EDITORIAL ESDEG

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

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

Martin Fernando Rincón Gallón

CITACIÓN APA:

Rincón Gallón, M. F. (2022). Los factores armados de inestabilidad frente a la ciberseguridad y la ciberdefensa nacional. *Ciberespacio, Tecnología e Innovación, 1*(1), 7-40. https://doi.org/10.25062/2955-0270.4768

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

Enviar un artículo a la Revista

Check for updates

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.