobierno colombiano (Parra, 2019).

El Centro Cibernético Policial: es una plataforma virtual que se encarga de regular todo lo relacionado con los delitos cibernéticos, tales como el extraer información confidencial de bases de datos de las empresas, suplantar sitios web y realizar pornografía infantil, también persigue y sanciona las nuevas redes criminales que usan las nuevas tecnologías para lograr sus acciones delictivas, también realiza campañas de prevención de los ciberataques, y realizar investigaciones en compañía del ColCERT para identificar las vulnerabilidades y eventos informáticos que se encuentran relacionados con la afectación de la seguridad de la infraestructura crítica cibernética del gobierno (Parra, 2019).

El CSIRT PONAL, que es un grupo conformado para brindar ayuda, prevenir e investigar los eventos relacionados con la seguridad de la información, y disminuir el impacto causado por los riesgos de las tecnologías de la información y las comunicaciones (Parra, 2019).

Adicionalmente, a causa de la implementación del documento CONPES 3701, el gobierno colombiano ha dispuesto algunas normativas y doctrinas, las cuales son:

- Política de defensa y seguridad para la nueva Colombia
- Plan estratégico militar PEM 2030
- Ley Estatutaria 1621 de 2013, que fortalece la normativa relacionada con actividades de inteligencia y contrainteligencia
- Resolución 3933 de 2013, que reestructura el Ministerio de Defensa
- Resolución 7436 de 2012, que contribuye a la creación del Comando Conjunto Cibernético
- Oficio no. 05289/cgfm-jemc-jeimc-disai-29-25 del 24 de agosto de 2012, referente a la creación de unidades de Ciberdefensa en las fuerzas militares

Igualmente, surge el CONPES 3854 en el año 2016, referente a la Política Nacional de Seguridad Digital, enfocada en el fortalecimiento de las capacidades de los organismos encargados de la seguridad digital en Colombia, para gestionar los riesgos relacionados

con entornos digitales, aspectos que no se incluyeron en el anterior CONPES 3701, lo cual toma forma en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital creado por el MinTic (Parra, 2019).

La aplicación de las tecnologías y su utilización desde el marco legal deben de presentarse con toda la claridad en una ley de Ciberdefensa y Ciberseguridad en Colombia, sobre todo teniendo en cuenta el nivel de desarrollo operacional y estratégico requerido en cualquier tipo de escenario; estableciendo los intereses del Estado como el factor primordial para contrarrestar o neutralizar las nuevas amenazas emergentes. Ahora bien, como dentro del amplio concepto de aplicabilidad; se encuentran diversos enfoques para el afrontamiento de este aspecto, considerando el entendimiento de la naturaleza del empleo de la tecnología, su transición y posicionamiento a través de (Comandos, Controles, Comunicaciones, Computadores, Inteligencia, Vigilancia y Reconocimiento), de acuerdo con los objetivos de defensa y seguridad para responder de manera oportuna a los ataques y cambios tecnológicos en el futuro (López, 2019).

Por otra parte, para Lind (2017) se debe fortalecer la taxonomía del marco de referencia internacional de ciberdefensa y ciberseguridad, como principal herramienta militar para la protección del Estado colombiano en cuanto a aspectos de conducción y manejo del Ciberespacio por parte de las Fuerzas Militares y los organismos nacionales para atender el funcionamiento y aplicabilidad de las tecnologías militares complejas disponibles en el mercado y producidas principalmente por empresas subsidiarias del estado o del sector privado de los Estados Unidos, Israel, Reino Unido Rusia, China, Francia, Dinamarca, Suráfrica, entre otros. Asimismo, este factor colaborará en resolver los problemas de origen taxonómico del abordaje de la Ciberdefensa y la Ciberseguridad para optimizar los recursos aportados por el Estado y desarrollando de manera efectiva por la fuerza pública, logrando un impacto social positivo de acuerdo a la utilización de nuevas herramientas tácticas operacionales en el modo de conducción de este contexto como parte de la inteligencia militar.

Estándares de Ciberdefensa y Ciberseguridad

Los estándares mínimos se convierten, según Murillo (2016) en un factor de suma importante en el origen y generación de un marco normativo para la Ciberseguridad y la Ciberdefensa en Colombia; en el cual se alberga su producción, directrices y tareas tácticas sobre el desarrollo de operaciones y las maniobras de armas combinadas y sus dimensiones para fundamentar el direccionamiento y conducción del ciberespacio en cualquier campo de combate. Esto deberá explicarse claramente desde el amplio rango de tácticas, técnicas y procedimientos de inteligencia, mediante el empleo de sistemas militares electrónicos para el desarrollo de operaciones, altamente útiles para la identificación de procedimientos, tácticas y técnicas utilizadas para el diseño de estrategias

militares; asimismo aportando al fundamento lógico para la implementación y optimización de las estrategias requeridas.

Los procedimientos y actividades deberán describirse junto al empleo de la inteligencia, de comunicaciones, electrónica, de imágenes, ataques electrónicos y de sensores activos, de acuerdo con el artículo 17 de la ley estatutaria 1621 del 17 de abril del 2013 ley de inteligencia y contrainteligencia, con el fin de obtener información para el posterior análisis con el fin de apoyar el proceso militar para la toma de decisiones. Esto, tal como lo menciona Pollit (2017) propone una precisión aclaratoria de los procedimientos y acontecimientos en la intervención de sistemas de seguridad y redes complejas de información, teniendo en cuenta la importancia en el empleo y acondicionamiento de tecnologías para la seguridad y defensa nacional con la preservación de la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y con el carácter de información reservada según la Ley de Inteligencia y Contrainteligencia 1621 (2013).

Resultados

Los resultados generados para el artículo *Importancia de una Ley de Ciberseguridad y Ciberdefensa en Colombia* se generan a partir del tratamiento de la información analizada para responder a la problemática planteada. Para ello, en primera instancia se efectuó un análisis unidimensional desde la frecuencia y repeticiones de palabras a partir de las similitudes asociadas a la categoría de importancia de una ley de ciberseguridad y ciberdefensa, para lograr en segunda instancia, la representación gráfica del fenómeno analizado a partir de la utilización del ATLAS ti 9.0. Así, se logró sintetizar la información establecida en 5 variables (Contexto, Escenario, Intereses, Falencias, Necesidades) por su incidencia y 18 códigos por su frecuencia igual o superior a 20, tal como se evidencia en la Tabla 1.

Tabla 1. Matriz de Categoría – Importancia Ley de Ciberdefensa y Ciberseguridad

Nº	Variables	Códigos	Frecuencia
1	Contexto	Nacional	56
		Internacional	60
2	Escenario	Legal	133
		Militar	140
		Operacional	150

Continúa tabla...

Nº	Variables	Códigos	Frecuencia
3	Intereses	Grupos Ilegales	60
		Políticos	62
		Defensa y Seguridad	84
		Operacionales	92
4	Falencias	Aplicación	60
		Persuasiva	66
		Normativas	72
		Legales	84
5	Necesidades	Unificar el Marco Normativo	60
		Marco Operacional	69
		Aplicabilidad de tecnologías	70
		Estándares de Ciber	93
		Respaldo Legal	106

Fuente: Elaboración propia

En este análisis se demuestra elementos comunes que certifican la importancia de una ley de ciberseguridad y ciberdefensa en Colombia. De esta forma, la simplificación de la información demuestra variables de mayor relevancia (Contexto, Escenario, Intereses, Falencias y Necesidades) en el cual, el contexto evidencia cómo esta problemática se relaciona directamente con el entorno nacional, pero con una mayor preponderancia a nivel Internacional.

En cuanto al escenario, se vinculan el legal, militar y operacional, con una preponderancia similar en su importancia, al tiempo que demuestra su relevancia en estos tres indicadores. Referente a los intereses relacionados en la temática analizada, se denotan los grupos ilegales, la política asociada al fenómeno, pero con mayor incidencia la necesidad de la defensa y seguridad nacional al tiempo del actuar operacional. Respecto a las falencias presentadas, se evidencia la falta de aplicación en la normatividad existente, la cual pasa a ser un tema más de persuasión, presentando a su vez grandes vacíos normativos y una necesidad legal efectiva.

Por último, en cuanto a las necesidades detectadas en el estudio, es importante mencionar que se requiere la generación de una ley en ciberdefensa y ciberseguridad desde la unificación del marco normativo existente, donde se fortalezca el soporte operacional, la aplicación de nuevas tecnologías y los estándares para lograr operar las Fuerzas Militares de Colombia bajo el respaldo de la ley y la aplicación de la misma. Por lo tanto, una posible propuesta para de una ley que integrase a todas las normativas mencionadas en el tema

de ciberseguridad y ciberdefensa, y que corrige la necesidad que señala la tesis planteada en este documento, estaría fundamentada en las siguientes condiciones:

- Adopción de estándares internacionales para fortalecer la seguridad de las redes de telecomunicaciones, incluyendo a empresas del sector privado.
- Formulación de disposiciones relacionadas con la protección de datos del usuario de las tecnologías de la información y comunicación
- Identificación de políticas de seguridad adicionales para garantizar el derecho al habeas data y la intimidad del usuario.
- Establecimiento de procedimientos claros para investigar los delitos informáticos y preservar la evidencia digital.

Conclusiones

Es importante destacar que el proceso de transformación tecnológica a nivel mundial requiere complementar el marco legal en materia de ciberseguridad y ciberdefensa en Colombia, implementando los procedimientos a nivel legal para que se puedan desarrollar las actividades operacionales ajustadas a las normas, parámetros y documentos soportados en la ley y no únicamente bajo el convenio de Budapest o bajo los parámetros establecidos por la OTAN. Adicionalmente, esta ley brindaría un aval jurídico de los resultados generados, dándole un valor tangible en el aspecto legal a estas actividades ejecutadas a través de técnicas, tácticas y procedimientos enmarcados en misiones de trabajo, acompañadas de órdenes operacionales de inteligencia, documentadas y descritas de forma detallada para abordar las amenazas y neutralizar las acciones de las mismas y con ello proteger al Estado colombiano.

Las amenazas de ciberseguridad y ciberdefensa en Colombia deben entenderse como eventos impredecibles y con un gran potencial para hacer daño, pero que adoptando medidas preventivas y ofensivas se puede obtener una ventaja sobre el adversario, sobre todo, si se cuenta con el soporte legal para operar desde una normatividad que respalde el accionar del Estado colombiano y sus funcionarios. En este contexto, las operaciones militares se podrán desarrollar abordando el ciberespacio de una forma legal, planeada a través del empleo de nuevas tecnologías, con el propósito de garantizar la seguridad y defensa del estado de la nación y reducir o neutralizar la acción del poder enemigo, con el fin de asegurar la ventaja operacional y adecuada acción del poder militar propio.

La creación de una ley integral de ciberseguridad y la ciberdefensa en Colombia sólida desde el contexto nacional e internacional depende de condiciones tales como la necesidad de implementar una cultura de seguridad digital en la sociedad, a través de mecanismos legales que hagan tomar conciencia sobre los riesgos y manifestaciones del delito informático que puedan afectar la seguridad de la nación, adopción de estándares internacionales de seguridad digital en las empresas del sector público y privado,

implementación de políticas relacionadas con la protección de los derechos humanos del usuario de la internet, además de protocolos que definan una línea a seguir para la investigación y sanción de los delitos informáticos en Colombia y de carácter transnacional.

La ciberseguridad y ciberdefensa necesitan de herramientas, mecanismos, estructuras eficientes y una sólida normatividad para regular el ciberespacio colombiano desde una perspectiva de seguridad nacional que permita promover el avance tecnológico, la promoción de expertos y el cumplimiento de la ley en general. Lógicamente, del ajuste de la normatividad se podrá generar una cultura de riesgos que permita la implementación de medidas de seguridad y control para mitigar las amenazas que enfrenta Colombia debido a las sofisticadas tecnologías que actualmente se presentan.

El identificar el marco legal de la seguridad informática en Colombia, permite conocer el avance del gobierno en relación con los continuos cambios de las tecnologías de la información y la comunicación, y cabe mencionar que esta problemática no solamente es exclusiva del gobierno, sino de la sociedad en general, pues se necesita la integración de todas las esferas sociales y políticas para contrarrestar los riesgos relacionados con el ciberespacio.

Los esfuerzos legales en Colombia en temas de ciberseguridad y ciberdefensa son en la actualidad más disuasivos y menos efectivos, ya que carecen de unas bases político militar que respalden los vacíos jurídicos presentados, sobre todo por el nulo campo de aplicación actual y el crecimiento del 37% entre el 2019 y el 2020 de delitos relacionados con este contexto que lo convierten en una de las principales amenazas para Colombia por la evasión de las sanciones penales y económicas amparadas en la carente instrumentalización de la ley y la ambigua definición técnica de los delitos que deben castigar.

Declaración de divulgación

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

Autor

Julián Antonio Guzmán Pacheco. Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Gerente en Seguridad y Análisis Sociopolítico, Escuela de Inteligencia y Contrainteligencia Brigadier General Ricardo Charry Solano, Colombia. Especialista en Administración y Conducción de Unidades Militares, Escuela de Armas Combinadas Ejército, Colombia. Especialista en Administración de Recursos para la Defensa Nacional, Escuela de Armas Combinadas Ejército, Colombia. Profesional en Ciencias Militares, Escuela de Cadetes José María Córdova, Colombia.

ORCID: https://orcid.org/0000-0003-0950-0733
Contacto: guzmanja@esdeg.edu.co

Referencias

Alcaide, Joaquín. (2019). *Delitos electrónicos ante el Derecho Internacional Contemporáneo*. Madrid: Editorial Tecnos.

Arboe, F. (2020). *Chile y legislación en Ciberseguridad ¿en qué punto nos encontramos?* https://blog.nivel4.com/noticias/chile-y-legislacion-en-ciberseguridad-en-que-punto-nos-encontramos/.

Asuntos Legales. (2020). *Ciberdelitos aumentaron 37% durante el primer trimestre de 2020.* https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480#:~:text=A%20pesar%20de%20la%20reactivaci%C3%B3n,en%202019%20a%2036.834%20delitos.

Becerra, A. Sánchez, E. Castañeda, A. Bohórquez, A. Páez, R. Contreras, A. y León, I. (2019). *La Seguridad en el Ciberespacio un desafío para Colombia*. Sello Editorial ESDEG.

Ceballos L., A. (2020). *Tendencias Cibercrimen en Colombia 2019-2020*. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Cepik, M. A. C., & Brancher, P. T. L. (2017). Structure and agency in international relations: state-building and the evolution of the international political system. *Austral. Porto Alegre.* Vol. 6, n. 11 (Jan./Jun. 2017), p. 154-189.

Choucri, N. (2014). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences.

Congreso de la República. (17 de Abril de 2013). *Ley Estatutaria 1621 del 2013* . Bogota DC, Colombia.

Consejo Nacional de Política Económica y Social República de Colombia. (2011). CONPES 3701 *Lineamientos de Política Para Ciberseguridad Y Ciberdefensa*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social República de Colombia. (2016). CONPES 3854 *POLITICA NACIONAL DE SEGURIDAD DIGITAL*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social República de Colombia. (2020). CONPES 3995 *Politica Nacional de Confianza y Seguridad Digital*. Departamento Nacional de Planeación.

Der Derian, J. (2009). *Virtuous war: Mapping the military-industrial-media-entertainment-network*. Routledge.

Feenberg, A. (2019). Postdigital or predigital?. *Postdigital Science and Education, 1*, 8-9.

Giral-Ramírez, W., Celedón-Flórez, H., Galvis-Restrepo, E., y Zona-Ortiz, A. (2017). *Redes inteligentes en el sistema eléctrico colombiano: Revisión de tema.* Tecnura, 21 (53), 119-137. ISSN: 0123-921X. https://www.redalyc.org/articulo.oa?id=257054721009

Guaqueta, F. (2015). *Dimensiones políticas y económicas de la seguridad en el Hemisfeio Latinoamericano: Relaciones Internacionales*. Nuevo Milenio.

Hannant, L. (2019). *Letter to the Editor: A Commentary on Patrizia Gentile's "Resisted Access? National Security, the Access to Information Act, and Queer(ing) Archives"*. Library and Archives Canada .

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

Hernández, A., & Fojón, E. (2016). Ciberseguros: la última línea de defensa. *Revista SIC: ciberseguridad, seguridad de la información y privacidad, 25*(120), 98-100.

Hernández, J. (2016). Infraestructura crítica cibernética (2016). Comando General de las Fuerzas Militares de Colombia.

Klimburg, A. (2020). Mixed Signals: A Flawed Approach to Cyber Deterrence. ***Survival***, ***62***(1), 107-130.

La Gaceta Caese. (2016). *Los ciberataques. Publicación de la Cámara de Comercio de Bogotá y Fundación País Libre No. 19*. Colombia. Rez Impresores.

Lind, M. (2017). Comprendiendo la importancia de la informacion de inteligencia "La guerra cibernetica" en Military Review. *Revista Politica.* Mexico DF.

López, O. (2019). *Caracterización de las organizaciones colombianas en la era de las nuevas tecnologías y sus controles. Un análisis documental*. En-Contexto *Revista de Investigación en Administración, Contabilidad, Economía y Sociedad*, 7 (11), 231-252. [Fecha de Consulta 03 de Abril de 2021]. ISSN: 2346-3279. https://www.redalyc.org/articulo.oa?id=551861265009

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Política Nacional De Confianza Y Seguridad Digital 3995 (2020). Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación*. Ministerio de Defensa Nacional. Dirección Nacional de Inteligencia. Departamento Nacional de Planeación.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020b). *Política nacional de confianza y seguridad digital 3701 (2011). Consejo nacional de política económica y social república de Colombia departamento nacional de planeación*. Ministerio de Defensa Nacional. Dirección Nacional de Inteligencia. Departamento Nacional de Planeación.

Ministerio del Interior y Seguridad Pública. (2018). *Estrategia Nacional de Ciberseguridad*. https://www.camara.cl/verDoc.aspx?prmID=176320&prmTIPO=DOCUMENTOCOMISION

Moreno, A. (2020). *Riesgos, avances y el camino a seguir en américa latina y el caribe (2020)*. Banco Interamericano de Desarrollo https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Naciones Unidas. (2018). *Resolución aprobada por la Asamblea General (2018) Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. Organización de las Naciones Unidas.

Nye, Jr., J. S., & Villanueva Rivas, C. (2017). El poder en el siglo XXI. Entrevista con Joseph S. Nye, Jr. *Revista Mexicana De Política Exterior*, (111), 165–179. https://revistadigital.sre.gob.mx/index.php/rmpe/article/view/318

Organización de los Estados Americanos. (2004). *Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*. Organización de los Estados Americanos OEA.

Parra, J. (2019). *Delitos informáticos y marco normativo en Colombia*. Universidad Nacional Abierta y a Distancia (UNAD).

Pollitt, M. (2019). *Economics and Policy of (Electrical) Energy Storage*. https://conferences.ncl.ac.uk/media/wwwnclacuk/engineering/Michael%20Pollitt.pdf

Quintero, Y. (2019). *La seguridad y Ciberdefensa en Colombia*. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00001596.pdf.

Real Academia Española. (2018). *Seguridad*. Real Academia Española.

Rodrigo, O. (2021). *Las acciones estatales contra el delito en Colombia*. Investigación realizada por solicitud de IKV Pax Christi.

Rojas, J. C. O. (2021). *Ciber seguridad de transacciones en sistemas de medición inteligente usando cadenas de bloques* (Doctoral dissertation, Instituto Tecnológico De Morelia).

Ruiz, S. (2018) *Protección de Datos y Seguridad Digital en Colombia Una propuesta sobre la necesidad de adhesión al Convenio de Budapest* (2001). Universidad de los Andes.

Salazar, P. G. (2019). *El libro blanco del hacker*. Ra-Ma Editorial.

Sánchez, L. (2017). *Por imperativo legal de las redes. Una vision desdes la perspectiva de la Ciberseguridad y la Ciberdefensa*. Murcia, España.

Sarmiento, J. (2016). La responsabilidad contractual por los riesgos previsibles, entre la autonomía de la voluntad privada y la rigurosidad de las normas de contratación pública. *Revista Derecho del Estado*, (37),189-211. https://www.redalyc.org/articulo.oa?id=337650446006

Serrano, A. X. O., Vaca, M. J. M., Rivadeneira, L. I. T., & Páez, C. F. (2019). Revisión sistemática del estado del arte de las Tecnologías de Información y Comunicación (TICS) y Seguridad Alimentaria. *Debates sobre innovación, 3*(2).

Universidad del Rosario. (2019). *Colombia no está preparada ante un ciberataque*. https://urosario.edu.co/static/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/index.html

Vargas, M. (2018). *Ciberseguridad y Ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* [Trabajo de Grado] Universidad Militar Nueva Granada.

Coyuntura

Defiances

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 93-98)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Riesgos cibernéticos para la aviación regular "el 11 de septiembre cibernético"

Cyber risks for regular aviation "cyber 9/11"

DOI: https://doi.org/10.25062/2955-0270.4775

Germán Darío Ramón Bonilla
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Durante los últimos años, en particular a partir de año 2020, se ha evidenciado un incremento considerable de ataques cibernéticos a la aviación, en particular a las aerolíneas, y en menor proporción a las entidades encargadas de liderar y controlar los servicios de tránsito aéreo o Civil Aviation Authorities (CAA). Tal como le sucedió a la Administración Federal de Aviación (FAA) que en un lapso menor a tres meses fue víctima de dos ataques a la disponibilidad de sus sistemas de información, afectaciones que colocan en evidencia que Estados Unidos a pesar de ser uno de los países con mayor madurez cibernética, aún presenta vulnerabilidades que se deben contrarrestar. Por tal motivo, este articulo explora los riesgos cibernéticos para la aviación regular.

Palabras Clave: Aviación; Riesgos cibernéticos; Seguridad

Abstract

During recent years, particularly since 2020, there has been a considerable increase in cyber attacks on aviation, particularly on airlines, and to a lesser extent on the entities in charge of leading and controlling air traffic services or Civil Aviation Authorities (CAA). Just as it happened to the Federal Aviation Administration (FAA), which in a period of less than three months was the victim of two attacks on the availability of its information systems, attacks that show that the United States, despite being one of the Countries with greater cyber maturity still present vulnerabilities that must be counteracted. For this reason, this article explores cyber risks for regular aviation.

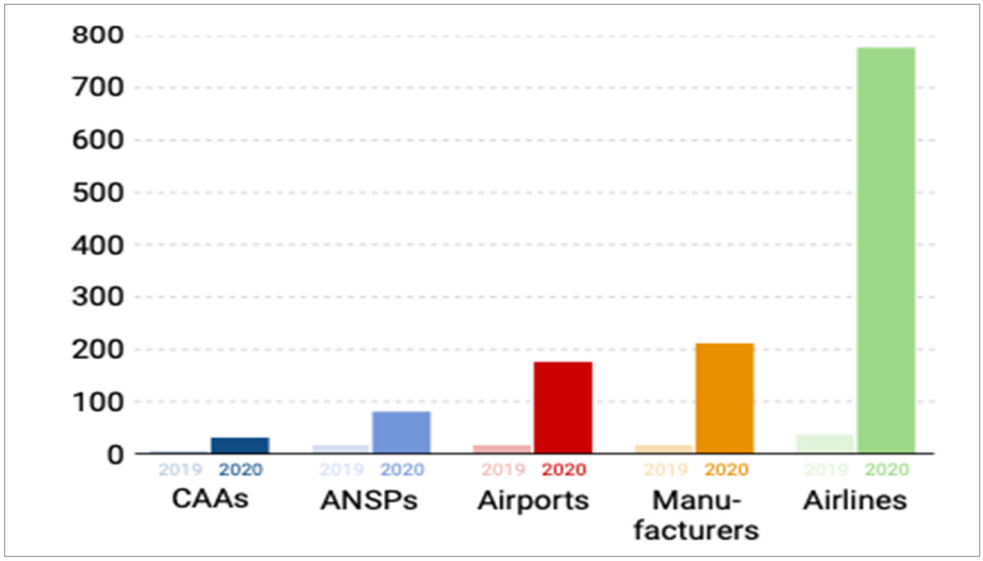
Key words: Aviation; Cyber risks; Security

Artículo de reflexión
Recibido: 23 de enero de 2022 • **Aceptado:** 14 de marzo de 2022
Contacto: Germán Darío Ramón Bonilla germanr@esdeg.edu.co

Introducción

Durante los últimos años, en particular a partir de año 2020, se ha evidenciado un incremento considerable de ataques cibernéticos a la aviación, en particular a las aerolíneas, y en menor proporción a las entidades encargadas de liderar y controlar los servicios de tránsito aéreo o Civil Aviation Athoroties (CAA), tal como le sucedió a la Administración Federal de Aviación (FAA[1],por sus siglas en inglés), una entidad norteamericana que en un lapso menor a tres meses fue víctima de dos ataques a la disponibilidad de sus sistemas de información, afectaciones que colocan en evidencia que Estados Unidos a pesar de ser uno de los países con mayor madurez cibernética, aún presenta vulnerabilidades que se deben contrarrestar.

Figura 1. Ciber Ataques Reportados en Aviación 2019 vs. 2020



Fuente: Elaboración propia a partir de EUROCONTROL EATM-CERT Services

Es importante reconocer que los aeropuertos, como infraestructura crítica de cualquier nación, son objetivos de alto valor estratégico para actores que buscan extorsionar, interrumpir o dañar la reputación de un estado; afectando directamente su economía, por supuesto, a las aerolíneas y a sus usuarios.

Con la aparición de nuevas tecnologías en aviación, sobre todo por la integración del Internet de las cosas (IoT) a sistemas de control y apoyo a la Gestión de Tránsito Aéreo (ATM), hay mayor probabilidad de sufrir ataques cibernéticos procedentes de actores que

1 FAA, Federal Aviation Administration

buscan las vulnerabilidades de la tecnología con la que operan ciertos aeropuertos, ocasionando pérdidas económicas reflejadas en retrasos, cancelaciones de vuelos e incluso llegando afectar la seguridad operacional.

La Agencia Europea de Seguridad Aérea (EASA[2] por sus siglas en inglés) afirma que la cantidad de ataques a los sistemas de información al servicio de la aviación crecerá de manera exponencial por el aumento de aplicaciones, dispositivos tecnológicos y el uso del internet de las cosas (IoT[3] por sus siglas en inglés) en la industria aeronáutica.

Si bien los ataques y fallas de software pueden causar retrasos, cancelaciones y restricciones de acceso a la información; las autoridades de aviación civil (CAA) como entes reguladores tienen la responsabilidad de identificar las nuevas amenazas y adoptar estrategias para mejorar la resiliencia cibernética: "capacidad de una organización para prevenir, resistir y recuperarse de incidentes de ciberseguridad" (IBM, 2020, párrafo 3).

A pesar de que los ataques de denegación de acceso a la información, DDoS, son considerados complejidad media y baja criticidad, la aplicación de estos a sistemas de información aeronáutica para el desarrollo de vuelos, genera un efecto cascada con afectaciones significativas al normal desarrollo de las operaciones aéreas, dos casos recientes de afectación por denegación de acceso a los servicios de información aeronáutica en Estados Unidos, serán expuestos con el propósito de dilucidar la magnitud de un ataque cibernético a los sistemas de información aeronáutica:

El pasado 11 de enero de 2023, a las 07:20 horas, la FAA debió ordenar a todas las aerolíneas estadounidenses pausar las salidas de sus vuelos nacionales mientras restauraban la base de datos del sistema de aviso de información de vuelo (NOTAMs[4] por sus siglas en inglés); información obligatoria para consulta de pilotos y despachadores, previo al desarrollo del vuelo.

La responsabilidad de esta interrupción aún es materia de investigación, no obstante, se indicó por la FAA que esta base de datos fue afectada por un archivo dañado, según lo manifestó comunicado de la misma organización por medio de Twitter.

Esta interrupción del servicio de información generó que, sobre el medio día, se cancelaran 1.100 vuelos y se retrasaran otros 7.300. El secretario de transporte de los estados Unidos, Pete Buttigieg, indicó el mismo día que la FAA identificará las causas para evitar que esto vuelva a suceder, por tratarse de una situación similar a la ocurrida el pasado 10 de octubre de 2022, en la que los sitios web de cinco aeropuertos estadounidenses se vieran afectados por un ataque de denegación de distribución de servicio

2 EASA, European Aviation Safety Agency

3 IoT, Internet of Things

4 NOTAMs, Notice for Air Missions

de información (DDoS[5] por sus siglas en inglés) a pasajeros; hechos atribuidos al grupo Pro-Ruso *Killnet*.

Si bien el evento más reciente se encuentra en investigación, es de notar que las afectaciones han sido progresivas en términos de contundencia y acercamiento a los sistemas operativos de información aeronáutica, situación que aumenta la preocupación por parte de las autoridades estadounidenses, por la incertidumbre de no saber cuál será el próximo ataque a enfrentar (Mundo Posgrado, 2021).

Respecto el evento del 10 de octubre de 2022, a pesar de no haber afectado de manera considerable el cumplimiento de los vuelos programados, es un ejemplo de ataque trascendental, utilizando el concepto de operaciones de zona gris (Hoffman et al., 2007, como se citó en Dziwisz, 2020), se hacen importante considerar acciones defensivas y ofensivas en el desarrollo de las operaciones cibernéticas, lo cual puede emplear tácticas convencionales. La misma Dziwisz (2020) argumenta que:

> La zona gris es cada vez más poblada, porque países como China o Rusia utilizan cada vez más herramientas cibernéticas y no cibernéticas para superar las fortalezas de EE. UU. en diplomacia, leyes y comercio global. No sorprende que esta nueva competencia de zona gris sea dura e inquietante para Estados Unidos (Dziwisz, 2020, p. 23).

Es así como los riesgos cibernéticos para los sistemas de apoyo a la aviación regular, podrán ser potencializados debido al desconocimiento de las vulnerabilidades de los sistemas del apoyo a la aviación, aumentando la probabilidad de materialización de ataques exitosos que buscan afectar la confidencialidad, disponibilidad e integridad de los sistemas de apoyo a la Gestión de Tránsito Aéreo, siendo esta la joya de la corona, por afectar a la seguridad operacional.

Expertos en ciberseguridad para la aviación, han identificado cuatro propósitos a lograr con el empleo efectivo de amenazas cibernéticas para la aviación: "el espionaje comercial, la ciberdelincuencia, la interrupción y los fines Político-Militares" (Safe Skies, 2018, párrafo), el último propósito coincidente con lo sucedido el pasado 10 de octubre de 2022 en EE.UU.

De igual manera, se ha identificado que las Amenazas Persistentes Avanzadas (APT[6] por sus siglas en inglés); son ejecutadas la principal amenaza para la aviación, ya que son desarrolladas por organismos militares o entidades de inteligencia extranjeras que buscan obtener alguna ventaja militar, política o estratégica trasnacional, mediante "Un conjunto de tácticas, técnicas y procedimientos que hacen compleja la detección de una intrusión cibernética en varios sistemas informáticos" (Parra, 2019, p. 32).

5 DDoS, Distributed Denial of Service

6 APT, Advanced Persistent Threat

Con mayor preocupación se debe considerar que amenazas emergentes seguirán en desarrollo; más aún cuando el avance de la tecnología y la modernización de aeropuertos y de aeronaves es proporcional a nuevas variables, la afectación podría pasar de eventos en tierra a situaciones en vuelo; como por ejemplo la manipulación de la señal satelital utilizada por las aeronaves para navegar y reportar posición a otras aeronaves y al ATC[7] siendo esta una preocupación reciente de la OACI[8] por el lanzamiento de la tecnología celular 5G, con recientes investigaciones por su incidencia con los sistemas de navegación de las aeronaves, (Federal Aviation Administration, 2023), situación que podría llegar a cambiar el concepto de secuestro físico de un avión, vulnerabilidad manifestada por Munro (2020):

> Estás conectando un avión que tradicionalmente no ha estado tan bien conectado y gran parte de la conectividad está empezando a romper muchos de los modelos de seguridad tradicionales que tenemos en torno al hecho de que el hacker puede saltar a una bahía de aviónica y empezar a jugar con un avión. (p. 16).

Podríamos listar muchas más amenazas, no obstante, lo importante es reconocer que ningún sector está lo suficientemente preparado para contrarrestarlas, siempre habrá algo más por hacer, pues cada paso que da la tecnología es una puerta que se abre a las amenazas cibernéticas; de esta manera es de reconocer que no se trata solo de adaptarnos a nuevas tecnologías, es también conocer su alcance.

Conclusiones

A pesar de que el sector aeronáutico está utilizando cada vez más tecnologías para mejorar las operaciones y los servicios que proporcionan a sus usuarios, hay un gran desafío en detectar cuáles son las ventajas y desventajas de estas tecnologías.

De igual manera, es apremiante recalcar a los entes reguladores de aviación, la importancia de diferenciar las redes de información (IT[9]) y (OT[10]), ya que, por practicidad y economía, algunas autoridades aeronáuticas y aerolíneas combinan sus portales operacionales, con temas administrativos e informativos de acceso público, siendo más vulnerables a que un solo ataque afecte ambos sistemas.

Finalmente, con urgencia se debe prestar atención a la interferencia de la tecnología celular 5G con los sistemas de navegación de las aeronaves, pues no existe manera de detectar si una perturbación a una señal satelital sea identificable oportunamente, sobre

7 ATC. Air Traffic Control

8 OACI, Organización de Aviación Civil Internacional

9 IT, Information Technology

10 OT, Operation Technology

todo en las fases cercanas al terreno (despegue y aterrizaje), y así evitar que se repita un 11 de septiembre, cibernético, mediante alteración, inserción e inhibición de señales a los sistemas de navegación a bordo de las aeronaves.

Declaración de divulgación

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

Autor

Germán Darío Ramón Bonilla. Mayor de la Fuerza Aérea Colombiana. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Administración Aeronáutica, Escuela Militar de Aviación "Marco Fidel Suarez", Colombia.

ORCID: https://orcid.org/0009-0000-8444-9187
Contacto: germanr@esdeg.edu.co

Referencias

Dziwisz, D. (2022). "Cyber Pearl Harbor Is Not Coming: US Politics Between War and Peace". *Politeja* 19 (4), 95-109. https://doi.org/10.12797/Politeja.19.2022.79.07.

Federal Aviation Administration. (2023). *FAA. 5G and Aviation Safety.* https://www.faa.gov/5g

IBM. (2020). *IBM.COM. ¿Qué es la resiliencia cibernética?* https://www.ibm.com/co-es/topics/cyber-resilience

Munro, K. (23 de Abril de 2020). *Airport-Technology. Roundtable: Are airports prepared for cyber threats?* https://www.airport-technology.com/features/cybersecurity-in-airports/

Mundo Posgrado. (2021). *Estos son los 7 tipos de amenazas cibernéticas más frecuentes*. https://www.mundoposgrado.com/amenazas-ciberneticas-mas-frecuentes/

Parra, J. (2019). *Amenazas persistentes avanzadas y su impacto en Latinoamérica ¿cómo estar preparados?* [Trabajo de grado]. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6285/00005219.pdf?sequence=1&isAllowed=y

Safe Skies. (2018). *Sskies.org. PARAS -Program for Applied Research in Airport Security* https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf

Perspectivas

Perspectives

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 1, enero-junio 2022 (pp. 101-104)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia

Interview with Marco Emilio Sánchez Acevedo. Cybersecurity in Colombia

DOI: https://doi.org/10.25062/2955-0270.4782

Mónica Lissette Flórez Cáceres
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Biografía

Doctor en Tecnologías y Servicios de la Sociedad de la Información – Derecho y TIC de la Universitat de València, España. Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Especialista en Derecho Administrativo y Constitucional de la Universidad Católica de Colombia. Abogado de la Universidad Central, Colombia. Docente de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Entrevista
Recibido: 2 de febrero de 2022 • **Aceptado:** 20 de mayo de 2022
Contacto: Mónica Lissette Flórez Cáceres monica.florez@esdeg.edu.co

Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia

¿Cuál es el rumbo de la ciberseguridad para en el país?

Colombia hace parte de un entorno tanto regional como mundial en el marco de las garantías para el derecho a la seguridad digital de sus ciudadanos, y bajo esa órbita, el país ha trazado una hoja de ruta desde hace más de 10 años en torno a la seguridad digital, y al fortalecimiento de las capacidades de ciberdefensa. Mencionada hoja de ruta inició con el establecimiento de una institucionalidad, que pasa precisamente por el Centro de Respuestas a Emergencias Cibernéticas de Colombia, el Centro Cibernético de la Policía, el Comando Conjunto de Operaciones Cibernéticas, los Centros de Respuestas a Emergencias Cibernéticas de cada uno de los sectores que se identifiquen como críticos para el país, y por supuesto, de la Fiscalía General de la Nación a través de las unidades de investigación de delitos informáticos.

Luego de ello, se avanzó en la construcción de un plan para gestionar los riesgos de seguridad digital, siendo un proceso que se ha venido dando durante varios años consolidando a su paso una institucionalidad desde la gobernanza de la seguridad digital, y ahí es cuando en el año 2022 aparece lo que significa el papel del Director Nacional de Seguridad Digital y el papel del Comité Nacional de Seguridad Digital del que hacen parte más de 20 entidades nacionales con distintos actores, con lo que se trató inicialmente, de reiterada institucionalidad es el fortalecimiento de las capacidades de gestión de riesgos y gestión de incidentes que sin duda ha venido en constante maduración.

Finalmente, el futuro no puede ser otro que fortalecer cada una de esas capacidades que se han desarrollado en el proceso desde hace bastantes años. No puede ser otro que el de enfrentar los desafíos que genera el uso de tecnologías de manera masiva a partir del uso de tecnologías emergentes, y así mismo, a partir de la construcción de ciudades y territorios inteligentes. De igual modo, el establecimiento de todas las actividades sociales por medios electrónicos: el comercio electrónico, la educación digital, la justicia digital, la salud digital, entre otros. Es decir, fortalecimiento de las capacidades para hacer frente a los desafíos que genera usar tecnologías en todos los sectores sociales y económicos del país.

Desde su experiencia profesional y académica, ¿cuáles considera que son los retos en torno a la regulación normativa para la ciberseguridad a nivel nacional?

Son bastantes. En esencia, las normas son de distinta naturaleza: normas internacionales, nacionales, y dentro de estas, leyes de la República, decretos reglamentarios

y actos administrativos que incorporen lineamientos y estándares, eso quiere decir que los retos son todos en todos estos frentes.

Primero, en lo que corresponde al frente internacional, la aplicación y materialización del Convenio de Budapest sigue siendo un instrumento normativo supranacional que permite combatir los delitos informáticos de manera articulada y colaborativa con los distintos actores de diversos Estados. Segundo, en los retos nacionales se ubica la necesidad de una ley de seguridad digital, particularmente para involucrar al sector privado en obligaciones de seguridad y defensa del Estado, dado que, muchísimas infraestructuras críticas y servicios esenciales son hoy en día administrados y gestionados por este sector, y ellos, sin duda, deben involucrarse desde la protección de las infraestructuras y servicios esenciales que están en sus manos.

De igual manera, en la legislación nacional es necesaria la identificación de infraestructuras críticas, entendiendo que no se puede proteger lo que no se conoce, y en consecuencia, se deben delimitar cuáles son los sectores y subsectores que están conectados a las tecnologías de la información y las comunicaciones, pues se convierten en sectores y servicios críticos que hay que proteger desde la seguridad y la defensa para el mantenimiento del orden constitucional, legal y lógicamente de la garantía de los derechos ciudadanos.

Por otra parte, en los instrumentos normativos de menor nivel existentes varios retos muy importantes porque la seguridad y defensa nacional pasa por diversos estándares y estos tienen que estar condicionados tanto para el sector público como para el sector privado, a partir de regulaciones homogéneas en torno a la gestión de los riesgos que genera el uso de tecnologías, pero al mismo tiempo la gestión de los incidentes. Partiendo de esto, mencionados lineamientos permitirán entender ¿qué hacer de manera colaborativa para enfrentar un ataque cibernético de gran escala? ¿Cómo incorporan los actores públicos y privados los estándares técnicos que permiten hacer frente a las emergencias cibernéticas?

Con todo lo anterior, y ante la inclusión de más sectores y actores económicos o del sector empresarial que se están conectando a tecnologías de manera masiva, se genera la necesidad de establecer unos estándares o lineamientos técnicos muy importantes para garantizar la seguridad digital.

Con ocasión a la actual situación y los retos evidenciados, ¿cuál considera usted que es la herramienta oportuna para mitigar a largo plazo las visicitudes que diaramente proliferan en torno a la ciberseguridad?

Desde mi criterio, la formación se convierte en un elemento fundamental para la construcción de capacidades a todo nivel. Esto quiere decir que el uso de la tecnología no responde a una moda, sino que aborda todo un modelo de desarrollo

planteado para la sociedad del siglo XXI, obligándo entonces a adquirir fortalezas y capacidades desde la formación de la ciudadanía y del personal militar.

Específicamente, programas como la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto"es una de las maestrías líderes, quizás la primera en Latinoamérica que abandera ese proceso de formación para personal del nivel estratégico, del nivel táctico y del nivel operativo, mismo que va a ser requerido por actores públicos y privados para el cumplimiento de las obligaciones derivadas de la seguridad y defensa nacional, así como de la protección de los derechos de los ciudadanos en el ciberespacio. En este sentido, contar con programas actualizados funge como respuesta a las necesidades de adquirir capacidades con los expertos referentes, posibilitando una formación especializada de más alto nivel.

Autora de la entrevista

Mónica Lissette Flórez Cáceres. Magister en Acción Política y fortalecimiento institucional de la Universidad Francisco de Vitoria, España. Especialista en Comercio Internacional y Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada, Colombia. Docente de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

ORCID: https://orcid.org/0000-0003-4777-2481
Contacto: monica.florez@esdeg.edu.co

Enfoques

Insights

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 1, enero-junio 2022 (pp. 107-109)
Bogotá, D.C, Colombia

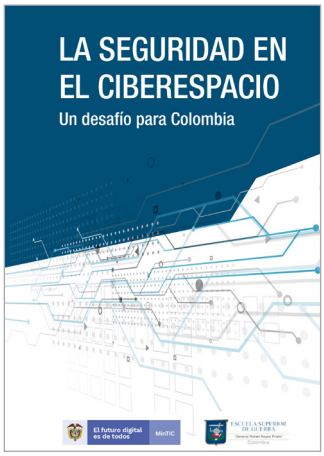
EDITORIAL **ESDEG**

Reseña de libro. La seguridad en el ciberespacio: Un desafío para Colombia

Book review. Security in cyberspace: A challenge for Colombia

DOI: https://doi.org/10.25062/2955-0270.4780

Henry Andrés Buchheim Duarte
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia



Editores del libro: **Jairo Andrés Becerra, Marco Emilio Sánchez Acevedo, Carlos Castañeda M., Alejandro Bohórquez Keeney, Rafael Vicente Páez Méndez, Arístides Baldomero Contreras, Ivonne Patricia León**
Editorial: Editorial Planeta Colombiana S.A.
Año: 2020
ISBN impreso: 978-958-42-8892-9
Páginas: 222

El propósito del libro es concientizar al lector acerca de la importancia que reviste para las organizaciones desde el ámbito académico, militar, empresarial y público, el uso adecuado del ciberespacio y la responsabilidad que tiene el Estado de preservar sus intereses y proteger la infraestructura de los nuevos riesgos que se vislumbran en el campo de la ciberseguridad y la ciberdefensa.

El libro, en una introducción hace acápite a la seguridad en el ciberespacio como un desafío para Colombia, expresa en los cinco (5) capítulos siguientes, donde se abarcan temas relacionados con la resiliencia, la investigación como eje fundamental de una política de seguridad digital en Colombia; así mismo, exponen la relevancia de la gestión de riesgos en el entorno de la Fuerza Pública y en el Sector Privado.

Entre los temas tratados, se plantea la dependencia de los flujos seguros de información para el correcto funcionamiento de las organizaciones empresariales y la operación del gobierno. De igual forma, la importancia que reviste la información y como los ataques cibernéticos se perciben como una amenaza de seguridad nacional e internacional, haciendo que los Estados manifiesten la necesidad de proteger sus redes de información, en especial las de seguridad nacional y las infraestructuras críticas.

Es así, como las sociedades están experimentando una transformación digital, basada en un mundo más interconectado, con nuevas tecnologías y, por consiguiente, nuevos riesgos que requieren la evolución de la política pública colombiana y mecanismos de cooperación en materia de delitos cibernéticos entre países. El autor define conceptos básicos como resiliencia, ciberseguridad, gestión de riesgos y como se relacionan entre ellos.

El primer capítulo hace un ejercicio académico enfocado a describir de forma detallada y clara el contexto del CONPES 3854 de 2016 entendido como una política base de seguridad digital colombiana, de esta manera disgregan las cinco dimensiones estratégicas sobre las que se adopta el enfoque de seguridad digital. Así mismo, se hace una adecuada conceptualización mediante diferentes referentes bibliográficos acerca de conceptos relevantes como ciberespacio, ciberdefensa, seguridad digital, ciberdefensa. De igual forma, el autor introduce los conceptos de las diferentes organizaciones que tienen responsabilidad de gestionar la seguridad y defensa a nivel cibernético en el país.

El segundo capítulo presenta una conceptualización general, buscando evidenciar las diferentes problemáticas que enfrenta la sociedad en el marco de la cuarta revolución industrial y como las nuevas tecnologías han generado una transformación en las actividades diarias y disminución en el tiempo para hacer las cosas, que se traduce en la reducción de costos y respuestas ágiles que generan transparencia y acceso oportuno a la información. Dentro de esta modernización aparece como eje fundamental el internet, siendo el actor principal en la globalización, ya que es el articulador en las comunicaciones e interacción digital entre personas y objetos.

Según indica el autor, la globalización y las nuevas tecnologías han hecho que los Estados se vean limitados por nuevas instituciones o actores no estatales, cuyo carácter dinámico no logra ser regulado por marcos judiciales nacionales. Por último, se describe y diferencian los conceptos de *Hacktivista, Hacker* y *Cracker,* lo cual se hace una contextualización de cómo gestionar los riesgos a nivel global y nacional con base a las nuevas amenazas, producto del carácter dinámico de las tecnologías y su acelerado ritmo de cambio.

El tercer capítulo definen los alcances académicos frente a la seguridad digital, de igual forma se realiza una interesante revisión bibliográfica, incluyendo dentro de estas,

las principales políticas públicas en materia de ciberseguridad de los actores regionales y de Estados Unidos, Israel, Estonia y Corea del Sur, lo anterior con el propósito de revisar cómo se ha llevado a cabo la ejecución de las políticas públicas en seguridad digital y la importancia de la academia en este entorno. De forma general, se abre un abanico de posibilidades para que desde la academia se genere conciencia y regulación en torno al ciberespacio. Finalmente, se ejecuta un paneo respecto al papel del sector académico en cuanto a la proyección a futuro en el área de ciberseguridad y las amenazas que se vislumbran.

El cuarto capítulo se observa cómo el autor hizo una exhaustiva comprobación de la estrategia de gestión de riesgos en seguridad digital de países europeos, así como de Estados Unidos y Canadá, con el fin de dar a conocer de una forma sucinta los avances en el tema. De igual manera, indica cómo Colombia ha avanzado para hacer frente a las amenazas latentes en el ciberespacio, generando como conclusión la importancia de involucrar a todos los actores a nivel gobierno para implementar políticas y procedimientos en la gestión de riesgos en materia de seguridad digital.

El quinto capítulo se enfoca en dar a conocer estadísticamente cómo los riesgos para la ciberseguridad han aumentado en prevalencia y potencial desestabilizador en las grandes empresas del sector público y privado. En esta investigación, el autor hace una recopilación hasta el año 2018 de las acciones adelantadas por los países latinoamericanos en relación con la implementación de políticas de seguridad digital, haciendo la claridad que se requieren mayores esfuerzos en ciberseguridad, esto en relación con que cada cuatro de cinco países carecen de estrategia de ciberseguridad.

En conclusión, el libro es una ayuda para conocer la importancia por parte de cada uno de los sectores sobre medir y mitigar los riesgos digitales, así como la necesidad de una mayor integración entre la ciberseguridad y modelos de desarrollo de resiliencia, partiendo de la premisa de que ningún sistema es cien por ciento seguro y para esto es necesario comprender la amplia gama de vectores de amenazas cibernéticas, generar conciencia y sensibilización en todos los niveles bajo el liderazgo del sector académico, que permita generar conocimiento en torno al tema.

Autor de la reseña

Henry Andrés Buchheim Duarte. Capitán de Corbeta de la Armada Nacional de Colombia. Especialista en Política y Estrategia Marítima, Escuela Naval del Cadetes "Almirante Padilla", Colombia. Ingeniero Electrónico, Escuela Naval del Cadetes "Almirante Padilla", Colombia.

ORCID: https://orcid.org/0009-0005-9784-9039

Contacto: henry.buchheim@armada.mil.co


EDITORIAL ESDEG

Revista **Ciberespacio, Tecnología e Innovación**

EDITORIAL **ESDEG**

ISNN 2955-0270

9 772955 027005