UCINA INTERNACIONAL
Revista de RI
2023 / nro. 3
ISSN 2796-7204

Desafío internacional en materia de ciberdefensa y cómo Colombia es considerada pionera de estrategias en la región

International challenge in cyberdefense and how Colombia is considered a pioneer in the region

(Fecha de recepción: 15/04/23 - Fecha de aceptación 27/06/22)

Lucía Sonego Castellanos[1]

Resumen

El avance de la tecnología ha permitido la creación de un nuevo estilo de vida, ofreciendo múltiples oportunidades, pero también, diversas amenazas. Estamos bajo este punto, en la presencia de actos ilícitos en el ciberespacio y el riesgo que representa esto en las infraestructuras críticas de los Estados y el campo internacional. Es fundamental entonces generar políticas y estrategias de ciberseguridad y ciberdefensa. Analizamos el caso de Colombia como pionero en la materia en Latinoamérica y observamos una breve comparación con algunos países de América del Sur que adoptan Estrategias de ciberdefensa propias y dentro del marco de la cooperación internacional.

Palabras clave: ciberterrorismo; ciberdefensa; ciberespacio; infraestructura crítica; amenaza.

Abstract

The advancement of technology has allowed for the creation of a new way of life, offering multiple opportunities but also various threats. We are currently facing illicit acts in cyberspace and the risk this poses to critical infrastructure of nations and the international arena. It is therefore crucial to develop cybersecurity and cyberdefense policies and strategies. We analyze the case of Colombia as a pioneer in this field in Latin America and provide a brief comparison with some countries in South America that adopt their own cyberdefense strategies within the framework of international cooperation.

Key words: cyberterrorism; cyberdefense; cyberespace; critical infrastructure; threat.

1 Universidad de Congreso, Mendoza, Argentina. Contacto: sonegolucia@alumnos.ucongreso.edu.ar

1. Introducción

Año 2023. Habitamos en un mundo globalizado donde la ciencia y la tecnología avanzan de manera exponencial, creando espacios y situaciones que, hace un par de años atrás, hubiesen sido impensadas. Facilitando en muchas ocasiones la vida de millones de usuarios, permitiendo el acceso inmediato a la información, impulsando nuevas industrias, entre miles de otras funciones, el ser humano encontró en la tecnología un nuevo estilo de vida. «Esta herramienta ha evolucionado de forma tal que ha creado un nuevo espacio virtual de interacción, que desdibuja las fronteras territoriales e integra a quienes tienen acceso al mundo digital en una red compleja de transmisión de información: ciberespacio» (Mansell y Raboy, 2011 en Perafán Del Campo, et al., 2021).

Sin embargo, no es ni ha sido utilizada siempre con fines lícitos o moralmente correctos, y ha permitido que pueda darse un nuevo espacio para dañar el orden social. Así es que dentro de este contexto mundial surgen nuevos escenarios para la existencia de conflictos y nuevos actores que los llevan a cabo. Hablamos entonces del ciberespacio como escenario de ataque y ofensa, para el cual muchos Estados no están preparados, sabiendo que cuentan muchas veces con pocas herramientas o la falta de muchas de ellas para hacer frente a esta problemática, pero que, paradójicamente, muchos de ellos son quienes motivan estos conflictos.

En este punto, parece importante diferenciar conceptos como ciberguerra y ciberterrorismo. Pérez Gómez, A. (2020) establece que hablar de ciberterrorismo es proveniente de ciberespacio y terrorismo y es llevado a cabo por actores no estatales, siendo esta la principal diferencia con la ciberguerra. Por tanto, al hablar de ciberguerra hacemos referencia a un conflicto donde los actores o uno de los principales actores es el Estado. Sin embargo, también afirma que no todos los actores no estatales pueden considerarse como ciberterroristas, ya que:

> En primer lugar, los ataques más dañinos y destructivos no están motivados por razones políticas ni sociales, en la mayoría de ellos se trata de un móvil lucrativo; en segundo lugar, los ataques han sido conectados con objetivos políticos y sociales sin llegar a ser intimidatorios ni nocivos, siendo ejecutados por activistas, no por terroristas (p. 7).

Diversos autores coinciden en que el ciberterrorismo es una amenaza futura para la cual debemos estar prevenidos y poder anticiparnos a la misma para actuar (Pérez Gómez, 2020; Piñeros, et al., 2020).

Para dar respuesta a ello, es que surgen los términos de ciberseguridad y ciberdefensa, diferenciados por el hecho de que el último mencionado es la capacidad estatal de prevenir y contrarrestar toda amenaza cibernética que pueda afectar la soberanía, mientras que ciberseguridad refiere a minimizar el nivel de riesgo al cual se exponen los ciudadanos de un Estado ante amenazas o incidentes en el ciberespacio (Mayorga Delgado, 2014).

Existen también otras definiciones que enmarcan y describen a la actividad ilegal en el ciberespacio y la respuesta estatal a la misma. A continuación, distinguimos algunas definiciones recuperadas del Seminario de Defensa Nacional y Relaciones Internacionales (2023, 17 de mayo):

Ciberoperaciones: aplicación en el ciberespacio de tácticas militares tradicionales. El disertante lo divide en dos tipos: operaciones de ciberinfluencia (influyen en la decisión del bando enemigo), y operaciones de ciberataques (uso de ciberarma de forma deliberada).

Ciberataque: uso deliberado de un ciberarma para producir un daño perjudicial en redes y sistemas de información.

Ciberefectos: daños o impactos producidos por ciberataques. Pueden ser ruidosos, aquellos de corta duración y recuperación; o silenciosos, aquellos largoplacistas y persistentes.

Teniendo presentes las distinciones entre las definiciones anteriores, nos proponemos analizar la existencia o no de ciberataques en distintos lugares del mundo, principalmente, Latinoamérica y la respuesta o medida preventiva que elaboran los Estados.

En el presente ensayo analizamos el caso de Colombia y las medidas de ciberdefensa que propone utilizar en su Estado nacional, bajo su marco normativo, buscando mejorar la ciberseguridad del país y cómo opera o no con distintos países y organizaciones en el plano internacional y de cooperación.

2. Metodología

Metodológicamente, este trabajo se desarrolla sobre la base de investigaciones académicas publicadas entre 2014 y 2023. Se realizaron diversas búsquedas en distintas plataformas de internet, con las siguientes palabras clave: «ciberterrorismo», «ciberdefensa» y «Colombia». De esta manera, todos los artículos que presentaron resúmenes coherentes con el tema fueron utilizados para el análisis y comprensión de estos temas en el país elegido. Así mismo, se utilizó bibliografía de cátedra para conceptos generales, y se integró el marco teórico propuesto en el Seminario en Defensa Nacional y Relaciones Internacionales.

3. Los fines ilícitos en el ciberespacio

Como se mencionó anteriormente, si bien los avances tecnológicos trajeron consigo un nuevo estilo de vida, no siempre es utilizado con fines lícitos. Hablamos entonces de la presencia de actos ilegales en el ciberespacio.

Las nuevas tecnologías de información y comunicación (TIC) se convierten en facilitadores y creadores de un escenario ideal para cometer actos ilícitos, principalmente por contar con la característica de mantener el anonimato, tener un alto poder de camuflaje, y atravesar y romper barreras, fronteras y largas distancias desde la comodidad del hogar o con el uso simple de un dispositivo electrónico (Pérez Gómez, Amanda, 2020). Estas características llevan a que el ciberterrorismo presente ciertas ventajas frente al acto terrorista. Cespedosa Rodríguez (2019) destaca que, en líneas generales, las mismas son no comprometer físicamente al terrorista y la garantía de mantener su anonimato; su actuación ilimitada respecto al ámbito geográfico; la repercusión mundial que generan sus actos mediante medios de comunicación y propaganda; y el beneficio económico que ofrece, ya que termina siendo menos costoso.

Tomamos el concepto de infraestructura crítica como el conjunto de redes de comunicación, información y telecomunicaciones que puede impactar en la seguridad, economía, salud pública, soberanía, de una nación si se ve atacada, interferida o destruida (Mayorga Delgado, 2014; González, 2022). Cualquier tipo de actividad o acto ilícito en el ciberespacio supone una amenaza a la infraestructura crítica de los Estados.

Si hablamos de grupos terroristas, se puede destacar el hecho conveniente de que el ciberespacio sea el lugar perfecto para que encuentren sus fuentes de financiación y puedan llevar a cabo cualquier acto ciberterrorista como difusión y propaganda, realización de ciberataques, divulgación de técnicas y herramientas, radicalización de individuos y reclutamiento (Pérez Gómez, Amanda, 2020).

Dion-Schwarz (2019) expone cómo es el uso del dinero y el financiamiento de grupos terroristas. Nos habla de la utilización que estos grupos hacen o pueden llegar a hacer de las criptomonedas, respondiendo a sus necesidades y oportunidades, ya que podrían «financiar ataques de manera más fácil que con las monedas fiduciarias actuales». Divide el análisis de financiación de grupos terroristas en tres partes: recepción o captación, gestión y gasto o inversión. Explica entonces que las fuentes de captación del recurso económico pueden ser muy diversas y pueden provenir tanto de manera legal

como ilegal, y en este punto, las criptomonedas podrían ayudarlos a recibir el recurso desde diversos medios, principalmente de procedencia ilegal. Una vez que sus fondos son gestionados y captados, la autora explica que la etapa de análisis siguiente es la gestión o manejo de ese recurso financiero. Estos grupos cuentan con diversas formas de transferencia de dinero, y diversas maniobras, que incluyen el lavado de dinero. Sin embargo, en cuanto a la información encriptada y el uso de criptomonedas por parte de ellos, puede llegar a resultar crítico en el contexto actual, a menos que en un futuro exista algún tipo de criptomoneda menos regulada que Bitcoin. Esto se debe a que las transacciones grandes pueden resultar llamativas y más aún cuando se establecen entre ciertos países específicamente. «Las transferencias de fondos grandes a través de Bitcoin que ocurren rápidamente requerirían la compra de suficientes bitcoins para que las autoridades lo noten, lo que crea riesgos, y cambiaría los precios del mercado, aumentando los costos» (p. 12). Y, finalmente, la última etapa propuesta, es la de gasto o inversión por parte de estos grupos. En este punto, Dion-Schwarz distingue entre costos operativos y costos para producir violencia, los cuales son difíciles de distinguir y delimitar. Lo que según ella ha llevado a los grupos terroristas a considerar la opción de las criptomonedas, es el hecho de las medidas impuestas en los últimos años en la lucha frente al financiamiento del terrorismo. Afirma que las medidas que cada grupo tome para gastar o invertir, financiar sus actos, presentan un desafío significativo y pueden generar distintos impactos.

4. Una aproximación al Estado colombiano y sus medidas preventivas en materia cibernética

Habiendo conceptualizado de manera general el marco del ciberterrorismo, vamos a analizar el caso estatal de ciberdefensa y ciberseguridad del Estado colombiano.

Colombia es considerado el Estado pionero en la región en materia de ciberdefensa y propuestas de prevención de ciberataques (Mayorga Delgado, A., 2014; Cujabante Villamil, 2020). Diversos autores coinciden en que el Estado colombiano busca adecuar su seguridad nacional a los nuevos escenarios de conflicto, combinando así las fuerzas cívico-militares y estableciendo que la mejor manera de prevenir un ataque ciberterrorista es teniendo a la sociedad como principal aliado y defensor de ello (Mayorga Delgado, 2014; Cujabante Villamil, 2020).

Anteriormente se hizo mención de «fuerzas cívico-militares». Estas deben ser comprendidas dentro de este nuevo contexto de nuevas amenazas, ya que se ha ido debilitando la línea divisoria entre civiles y militares (Cujabante Villamil, 2020). En este punto, la relación cívico-militar en Colombia es catalogada de tipo objetivo, debido a que son los civiles quienes quieren asegurar la no injerencia militar en la política y su seguridad (Andrade, 2012 en Cujabante Villamil, 2020).

Sin embargo, en la historia del país, han sufrido distintos altibajos entre la relación civil y militar, y de esta con la influencia política. En la actualidad, hay quienes aseguran que esta relación cívico-militar no está dada por un control civil y democrático o de educación democrática hacia los militares, y esta es la razón principal por la cual es necesario crear nuevos mecanismos y organismos de defensa, principalmente en materia cibernética (Cujabante Villamil, 2020).

Por esta razón, y para hacer frente y prevenir cualquier tipo de amenaza cibernética, es que hacia el año 2011 se crea un organismo estratégico en el Ministerio de Defensa, materializado como Conpes 3701 del 14 de julio de 2011 (Mayorga Delgado, A., 2014; Cujabante Villamil, 2020).

4.1. Conpes 3701 de 2011 y la normativa nacional colombiana

En julio de 2011, se elabora una política de ciberseguridad y ciberdefensa que tiene como base el documento Conpes 3701, orientado a medidas preventivas ante posibles amenazas informáticas (Mayorga Delgado, A., 2014).

El 14 de julio de 2011, Colombia se convirtió en uno de los primeros países en la región en establecer planes de acciones concretas en la defensa del ciberespacio (Cujabante Villamil et al., 2020). Publicado en esa fecha, el Conpes 3701 establece los lineamientos para la ciberseguridad y ciberdefensa en Colombia, con el objetivo central de «fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio» (p. 20).

Es importante hacer mención a la normativa nacional y los esfuerzos realizados por el país. A continuación, entonces, nombramos las leyes y resoluciones colombianas sobre esa materia para que sea posible comprender su evolución cronológica. Primero, en 1999 la Ley 527 de Comercio Electrónico, definiendo y limitando el manejo de datos. Luego, en el 2000 la Ley 599 donde se estructura el tipo penal de «violación ilícita de comunicaciones». En el año 2005, la Ley 962 establece la ilegalidad de la utilización de medios tecnológicos para disminuir costos de trámites por parte de los administrados. Año 2007, Ley 1150, y año 2009 Ley 1273 por la que se modifica el Código Penal. Este año también se sancionó la Ley 1341, donde se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 y Circular 052 de 2007 (Superintendencia Financiera de Colombia) (Normatividad Nacional en la materia, Conpes 3701, 2011, p. 11).

4.2. El COLCERT

En cabeza del Ministerio de Defensa Nacional, en Colombia fue creado el Grupo de Respuesta a Emergencias Cibernéticas (COLCERT), que define su misión como:

> Identificar infraestructuras críticas, gestionar sus riesgos de ciberseguridad, ofrecer a las empresas del sector público y privado, información preventiva sobre amenazas y vulnerabilidades, apoyo y asesoría en la gestión de los incidentes de ciberseguridad, que garanticen la continuidad de las operaciones y servicios a la ciudadanía colombiana (COLCERT, 2022).

Entre los objetivos del grupo se pueden mencionar: coordinar el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), entre otros, con las instancias responsables, para la gestión de amenazas e incidentes de Seguridad Digital Nacional; coordinar respuestas rápidas y eficientes a incidentes; acompañar y apoyar a las entidades de la administración pública en Colombia para mejorar sus procesos de seguridad de la infraestructura tecnológica y gestión de incidentes; promover el desarrollo de capacidades locales y sectoriales para la gestión operativa de los incidentes de Seguridad Digital; desarrollar y divulgar procedimientos y recomendaciones; coordinar la actividad de identificación de las infraestructuras críticas y generar mecanismos de defensa; promover espacios de cooperación nacional e internacional; y mantener actualizado el Sistema de Gestión (COLCERT, 2022).

4.3. Política comparada: normativa argentina y otros ejemplos de Latinoamérica

En el Seminario en Defensa Nacional y Relaciones Internacionales que se dictó el pasado 17 de mayo de 2023 en la Ciudad de Mendoza, se expuso el marco normativo y regulación argentina sobre el asunto competente a ciberseguridad y ciberdefensa.

Habiendo contextualizado y brindado información general sobre la normativa colombiana, proponemos generar una comparativa entre distintos Estados de América Latina, principalmente, con nuestra normativa argentina.

En Argentina existe una serie de leyes relacionadas a la ciberseguridad, una serie de disposiciones y resoluciones normativas vinculadas a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad y una serie de decretos y resoluciones que dieron origen al Comité de Ciberseguridad (disponible en Argentina.gob.ar)

En el año 2017 en Argentina se crea el Comité de Ciberseguridad, que luego en el año 2019, serían modificado los artículos 1°, 3° y 5° de dicha norma constitutiva. Dicho Comité se crea con el objetivo principal de elaborar una Estrategia Nacional de Ciberseguridad. Este Comité está integrado por la Secretaría de Gobierno, la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros, el Ministerio de Defensa, el Ministerio de Seguridad, el Ministerio de Relaciones Exteriores y Culto, y el Ministerio de Justicia y Derechos Humanos y tiene el fin último, anteriormente mencionado de la elaboración de la Estrategia Nacional de Ciberseguridad (Art. 1° del Decreto 480/2019). Sin embargo, ya desde los años noventa venía teniendo intentos de creación de equipos que pudieran regular esta materia.

Otro país avanzado en materia de prevención y contraprestación a amenazas cibernéticas, es Brasil. Este país cuenta con el Servicio de Represión de Delitos Cibernéticos, a cargo de la Policía Federal. Así mismo, hacia el año 2010, aprobó en Brasilia la creación del Centro de Defensa Cibernética del Ejército que cuenta con un Departamento de Seguridad de la Información y las Comunicaciones (Mayorga Delgado, 2014).

Finalmente, exponemos una comparativa con Ecuador, el cual no cuenta con un órgano regulador ni de prevención de amenazas cibernéticas. Sin embargo, en agosto de 2022 se aprobó el primer plan de Estrategia Nacional de Ciberseguridad con el objetivo de crear un ciberespacio seguro para los ciudadanos y bajo altos estándares internacionales de influencia (Ministerio de Telecomunicaciones y de la Sociedad de la Información, disponible en línea).

Conclusiones

Finalmente, podemos llegar a las siguientes conclusiones:

En primer lugar, vivimos en una realidad donde las tecnologías se apropian cada vez más de nuestros estilos de vida, generando oportunidades, pero también nuevos riesgos y amenazas que atentan a los Estados y su soberanía y al contexto internacional en su conjunto. Esto se debe a la existencia de actividades ilícitas en el ciberespacio que presentan una fuerte amenaza en la infraestructura crítica de los Estados.

Por otra parte, las nuevas tecnologías de información y comunicación (TIC), presentan nuevos escenarios ventajosos para la actividad ciberterrorista y, con el surgimiento de criptomonedas, se presentan nuevos medios de financiamiento para estas organizaciones debido a la garantización del anonimato y el permiso asequible para la obtención de recursos ya sea de manera lícita o ilícita para financiar y sustentar sus actos.

En lo que respecta al Estado colombiano, si bien es considerado pionero en materia de desarrollo de ciberseguridad y ciberdefensa en Latinoamérica, no es el único. Por el contrario, cada vez más Estados despiertan su interés y asumen su responsabilidad frente a esta problemática y buscan su participación en el ámbito de cooperación internacional, principalmente bajo el marco europeo.

Es fundamental el desarrollo de ciberseguridad y ciberdefensa en los Estados. El gobierno colombiano ha buscado fortalecer

las capacidades del Estado y ha establecido lineamientos para la ciberseguridad y ciberdefensa a través del Conpes 3701, que tiene como objetivo principal proteger el ciberespacio y brindar seguridad en este ámbito.

Finalmente, el ciberterrorismo y los ciberataques representan desafíos significativos en la actualidad. Los Estados, deben adoptar medidas preventivas y fortalecer su capacidad de ciberdefensa para proteger sus infraestructuras críticas y la seguridad nacional e internacional. El ciberespacio es un escenario complejo que requiere una atención constante y acciones coordinadas para garantizar la seguridad en el mundo digital.

Referencias bibliográficas

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Bie3: Boletín IEEE.ES.* Disponible en línea en https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Cespedosa Rodríguez, Carolina. (2019). Yihadismo, Internet y Ciberterrorismo. *Comillas.edu*. https://doi.org/http://hdl.handle.net/11531/30875

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. Disponible en https://revistacientificaesmic.com/index.php/esmic/article/view/588/666

Dion-Schwarz, C. (2019). *Terrorist use of cryptocurrencies: technical and organizational barriers and future threats*. Santa Monica, Calif.: Rand Corporation. (Capítulo IV)

González, Sol (10 de marzo de 2022). Ciberataques a la infraestructura crítica de un país y sus consecuencias. Recuperado en línea: https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/

Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2022). Grupo de respuesta a emergencias cibernéticas de Colombia. http://www.colcert.gov.co/

Jefatura de Gabinete de Ministros. (s.f.). Normativa. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

Mayorga Delgado, A. (2014). Lineamientos, Tendencias y Estrategias sobre Ciberseguridad y Ciberdefensa en Colombia (Trabajo de Grado). Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2868

Ministerio de Telecomunicaciones y de la Sociedad de la Información (5 de agosto de 2022) Gobierno de Ecuador. Recuperado de: https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

Montenegro Moreno, H. M., Pantoja Rosero, M. J., Rojas Larrotta, A. Y., & García Briceño, R. (2022). Políticas públicas de ciberdefensa en Chile y Colombia: Un análisis desde el rastreo de procesos. *Brújula Semilleros De Investigación*, *10*(20), 7–16. https://doi.org/10.21830/23460628.118

Piñeros, D. V., Prieto, P., & Garzón, D. La ciberseguridad, la ciberdefensa, la identidad y los intereses nacionales y las Fuerzas Militares de Colombia. *Identidad*, 507.

Perafán Del Campo, E. A., Polo Alvis. S., Sánchez Acevedo, M. E. y Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. Via Inveniendi Et Iudicandi, 16(1). https://doi.org/10.15332/19090528.6480

Pérez Gómez, A. (2020). Ciberterrorismo, ¿una nueva amenaza? *Bie3: Boletín IEEE*,*19*, 386–400. https://doi.org/https://dialnet.unirioja.es/descarga/articulo/7625260.pdf

Seminario en Defensa Nacional y Relaciones Internacionales. 17 de mayo de 2023. Ciudad de Mendoza, Argentina.