Capítulo 4

Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance del cibercrimen en Colombia y la región*

DOI: https://doi.org/10.25062/9786287602120.04

Gabriel Andrés Jiménez Almeira
María Paula Morales Lince
Israel Patiño Sánchez
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El objetivo de este capítulo de libro es identificar los métodos y estrategias que se emplean como anticipación al avance de los delitos de origen ciberespacial, en los que prosperan las economías ilícitas, las conductas típicas transnacionales y la globalización desviada en general. Con este fin, se utiliza un método de investigación cualitativo que, desde el análisis de diversas fuentes primarias y secundarias establece las herramientas precisas por las que se pretende prevenir la actividad delictiva, como lo es el caso de la cooperación internacional, la cual permite, a través de conversaciones y la generación de estrategias conjuntas la solidificación de barreras de protección, conectadas desde la ciberseguridad y la ciberdefensa. En conclusión, la implementación de estrategias de alcance tanto nacional como internacional construyen oportunidades de respuesta temprana que mitigan las amenazas a la seguridad de los Estados y de sus coasociados, siempre y cuando estas estimen el contexto, la inmediatez y las necesidades particulares.

Palabras clave: Amenazas; cibercrimen; ciberdefensa; ciberseguridad; globalización.

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

Gabriel Andrés Jiménez Almeira
Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra. Internacionalista, Universidad del Rosario. https://orcid.org/0000-0003-4867-0073 - Contacto: jimenezg@esdeg.edu.co

María Paula Morales Lince
Internacionalista, Universidad del Rosario. https://orcid.org/0000-0002-9173-1049 - Contacto: maria.morales@esdeg.edu.co

Israel Patiño Sánchez
Teniente coronel del Ejército Nacional de Colombia. Magíster en Derechos Humanos y DICA, y Especialista en Seguridad y Defensa Nacionales, Escuela Superior de Guerra. https://orcid.org/0000-0001-6726-2433 - Contacto: israel.patino@esdeg.edu.co

Citación APA: Jiménez Almeira, G. A. Morales Lince, M. P. & Patiño Sánchez, I. (2022). Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance del cibercrimen en Colombia y la región. En P. A. Sierra-Zamora, T. L. Fonseca-Ortiz, & F. Coronado-Camero (Eds.), *De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales* (pp. 137-155). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602120.04

De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales
ISBN impreso: 978-628-7602-11-3
ISBN digital: 978-628-7602-12-0
DOI: https://doi.org/10.25062/9786287602120
Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2022

Introducción

En los últimos años, la ciberdefensa ha pasado de ser una parte ignorada del planeamiento de seguridad en muchos países a uno de los temas de mayor relevancia en la agenda internacional. La revolución tecnológica ha ocasionado que las formas en que los actores del sistema internacional toman decisiones y se comunican entre ellos cambie rápidamente; por esto, Cano (2011) menciona que "las amenazas que en el pasado se encontraban recluidas en una punta del mundo, ahora pueden llegar a la otra por medio de tecnologías".

Por tal razón, la globalización (desviada) ha traído como resultado el aumento de las economías ilícitas, lo que ha afectado a los Estados por la falta de controles; sobre todo, en países en desarrollo, los cuales se han involucrado en una categoría del cibercrimen, como lo son los paraísos fiscales en los que la utilización de *money donkeys* (presentada en su mayoría a través del ciberespacio) beneficia y, en varios casos, financia grupos armados organizados y delincuenciales (acción que se cataloga como un ciberdelito).

Sin embargo, en diferentes regiones del mundo se han venido creando estrategias para detener el alcance del cibercrimen dentro de sus fronteras soberanas en las cuales se evidencia una distinción entre los países del norte y del sur global. Los primeros parecen haber sido más eficientes en la creación de estrategias y dinámicas para enfrentar esta nueva amenaza; los segundos, ya sea por falta de presupuesto o por no verlo tan claramente como un posible objetivo (o amenaza nacional), han llevado este proceso con mayor lentitud y han creado políticas de manera paulatina tras identificar tan solo algunos de los sectores vulnerables frente a esta nueva forma de hacer crimen. La diferenciación entre estas dos zonas, y las dinámicas de cooperación que pueden haberse dado en los últimos años, son importantes para identificar los métodos y procedimientos

que permiten posicionar a países como Colombia de modo más seguro en el conjunto de naciones que se encuentran preparadas para sobrellevar la evolución tecnológica del aspecto criminal global.

El presente capítulo de libro tiene un enfoque cualitativo, con un diseño basado en investigación documentada, cuya técnica de recolección de datos se basa en fuentes primarias y secundarias. La técnica de análisis de información se da a partir de la teoría fundamentada y de un análisis axial de variables independientes y dependientes de la ciberdefensa y del cibercrimen. Así mismo, postula una correlación de variables que permiten identificar las acciones para la construcción de una estrategia de anticipación al aumento del ciberdelito, razón por la cual el texto expresa la importancia de estudios prospectivos de defensa y seguridad que busquen anticiparse a los delitos (del ciberespacio) y que permitan apoyar y fortalecer las políticas públicas que pretenden contrarrestar esta amenaza a la seguridad.

Ciberseguridad: del contexto regional al caso colombiano

Los métodos en los que se ha utilizado el espacio cibernético alrededor del mundo y la manera en la que en este se cometen diferentes tipos de crímenes que afectan a las personas de todos los rincones del mundo, lo ha llevado a ser catalogado en agendas regionales como un factor de amenaza a la seguridad nacional y humana. En consecuencia, el rol de las organizaciones internacionales dentro del sistema internacional se ha vuelto determinante; por ejemplo, la Interpol (2020), una organización internacional que ayuda a "conectar a los cuerpos policiales de diferentes países del mundo para promover la cooperación y permitir que crímenes que traspasen fronteras puedan ser solucionados más rápidamente" ha sido clave para poder contener el avance delictivo de los grupos transnacionales que utilizan el cibercrimen y el ciberdelito.

En los últimos años, con el desarrollo del ciberespacio (Paya-Santos & Luque, 2021) y la evolución de las dinámicas criminales, esta organización ha ayudado, a nivel mundial, a la adaptación de las fuerzas policiacas y la resolución de estos crímenes. Según la Interpol (2020), "los cibercrímenes más comunes mundialmente parecen estar ligados a beneficios económicos, con robo de identidad, sitios falsos y *hackeo* ocupando los primeros puestos". Debido a la presencia

de los grandes países precursores de la ciberseguridad, la forma en la que esta institución trabaja contribuye a ayudar al delineamiento de leyes en los países más pequeños que forman parte de esta.

Muchos de estos crímenes son ejecutados entre un país y otro, ya que los criminales tienden a confiar en estos métodos de distanciamiento para hacer que las autoridades pierdan el rastro al momento de investigar el crimen; no obstante, la cooperación internacional permite encontrar y seguir tanto el rastro como los patrones de estos crímenes. Aun así, la forma en la que cada país busca defenderse puede influir en la condena de los criminales y en la cantidad de este tipo de crímenes en su territorio.

Al haber sido identificada como atractiva para los ataques cibernéticos que se han popularizado en todo el mundo, la región latinoamericana se ha visto obligada a desarrollar rápidamente políticas de seguridad y defensa para contrarrestar esta nueva ola del crimen (Lavinder, 2018). De este modo, la cooperación con países más experimentados en este *issue* ha permitido que países de esta región logren aprobar con mayor eficiencia legislaciones contra el cibercrimen.

En la actualidad, el país de esta zona que ha sido considerado como el mejor preparado en temas de ciberdefensa es Brasil. Esto no se ha debido únicamente a su deseo de establecerse como un líder regional, sino porque se encuentra en tercer lugar (en cuanto a ataques cibernéticos en el mundo), como ha quedado consignado en múltiples estudios en ciberseguridad, como el de Abdenur (2014); en su mayoría, estos ataques han estado dirigidos hacia sitios gubernamentales con el objetivo de dejarlos en blanco o reemplazar su contenido con información diferente. Adicionalmente, el incremento de la población que tiene acceso a internet obligó al gobierno brasileño a establecer leyes y plantear múltiples estrategias para protegerse de los ataques cibernéticos que comenzaban a llegar.

La estrategia de ciberseguridad y ciberdefensa brasileña es descentralizada, con el objetivo de concentrarse más en el tema conceptual y las diferencias entre la ciberseguridad, la represión, la prevención y la ciberdefensa (acciones en combates ofensivos). Aun así, no existe una organización específica que se enfoque en la evolución de la seguridad cibernética. Por el momento, varias oficinas bajo el Ministerio de Defensa están realizando estudios y creando estrategias para ampliar el marco institucional frente a esta nueva forma de seguridad; al respecto, Lobato (2017) afirma que "ha sido posicionada junto con los sectores aeroespaciales y nucleares como los más importantes para el desarrollo

estratégico a futuro del país debido a la importancia que le están dando otros actores en el sistema internacional".

El caso de México, como vecino de Estados Unidos, es especialmente interesante, ya que la cercanía geográfica con el gigante americano hace que sea altamente atractivo al momento de someterlo a crímenes cibernéticos y de utilizar servidores en su territorio para cometer crímenes en los Estados Unidos. El enfoque de ciberseguridad y ciberdefensa de México está concentrado en identificar a los actores de estas nuevas actividades ilegales y las formas en las que se puede trabajar para debilitar y detener algunos de los crímenes que tienen lugar en el ciberespacio. También se tiene una definición específica de las situaciones que son consideradas como cibercrímenes y de "los que entran en la legislación de ciberseguridad versus los que son identificados como seguridad de la información" (OEA, 2017).

Los ataques más comunes en este país tienden a tener un trasfondo económico que, en ocasiones, abarca aspectos políticos, como la desinformación (que se ha popularizado a través del mundo como las *fake news* o los *bolos*). El gobierno mexicano tiene una estrategia para identificar a los actores y a su forma de actuar, de modo que se pueda establecer qué acciones ilegales son realizadas por cada actor y, a su vez, separar los objetivos políticos o económicos por los que suelen ser conocidos estos actores. Lo anterior, sumado a la separación de la gravedad de los crímenes, permite que las acciones sean más efectivas y que las víctimas de los cibercrímenes tengan más claro qué acciones llevar a cabo para protegerse y la forma en la que pueden hallar una solución.

En el caso de Argentina, su implementación de leyes para la protección contra los crímenes cibernéticos comenzó tras un informe de la UNASUR acerca de la importancia de tomar medidas al respecto (en lo cual los gobiernos de este país y de Brasil se volvieron precursores). Aun cuando la ciberdefensa (Cujabante et al., 2020) ha sido una herramienta complicada de aplicar, debido a su complejidad, flexibilidad de interpretación y debate continuo, el gobierno argentino la incluyó en la tradición institucional de su sistema de defensa, dentro del cual la cooperación interestatal y la cooperación entre la seguridad y defensa estatal propia permite incrementar la capacidad para contrarrestar esta clase de amenazas.

Es importante tener en cuenta que para que un ataque entre en el marco de la ciberdefensa debe ser llevado a cabo por un actor estatal y que su magnitud sea suficiente para afectar la soberanía, la integridad territorial y la independencia;

por lo cual, como dice Cornaglia (2017), "pequeños cibercrímenes que son incluidos en la legislación de ciberseguridad en otros países de la región no tienen una legislación clara en Argentina". Lo anterior puede hacer que los civiles, que tienen acceso al internet de ese país, se vean expuestos a múltiples ataques cibernéticos de objetivo financiero y económico frente a los que pueden no tener la suficiente protección.

En contraste, Chile mantiene una visión más a futuro (o prospectiva) que otros países de la región, dado que utiliza planificaciones a largo plazo. Para ese país, el ciberespacio es un ambiente nuevo en el que se desenvuelven nacionales e internacionales y en el cual los sectores público, administrativo y financiero son los que se ven más afectados, y los que, a su vez, cuentan con la habilidad de afectar la soberanía, estabilidad y seguridad nacional. La mayoría de los crímenes cibernéticos que ocurren allí tienen como blanco estructuras financieras y suelen tener un objetivo económico. Por lo tanto, el propósito principal de la política chilena frente a la ciberseguridad y la ciberdefensa es "lograr que el ciberespacio sea un lugar libre, abierto, seguro y resiliente para cada nacional chileno que tenga acceso a este" (Gobierno de Chile, 2016).

En tal sentido, mediante algunos lineamientos específicos, Chile permite que las instituciones del Estado evolucionen de manera que se pueda concretar una estructura de información para lograr tener una gestión de riesgo efectiva al momento de que un ataque de gran magnitud debilite las estructuras cibernéticas más importantes del país. De modo similar, crea una estructura bajo la cual todos los nacionales que se encuentren en el entorno cibernético sean educados sobre la forma en la cual funciona la comunidad de internet (junto con los riesgos que esta posee) y se asegura de que disfruten de ciertos derechos que son protegidos por el gobierno chileno. Esto se hace más efectivo a través de la cooperación con otros países de la región para crear estructuras eficaces y tener más claro cuáles son las amenazas a las que se enfrenta el país.

Mientras tanto, la ciberseguridad de Perú se concentra en proteger la estructura institucional cibernética del Estado, como la infraestructura de la información y la tecnología que se utiliza para acceder a esta. Se toma en serio la posibilidad de cualquier ataque deliberado o imprevisto hacia estas estructuras, de forma que el hecho de que la amenaza sea nacional o internacional hace que se dé un ajuste en las medidas. Ahora bien, en el mismo sentido que Poma y Vargas (2019) los objetivos de los gobiernos se sedimentan en asegurar la información desde la confidencialidad, legalidad, integridad e incluso disponibilidad para que

su posicionamiento a nivel internacional en el aspecto de la ciberseguridad y la ciberdefensa sea relevante y se alinee con las necesidades de la globalización, mediante políticas de seguridad, ente otras herramientas de protección.

El gobierno peruano hace uso de marcos teóricos y estructurales de países y organizaciones aliados para asegurarse de que sus métodos de ciberseguridad sean lo más efectivos posible. La participación en foros sobre este tema, junto con la creación de estrategias de cooperación entre el sector privado y el público (para que los ataques cibernéticos sean identificados más rápidamente en cuanto a la gestión de estos riesgos, la evaluación de las amenazas y la implementación de medidas para atacarlo) y la colaboración de la academia (para impartir educación a la población sobre la forma en la que se pueden proteger de ciertos tipos de ataques cibernéticos), permite que se realicen acciones con mayor rapidez y que se disminuyan los riesgos de estos ataques.

En lo concerniente a Ecuador, debido al crecimiento progresivo de la población con acceso a internet, el país se ha visto obligado a crear márgenes de protección contra el aumento de los cibercrímenes a los cuales se han tenido que enfrentar los nacionales. Por causa del incremento en la oferta de servicios en línea por parte de entidades financieras (como bancos), la mayoría de los crímenes que ha afectado a la población ha tenido objetivos económicos; en consecuencia, "estas instituciones también han tenido que protegerse más efectivamente y el gobierno ha comenzado un proceso para evitar que esto crímenes continúen y mediante la creación de un gobierno y redes comunitarias de protección asegurarse de que el ciberespacio sea un ambiente seguro para cada nacional que haga parte de este" (Vargas et al., 2017).

A partir de la toma de decisiones político-coyunturales, como la creación de instituciones para la regulación, el análisis y el monitoreo de posibles amenazas en el ciberespacio, se han implementado ciertos marcos estratégicos mediante los cuales las instituciones gubernamentales y públicas deben implementar un esquema de protección de la información que manejan para que la población civil mantenga la confianza en las publicaciones de estas páginas. Este aumento de esquemas de seguridad incluye la forma en la cual serán llevadas a cabo las comunicaciones entre diferentes entidades del Estado, con el fin de asegurar y mantener su integridad y confidencialidad.

Colombia fue uno de los primeros países en crear una estrategia integral para proteger a sus ciudadanos de los peligros del ciberespacio. Lo anterior contemplaba que los retos en cuanto a la seguridad doméstica y los ataques

cibernéticos a las empresas, instituciones y/o connacionales podrían tener un valor estratégico. Los principales riesgos identificados por el gobierno colombiano, alude Moreno (2015), han sido "el daño a infraestructuras importantes del país, como la hidroeléctrica o el transporte, o daño a instituciones, como la salud y la educación, debido a amenazas que vienen por la creciente utilización del ciberespacio".

La necesidad de adaptarse y capacitar a las instituciones del país para hacer frente a este nuevo fenómeno se encuentra dentro de la securitización de la agenda nacional actual. Bajo esta premisa, se ha construido una jurisprudencia que busca proteger y anticiparse a las acciones que trae la criminalidad por medio del ciberespacio. Precisamente, en la tabla 1 se muestran las leyes del orden interno de Colombia que han fortalecido los procesos administrativos en el ciberespacio, desde el año 2005, con la intención de adaptarse a las nuevas tecnologías y permitir una mejora en la priorización de acciones que surgen de los procesos económicos, jurídicos, sociales y culturales.

Así mismo, para el año 2009, se vio la necesidad de asegurar penas específicas y útiles en el Código Penal para los delitos que se consumen en el ciberespacio, evidenciando su necesidad para la integridad, la protección y la seguridad nacional, y de igual modo, se resalta el papel de la justicia con las víctimas incluso en espacios no físicos como el internet. Esta acción jurídica trajo como resultado una acción unificada interinstitucional, puesto que amplió la cobertura a más instituciones y hogares nacionales que se encontraban en un estado de peligro o alarma.

Tabla 1. *Leyes que regulan la ciberdefensa y la ciberseguridad en Colombia*

Leyes	Disposición
Ley 962 de 2005	Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	La administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea u nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos".

Leyes	Disposición
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC), se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones.
Modelo de seguridad de la información para la estrategia de gobierno en línea	Este modelo de seguridad hace referencia al conjunto de políticas estratégicas que soportan objetivos de Gobierno en Línea como la "protección de información del individuo" y la "credibilidad y confianza en el Gobierno en Línea".

Fuente: Elaboración propia

Además, la visión internacional del derecho en conjunto con el marco normativo interno busca regular las interacciones estatales y de los sujetos de derecho (dentro del derecho internacional público y privado). Tal y como se ilustra en la tabla 2, existen diversos convenios, acuerdos y tratados internacionales que el Estado colombiano ha ratificado para generar un proceso de cooperación internacional, a fin de castigar los delitos trasnacionales que ponen en riesgo la soberanía territorial y la seguridad nacional; por tal razón, la jurisprudencia internacional permite entender que es necesario blindar (desde lo interno hasta lo externo), las dimensiones en las cuales se camuflan la criminalidad y el delito.

Tabla 2. *Marco internacional que regula la ciberdefensa y la ciberseguridad*

Leyes	Disposición
Convenio sobre Ciberdelincuencia del Consejo de Europa (CCC) (conocido como el convenio sobre cibercriminalidad de Budapest).	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.
Resolución AG/RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.
Decisión 587 de la Comunidad Andina adoptada el 10 de julio de 2004.	Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.

Leyes	Disposición
Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas (2209).	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surgen en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información.
Modelo de seguridad de la información para la estrategia de gobierno en línea	Este modelo de seguridad hace referencia al conjunto de políticas estratégicas que soportan objetivos de Gobierno en Línea como la "protección de información del individuo" y la "credibilidad y confianza en el Gobierno en Línea".

Fuente: Elaboración propia

Adicionalmente, los CONPES 3701 (2011), 2894 (2016) y 3995 (2020) posibilitaron la creación de oficinas encargadas de desarrollar estrategias para proteger ciertos ámbitos de la vida cibernética y un factor fundamental para la gobernanza: la arquitectura de la ciberseguridad y ciberdefensa. Recopilación de acciones, eventos y antecedentes nacionales e internacionales para avanzar en la construcción de una estrategia de ciberdefensa efectiva en cuanto a las amenazas a las que se ha enfrentado el país y la región. El objetivo de esto no consiste únicamente en tener una ciberdefensa capaz de proteger a las instituciones del Estado, sino que la ciberdefensa sea una estructura activa, dinámica y actualizada, que permita (mediante un sondeo digital) saber a qué tipo de amenazas se enfrenta el país en un momento dado y, de esa manera, crear prospectivas sobre la gestión de riesgo dependiendo del nivel de severidad del ataque cibernético.

Uno de los hallazgos de esta investigación es que los países tienden a separar la forma en la que implementan la ciberseguridad y la ciberdefensa dependiendo del objetivo detrás del ataque y de la identidad de la víctima atacada, lo que ocasiona que las legislaciones sobre la forma de definir el crimen, y todo lo que este conlleva, puedan ser insuficientes en cuanto a la cantidad de crímenes que pueden ser cometidos en el ciberespacio. Por ejemplo, se muestra que un

ataque con motivo económico y en el cual la víctima sea un civil estará bajo el marco de ciberseguridad de la Policía Nacional, mientras que si tiene un motivo político o si la víctima es una institución del Estado, se verán involucradas las entidades gubernamentales encargadas de implementar la ciberdefensa del país. De esta manera, las amenazas se categorizan según su rango de peligrosidad, con el propósito de que la estrategia a implementar sea la más efectiva posible y que una institución no se vea abrumada al momento de enfrentarse a cada cibercrimen que suceda en el país (Ulises et al., 2017).

La identificación del tipo de crímenes que parecen ser más comunes en cada territorio, junto con la identidad de los actores que los cometen, ayuda a la creación de estrategias y marcos de acción efectivos para enfrentarlos. En el occidente, los países afectados por la creciente presencia en el ciberespacio y como consecuencia la cantidad de actividades ilegales que se vieron trasladadas o que se crearon a raíz de la ampliación de este nuevo territorio dieron origen a organizaciones y foros por medio de los cuales compartían inteligencia, se entrenaban los unos a los otros y se aliaban para identificar los riesgos que el ciberespacio traía consigo para hacer frente a este fenómeno de mejor manera. En la época de la globalización, la interconexión entre países aliados es esencial para que estos logren combatir de manera competente las amenazas que la revolución tecnológica ayudó a crear.

Aproximaciones teóricas al cibercrimen

Las organizaciones criminales tienden a ser extremadamente efectivas en el empleo de elementos modernos en su estrategia de acción. La globalización ha ayudado a que muchos grupos tengan un alcance más amplio en el mundo; de esto sale el concepto de la 'globalización desviada', la cual puede ser resumida, según Gilman et al. (2011), como la parte inferior desagradable de la integración transnacional, lo que consiste en crímenes que fueron cometidos por causa del fenómeno de la globalización.

La revolución de la tecnología ha permitido que los alcances de grupos ilegales aumenten y ha dado inicio a una nueva generación de crímenes que utilizan el ciberespacio para ser organizados o cometidos. De igual manera, los medios a través de los cuales estos crímenes se llevan a cabo han evolucionado; en un principio, el ciberespacio servía para informar a las personas acerca de las formas o los lugares en los cuales algunos de los crímenes se encontraban.

Sin embargo, esto cambió tras la creación de la '*deep web*', la cual, según Mike Bergman, se define como el contenido de internet que no está indexado por los buscadores.

Ahora bien, esta misma no se constituye en el lugar en el que se encuentran los dominios para actividades, grupos o compras ilegales. Gracias a su creación y popularización, la denominada '*dark web*', que alberga los enlaces particulares para ingresar a las comunidades de interés, y la '*DarkNet*', que puede ser simplificada como el dominio dentro del cual se llevan a cabo las conversaciones y negocios de una comunidad en específico (Rudesill et al., 2015).

Es importante entender que el ingreso a la '*dark web*' y los filtros que se tienen presentes al momento de dar a conocer el dominio de una '*DarkNet*' son extremadamente controlados. A pesar de que existen buscadores específicos en la '*deep web*' para dar con la '*dark web*', esta exige la existencia de *software*, contraseñas y, en ocasiones, invitaciones; por lo tanto, no es posible que una persona sin conocimiento o conexiones previas ingrese a uno de estos sitios. Una vez la persona consigue acceso a uno de estos dominios se encuentra con múltiples actividades, conversaciones, comercios y propaganda sobre la comunidad en la que se encuentra. Este tipo de evoluciones en el internet es lo que ha permitido que el crimen se pueda planear con mayor facilidad, no solo en el ámbito cibernético, sino en situaciones en la que se ha trasladado al mundo físico.

La revolución tecnológica ha permitido que muchas comunidades se trasladen al ciberespacio y que crezcan y evolucionen dentro de este ambiente para adaptarse a las nuevas tecnologías y a la posibilidad de crear una conexión con personas de cada rincón del mundo. Además, esta revolución les ha facilitado la vida a muchas personas, creó un sinfín de posibilidades para la población civil del mundo y permitió que la información viajara con mayor rapidez gracias a esta nueva interconexión. No obstante, esto también ha permitido que las organizaciones criminales sean capaces de trasladar sus acciones, objetivos y negocios del mundo físico al mundo cibernético y que se les abra una nueva dimensión.

Es necesario tener en cuenta que hay dos formas en las que un cibercrimen puede tener lugar: un cibercrimen puede ser llamado como tal cuando la acción al margen de la ley ocurre en el ciberespacio y cuando el plan ocurre en el ambiente cibernético y la acción en el plano físico. El ambiente en el que el crimen ocurre sea este en el ciberespacio o en el mundo físico puede afectar su definición al momento de ser investigada, es por esto que es necesario que se

entienda que crímenes entran dentro de la categoría de cibercrimen, para a su vez, ampliar la estrategia y la importancia que se le da a este fenómeno (Wittes & Blum, 2015). El entender que el cibercrimen no siempre se mantiene de manera exclusiva en el ciberespacio y que las estructuras físicas también se pueden ver afectadas por esta forma de crimen permitirá que este pase al primer plano en la estrategia de seguridad.

Se tiende a dividir completamente al ciberespacio y al espacio físico en muchas formas. Las comunidades virtuales, las formas en las que las redes sociales funcionan o la información que es compartida en internet tienden a ser separadas de su contraparte en el mundo físico. Sin embargo, esta separación no debería ser hecha de manera tan definitiva, ya que, se ha visto que, en el caso de ataques a las estructuras del estado, algunos de los ataques a las estructuras físicas son planeados en estructuras cibernéticas como foros o chats. Este tipo de ataques duales también deben estar incluidos en el término de ciberataque (Padalka, 2022) para así facilitar la forma de buscar a los responsables, permitiendo que no solo las redes sociales sino foros de internet sean considerados posibles lugares de encuentro para la planeación del ataque, por lo mismo, no se debe tener una separación tajante entre los ámbitos físicos y del ciberespacio.

Siguiendo lo anterior, la existencia de grupos que funcionan dualmente en el ambiente cibernético y físico también debe ser tenida en cuenta. La implementación del ciberespacio para ampliar su alcance y para iniciar un nuevo proceso de reclutamiento, haciendo uso de sitios públicos y fáciles de encontrar si una persona cumple con un perfil especifico (Skopik et al., 2016). La evolución de los grupos ilegales y la forma en la que estos han implementado los avances tecnológicos que se han dado en los últimos años hace que los estados deban evolucionar de igual manera, o incluso más rápido, incluyendo al ciberespacio dentro de las estrategias de seguridad y estudiando la forma en el que el nuevo ambiente tecnológico mundial afecta la velocidad y la forma en la que el crimen se mueve a través del mundo y afecta a los diferentes actores de la sociedad internacional, para poder prevenir el avance de los grupos ilegales.

Métodos y estrategias para la anticipación del cibercrimen

La competencia que existe entre los diferentes actores de la sociedad internacional en cuanto a la forma en la que se implementan las nuevas tecnologías y evolucionan los marcos y las estrategias que estos actores poseen para contrarrestar los efectos negativos que la Revolución Tecnológica pueda tener en el mundo. Esta metodología permite que los Estados pongan estos temas en el primer plano de los nuevos intereses de seguridad y que se sientan obligados a iniciar marcos de estrategias y prospectivas para la protección contra la nueva generación de crimen. Tal como la carrera armamentística que se llevó a cabo durante la Guerra Fría, la competencia para adquirir protección frente a temas del ciberespacio ayuda a la ampliación de los marcos de seguridad y defensa y a detener, de alguna manera, a los actores ilegales (Realpe & Cano, 2016).

Otra forma en la que esta competencia puede ayudar a los países a posicionarse de manera más segura en el mundo globalizado y la manera en la que sus políticas de ciberseguridad y ciberdefensa funcionan en cuanto a otros actores de la sociedad. Las organizaciones internacionales han permitido que se creen algunos marcos de acción que sus países miembros pueden implementar en sus políticas nacionales o analizar los documentos para así construir unas políticas que pueden estar inspiradas en estos, pero que se acomoden de mejor manera a la realidad del país en cuestión (Cano, 2011). Las influencias regionales en cuanto a las formas que otros países utilizan para enfrentarse a amenazas, que pueden ser las mismas o similares a las de otros países en la región.

Teniendo en cuenta lo anterior, se puede afirmar que la cooperación internacional es necesaria para lograr solucionar estas amenazas a la seguridad, especialmente en un contexto regional, en el cual los peligros a los que los Estados se enfrentan tienden a ser similares y la estructura de los gobiernos pueden ser parecidos de igual manera. La cooperación entre los diferentes actores, junto con la acción de compartir inteligencia con otros países de la región que se encuentren menos preparados para estos crímenes permite que la región como un todo se encuentre más preparada.

Otro aspecto que puede ayudar a que los países se encuentren mejor preparados al momento de enfrentarse a las amenazas que la revolución tecnológica, y que la evolución que está a causado en los actores criminales de la actualidad, ha creado es la educación de todos los sectores de la sociedad. La necesidad de

que las poblaciones de un país en el que el acceso a internet ha ido en aumento tengan conocimiento de la existencia del cibercrimen, los tipos de este a los que se pueden ver expuestos y las formas en las que pueden protegerse, ha ido en aumento de igual manera, la educación en protección cibernética debe ser priorizada, para permitir que el Estado pueda concentrarse principalmente en los grandes ciberataques a los que pueden verse expuestos y a la forma en la que la falta de conciencia y educación de la población civil en cuanto al ciberespacio puede ponerlos en riesgo, ya que, las direcciones de IP desprotegidas le dan a los cibercriminales una entrada y salida fácil del país (Ulises et al., 2017).

La forma en la que esto se presenta muestra que los actores ilegales hacen uso de ordenadores desprotegidos para entrar a un país y llevar a cabo crímenes, es más fácil hacer esto sin ser detectados si se utilizan varios IP del país, y de otros países para borrar el rastro del ordenador original. Esto hace que los computadores que no cuentan con protecciones como antivirus se convierta en un tipo de "mula" de la nueva generación de crimen. Comúnmente se denomina el nombre de "mula" a una persona que se presta para transportar sustancias u objetos ilegales de un lugar a otro, a cambio de una pequeña suma de dinero, en el contexto del ciberespacio se pueden identificar dos tipos, la "mula" que no está enterada de que su dirección IP está siendo utilizada para redireccionar a las autoridades, y los *money donkeys*, quienes son los encargados de limpiar el dinero recolectado de estas acciones y de posteriormente guardarlo en un paraíso fiscal (Montoya et al., 2017).

Por lo anterior, la educación de los sectores público, privado y de la ciudadanía debe ser vista como una herramienta, no solo útil, sino, necesaria para asegurar un nivel básico de protección en el ciberespacio del país. Esto puede conseguirse por medio de la implementación de una educación en seguridad informática básica obligatoria en los colegios del país, además, reglamentar que cada computador en el país posea un tipo de antivirus, también puede ayudar a proteger a los diferentes grupos del país de ataques indeseados.

Conclusiones

Para conseguir que un país se encuentre lo más protegido posible para los ataques cibernéticos más comunes, y a su vez preparado para los ataques de mayor impacto, sin que la combinación de estos dos cause un sistema abrumado y poco eficiente. Se debe entender que el triunfo de un sistema de ciberseguridad

y ciberdefensa de un país se basa en iniciar desde el nivel de seguridad más bajo e ir subiendo de nivel. De esta manera, los organismos del Estado pueden estar más seguros de que las bases de su protección y el nivel de seguridad que se tiene, tanto en los sectores público y privado, como en la sociedad civil que tiene presencia en el ciberespacio y así, preocuparse de manera más específica por crear estrategias para los casos en los cuales estas primeras barreras de protección se vean traspasadas, en los cuales las amenazas tendrán una magnitud mayor (Perdomo González, 2016).

Otra parte importante de la forma en la que un país puede crear una buena estrategia de ciberseguridad y ciberdefensa es mantener una mirada hacia el exterior, por medio del análisis y estudio de documentos acerca de la región publicados por organizaciones internacionales o foros de interés, para así entender de mejor manera como se ve la situación del país y la región como un todo. La cooperación internacional mediante la construcción de conversaciones y la normalización de generar comunicaciones acerca de información e inteligencia que pueda ser útil para la construcción de estrategias y la protección de los países de la región (Fernández-Osorio et al., 2019). La generación de un muro de protección tanto nacional como regional y un sistema de *whistlerblower* mediante el cual las amenazas y los actores ilegales más comunes sean identificados más rápida y efectivamente permitirá que las estrategias de los países sean llevadas a cabo de mejor manera.

Referencias

Abdenur, A. (2014). China and the BRICS Development Bank: Legitimacy and Multilateralism in South-South Cooperation. *IDS Bulletin, 12*(4), 85-101. https://doi.org/10.1111/1759-5436.12095

Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas* (Asociación Colombiana de Ingenieros de Sistemas), (119), 4-7.

Cornaglia, S., & Vercelli, A. H. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO: Revista Latinoamericana de Estudios de Seguridad*, (20), 46-62.

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

Fernández-Osorio, A., Cúfiño-Gutiérrez, F., Gómez-Díaz, C., & Tovar-Cabrera, G. (2019). Dynamics of State modernization in Colombia: the virtuous cycle of military transformation. *Democracy and security, 15*(1), 75-104. https://doi.org/10.1080/17419166.2018.1517332

Gilman, N., Goldhammer, J., & Weber, S. (2011). *Deviant globalization: Black market economy in the 21st Century*. Continuum.

Gobierno de Chile (2016). *Política Nacional de Ciberseguridad (2017-2022)*. Gobierno de Chile.

Interpol. (2020). Centro de mando y coordinación. *https://tinyurl.com/yeeckfdp*

Lavinder, K. (2018). Cyber Attacks: Is Latin America Prepa-red? *Air & Space Power Journal*. https://tinyurl.com/yckmve3m

Lobato, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. *Revista Latinoamericana de Estudios de Seguridad*, 16-30. https://doi.org/10.17141/urvio.20.2017.2576

Montoya, Y. C., Verdezoto, V. H., & Ramírez, A. V. (2017). Ciberdefensa, ciberseguridad y sus efectos en la sociedad. *International Multilingual Journal of Science and Technology*. https://tinyurl.com/5472b48z

Moreno, W. C. (2015). *Ciberdefensa y ciberseguridad en el sector defensa de Colombia*. Universidad Piloto de Colombia. https://tinyurl.com/5t4c8swm

Organización de Estados Americanos (OEA). (2017). *Desafíos del riesgo cibernético en el sector financiero para Colombia y américa latina*. https://tinyurl.com/yc5drv4k

Padalka, A. (2022). Forensic and technical criminalistics support in cybercrime investigation: countering cyber threats in Ukraine. *Revista Científica General José María Córdova, 20* (38), 407-423.https://dx.doi.org/10.21830/19006586.901

Payá-Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova, 19*(36), 1121-1136. https://dx.doi.org/10.21830/19006586.855

Perdomo González, C. (2016). *Operaciones de información y ciberdefensa; conceptualizaciones en las estrategias de seguridad nacional* [Tesis doctoral]. Universidad de Las Palmas de Gran Canaria.

Poma, A., & Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *Sciéndo*, 275-282.

Realpe, M. E., & Cano, J. (2016). Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. En *Seguridad Informática. X Congreso Iberoamericano*. Universidad del Rosario.

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). *The deep web and the darknet: a look inside the internet's massive black box*. Woodrow Wilson International Center for Scholars. https://tinyurl.com/26a3xep7

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 154-176. https://tinyurl.com/yckhkdx3

Ulises, J., Fonseca, C., Arsolena, M., & Perdomo, L. (2017). *La defensa cibernética, alcances estratégicos y proyecciones doctrinarias y educativas*. Universidad de la Defensa Nacional.

Vargas, R., Reyes Chicango, R., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (20), 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Wittes, B., & Blum, G. (2015). *The future of violence: Robots and germs, hackers and drones-confronting a new age of threat*. Basic Books.