Capítulo 4

La estrategia de ciberseguridad y ciberdefensa en Colombia: una política pública en constante construcción [24]

Carlos Alberto Ardila Castro [25]
Escuela Superior de Guerra

Resumen

La Revolución Tecnológica propiciada por la globalización ha significado un proceso de transformación de las relaciones sociales, políticas y culturales alrededor del mundo, estas fundamentadas en el desarrollo de nuevas tecnologías de la información y de la comunicación, aspectos que han generado una creciente dependencia de las actividades humanas por la tecnología. En consecuencia, nuevos actores y amenazas convergen en un

24 Capítulo de libro resultado de investigación vinculado al proyecto de investigación "Desafíos para la Seguridad y Defensa Nacional de Colombia - Fase III", que hace parte de la línea de investigación: "Políticas y modelos de seguridad y defensa" perteneciente al Grupo de Investigación "Centro de Gravedad", reconocido y categorizado en (A) por COLCIENCIAS registrado con el código COL0104976 vinculado al Centro de Estudios Estratégicos en Seguridad y Defensa Nacionales -CSEDN-, adscrito y financiado por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

25 Candidato a Doctorado en Educación en la "Universidad Internacional Iberoamericana", México. Magister en Relaciones y Negocios Internacionales de la Universidad Militar Nueva Granada. Profesional en Ciencias Militares de la Escuela Militar de Cadetes "General José María Córdova". Investigador Asociado de COLCIENCIAS. Jefe de Investigación de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Docente Investigador y Líder del grupo de investigación "Centro de Gravedad" de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Contacto: carlosardilacastro@gmail.com.

escenario de dominio de Quinta Generación, fuera de cualquier regulación internacional y lejos de los alcances del control de cualquier Estado: el ciberespacio. Con respecto a lo anterior, cabe plantear el siguiente interrogante: ¿Cómo ha evolucionado la estrategia de ciberdefensa en Colombia en los últimos 20 años? Para dar respuesta a lo planteado, el presente capítulo se organiza en los siguientes apartados; a) explicación del concepto de ciberespacio, b) categorización de los conceptos de ciberseguridad y ciberdefensa en Colombia, c) identificación de las políticas públicas de ciberseguridad en Colombia, y d) descripción de la arquitectura del Sistema en Colombia.

Palabras Claves: Seguridad, Ciberespacio, Ciberseguridad, Ciberdefensa.

Abstract

The Technological Revolution favored by globalization has meant a process of transformation of social, political and cultural relations around the world. These are based on the development of new information and communication technologies, aspects that have generated an increasing dependence on human activities for technology. Consequently, new actors and threats converge in a Fifth Generation domain scenario, outside of any international regulation and far from the scope of control of any state: cyberspace. Regarding the above, the following question should be asked: How has the cyberdefense strategy evolved in Colombia in the last 20 years? In order to answer this question, this chapter is organized in the following sections; a) explanation of the concept of cyberspace, b) categorization of the concepts of cybersecurity and cyberdefense in Colombia, c) identification of public cybersecurity policies in Colombia, and d) description of the architecture of the System in Colombia.

Key words: Security, Cyberspace, Cybersecurity, Cyberdefense.

Sumario. 1. *Introducción*. 2. *El concepto de Ciberespacio*. 3. *Concepto de Ciberseguridad en Colombia*. 4. *Concepto de Ciberdefensa en Colombia*. 4.1. *Hackers*. 4.1.1. *Hacktivistas*. 4.1.2. *Actores no estatales*. 4.1.3. *Grupos terroristas*. 4.1.4. *Infiltrados*. 5. *Política pública de Ciberseguridad en Colombia*. 5.1. *El Consejo Nacional de Política Económica y Social: CONPES 3701/11 y 3854/16*. 5.1.1. *CONPES 3701 del 2011*. 5.1.2. *CONPES 3854 del 2016*. 5.1.3. *Plan Nacional de Desarrollo 2014-2018*. 5.1.4. *Política de Seguridad del Ministerio de Defensa Nacional 2015-2018*. 6. *Arquitectura del sistema en Colombia*. 6.1. *Fuerzas Militares de Colombia*. 6.1.1. *Comando Conjunto Cibernético*. 6.2. *Policía Nacional de Colombia*. 6.3. *Sector Privado*. 7. *Conclusiones*.

1. Introducción

Hoy Colombia se enfrenta a una nueva era de transformación de las relaciones sociales, económicas y políticas a raíz del desarrollo de nuevas tecnologías de la información y comunicación, producto de los procesos de globalización e inserción del país a la esfera internacional. Este un proceso inevitable de liberalización de todos los ámbitos sociales, pero también necesario por la interdependencia de actores que confluyen en las diferentes esferas.

Dicho esto, hoy por hoy en el escenario nacional e internacional un nuevo espacio de dominio de Quinta Generación lejos de control estatal y de cualquier regulación normativa

internacional emerge con ímpetu y potencial para ser, por lejos, un espacio de trasformación social: el ciberespacio. No obstante, todo escenario está sujeto a actores que desarrollan dinámicas o actividades legales como ilegales y, por tanto, emergen de este escenario nuevas amenazas.

En el caso particular de Colombia, la implementación de nuevas tecnologías a finales de los años 90 ha significado el surgimiento de nuevos actores que se encuentran inmersos en el ciberespacio, nuevas amenazas que realizan actividades ilegales en contra de la seguridad de los usuarios e intereses nacionales. A estas acciones hostiles se les conoce como ciberataques.

Ejemplo de lo anterior se evidencia con el sistemático aumento del cibercrimen en el país. Entre los delitos que registran mayor aumento se encuentran la estafa por suplantación, el tráfico de datos financieros personales, el fraude y los ciberataques a entidades privadas y gubernamentales (Policía Nacional de Colombia, 2016). Por otra parte, existen sectores económicos, industriales y del gobierno que, por su alto valor e importancia estratégica para el desarrollo nacional, se convierten en blancos para las nuevas amenazas, debido a que estos cada vez implementan nuevas tecnologías de información y de comunicación, lo cual hace que sean más vulnerables. Estos sectores hacen de una red de infraestructura crítica nacional vulnerable.

En consecuencia, de lo anterior, cabe plantearse: ¿Cómo ha evolucionado la estrategia de ciberseguridad y ciberdefensa en Colombia en los últimos 20 años? Para dar respuesta a lo planteado, el presente documento se organiza en los siguientes apartados: a) explicación del concepto de ciberespacio, b) categorización de los conceptos de ciberseguridad y ciberdefensa en Colombia, c) identificación de las políticas públicas de ciberseguridad en Colombia, y d) descripción de la arquitectura del Sistema en Colombia.

2. El Concepto de Ciberespacio

Actualmente nos encontramos en un mundo globalizado donde el acceso a nuevas tecnologías hace parte del quehacer humano, debido a que en estas el factor Espacio-Tiempo no representa un impedimento. Este proceso de innovación iniciada en el siglo XX se conoce como Revolución Tecnológica (en adelante: RT), entendida según Castell (1997), como un proceso donde convergen en su núcleo dos aspectos para la innovación del procesamiento del conocimiento y su aplicación: la información y la comunicación.

A diferencia de otras revoluciones como la Revolución Industrial (1760-1840) iniciada en Reino Unido, la RT aplica de manera inmediata el acceso a las tecnologías que en esta se generan, buscan enlazar en un principio al mundo a través de la información (Castell, 1997). En esta medida, la tecnología de la información[26] trastoca cada vez más aspectos de la actividad humana, generando que dicha dependencia sea cada vez más ineludible. A estas nuevas sociedades se les conoce como Sociedad de la información.

Por otra parte, el sistema de comunicación en la era de la globalización juega un papel imperante. Según Hugo Fazio (2001), los alcances de la globalización se evidencian en la expansión de comunicaciones y la aparición de referentes culturales mundiales, en una suerte de cultura mundo. Dicho sistema de comunicación genera estructuras sociales que producen su propio lenguaje, sonidos e imágenes.

Actualmente, el mundo se encuentra en un nuevo escenario, un nuevo tipo de domino no físico donde se entablan y desarrollan dinámicas sociales, económicas y políticas, fuera del alcance de

26 Se entiende por tecnologías de la información a todos aquellos aspectos relacionados a la microelectrónica, la informática y las telecomunicaciones (Castell, 1997).

toda norma internacional o algún tipo de regulación estatal. Este nuevo escenario se conoce como ciberespacio. Según Kuehl, el ciberespacio se entiende como "un dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar información a través de redes sistemas de información e infraestructuras físicas" (Capitulo 2, 2009). En dicho escenario, convergen múltiples actores de diferentes partes del mundo, quienes interactúan libremente y fuera de cualquier tipo de restricción normativa, cultural y espacial.

A lo anterior, cabe preguntar ¿Por qué el ciberespacio representa una amenaza a la seguridad y defensa del Estado? En respuesta, se puede señalar que una de las grandes paradojas de la globalización se asocia a los principios del liberalismo contemporáneo, donde cada vez el Estado pierde su protagonismo. Al respecto, Gilbert Larochelle (2004), manifiesta que las interacciones locales y globales trasforman los marcos de racionalidad frente al entendimiento de lo público y lo privado, desafiando las tradicionales formas de control social, en una suerte de disolución de las jerarquías estructurales. Ejemplo de lo anterior es el protagonismo cada vez mayor de las subculturas que resisten cada vez más al poder legal del Estado, hecho que se materializa en activismo social y, por ende, el ciberespacio, un dominio fuera del alcance del poder estatal, se convierte en un punto de convergencia.

Por otra parte, existen actores asimétricos tradiciones que aprovechan el nuevo dominio y sus características lejanas a cualquier tipo de control legal para generar acciones contra el Estado, considerando la dependencia institucional cada vez más fuerte referente al uso de las nuevas tecnologías e innovaciones digitales, lo cual implica una alta vulnerabilidad en cuanto a seguridad se refiere.

El nuevo escenario de dominio al cual se hace referencia corresponde al escenario de Quinta Generación. En la actualidad, existen cinco dominios de la guerra: tierra, agua, aire, espacio exterior o ultraterrestre y ciberespacio. Los cuatro primeros son reales y físicos, por ende, existen Fuerzas, cuerpos armados de seguridad que se especializan en cada escenario (Ejército, Armada y Fuerza Aérea-espacial), mientras que, en el quinto escenario de dominio relativamente nuevo, hasta el momento se están configurando las bases de un cuerpo de seguridad.

Con respeto a lo anterior, José Casar (2012) afirma la existencia una serie de características propias del ciberespacio que resultan convenientes señalar: a) En el entorno único ofrecido por este escenario es imposible detectar el origen de cualquier ataque; b) En la defensa intervienen factores públicos y privados que coordinan estrechamente; c) Las características de confrontación son propias de una confrontación asimétrica; d) No es necesaria la destrucción para la obtención de información de los objetivos; e) El chantaje como la disuasión son herramientas válidas y aplicables al mismo tiempo; y f) El escenario evoluciona siguiendo la innovación de las Tecnologías de la Información y la Comunicación.

3. El Concepto de Ciberseguridad en Colombia

A finales de los años 90, se registraron los primeros ciberataques en Estados Unidos (En adelante EE.UU.). Precisamente, en 1998, se generaron 6 ataques, frente a 82.094 ataques registrados para el año 2002 (Molist, 2003). Según Richard Pethia, director del CERT Coordination Center en 1998, un centro de coordinación mundial creado en el Instituto de Ingeniería de Software en Pensilvania, los aumentos de los ataques responden a la cobertura descentralizada de nuevas tecnologías (Molist, 2003).

En el caso particular de Colombia, a partir del año 2002, el país avanzó en la implementación de una serie de reglamentaciones para el cuidado y protección de la información personal, motivada por la implementación de las nuevas Tecnologías de la Información y la Comunicación (En adelante: TIC). Estas acciones guiadas por la necesidad de establecer un ambiente de seguridad para la información frente a los casos registrados a nivel internacional.

No obstante, fue en el año 2009 cuando se sanciona la Ley 1273 de 2009 denominada "de la protección de la información y de los datos" (Ley 1273, 2009). Entre los alcances más significativos se encuentra la reestructuración del Ministerio de Comunicaciones, el cual pasó a ser llamado Ministerio de Tecnologías de la Información y las Comunicaciones (En adelante: MINTIC). Dicha reestructuración mantiene como objetivo, hasta el día de hoy, atender las necesidades resultantes de los cambios producidos por las tecnologías (Ministerio de Tecnologías de la Información y las Comunicaciones, s.f).

En esta medida, se puede definir que la ciberseguridad, en el caso colombiano, se entiende como el conjunto de herramientas, sugerencias y medidas que permite al Estado proteger su integridad, disponibilidad y confidencialidad de la información (Cáceres, 2017).

Actualmente, se evidencia un nuevo panorama de amenazas operantes en el ciberespacio, actores que representan riesgos para las organizaciones y la sociedad en su conjunto, debido a los impactos reales de sus acciones (MINTIC, 2014). Según el MINTIC, el Estado requiere:

> Plantear estrategias e iniciativas que minimicen la posibilidad de que estos nuevos riesgos se hagan efectivos, que eviten que los ciudadanos, los sectores productivos y el Estado en general se

> vean afectados, y que con esto se altere la forma de organización social, económica, política soberana y coercitiva del país. (2014, p. 4)

Uno de los ataques más relevantes registrados en los últimos 5 años, fue el provocado en 2017 con el virus extorsionador WannaCry, un virus que utilizaba como modalidad el secuestro de información con el objetivo de pedir rescate a cambio de sumas de dinero. Este ataque a gran escala paralizó entidades públicas y privadas alrededor del mundo, incluso sus estragos se registraron en Colombia.

Según la plataforma NORSE, una plataforma que identifica y registra los ciberataques alrededor del mundo en tiempo real, Colombia es el tercer país con más ataques registrados por minuto en Latinoamérica, después de Brasil y Argentina. En comparación con otros países a nivel mundial, Emiratos Árabes Unidos es el país con mayor recepción de ataques por minuto, siendo la ciudad de Dubái uno de los blancos más llamativos. Con respeto a los países donde se originan los ciberataques, la lista la encabeza China, donde la mayoría de sus ataques tienen como destino EE.UU. y la Unión Europea (NORSE, s.f).

4. El Concepto de Ciberdefensa en Colombia

Si bien es difícil identificar el origen de la mayoría de los ciberataques realizados alrededor del mundo, lo que sí se puede afirmar es que estos ataques no solo amenazan la seguridad del sistema de información nacional, sino que implican una amenaza para la defensa nacional, debido a que la mayoría de los ataques se originan en suelo extranjero y buscan, en algunos casos, afectar la infraestructura critica del Estado.

Se entiende como infraestructura critica, a saber:

> Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas. (Sánchez, 2011, Párrafo 1).

En el año 2013, el S2 Grupo, una empresa especializada en ciberseguridad, publicó un informe donde se identifican 12 sectores estratégicos o infraestructura critica vulnerable para cualquier Estado, entre los cuales se encuentran: administración pública, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, Tecnologías de la Información y las Comunicaciones (TIC), transporte, alimentación, y sistema financiero y tributario (Villalón y Marín, 2013).

Dichos sectores tienen una alta vulnerabilidad, debido a que se encuentran articulados a una red de información vulnerable a ciberataques, sin desconocer que hacen parte de una compleja red de instalaciones que posibilitan el funcionamiento de la sociedad. Por lo tanto, la defensa de dicha estructura crítica frente a amenazas provenientes del ciberespacio, donde se originan los ataques, hace parte de los objetivos del Estado, particularmente de las Fuerzas de Seguridad.

Al respecto, la defensa de los intereses en el ciberespacio se conoce como ciberdefensa, esta entendida como:

> Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones,

> investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (Hernández, 2016).

Ahora bien, es necesario puntualizar cuáles son las amenazas que convergen en el ciberespacio. Para ello, Emilio Iasielo (2013), un experto analista de amenazas cibernéticas, clasificó las amenazas provenientes del ciberespacio en 5 grupos:

4.1. Hackers.

Son conocidos como piratas cibernéticos, actores que penetran redes de información con objetivos particulares. Estos se caracterizan por tener un grado de destreza y conocimiento informáticos para llevar a cabo operaciones cibernéticas contra diferentes blancos, bien sea de manera individual o simultáneamente.

4.1.1. Hacktivistas.

A diferencia de los hackers, estas categorías de individuos son motivados por una política o ideología para establecer sus blancos. Se caracterizan porque la mayoría de los ataques tienen como objetivo la negación del servicio; no por eso se consideran menos peligrosos.

4.1.2. Actores no estatales.

Aunque pueden estar relacionados con hackers, esos se caracterizan por que la mayoría de ataques son producto de

un espionaje cibernético para recopilación de algún tipo de información confidencial. Asimismo, las operaciones realizadas por esos actores son producto de acciones de inteligencia previas sobre sus blancos.

4.1.3. Grupos terroristas.

Este tipo de categoría se encuentra en auge, debido a que cada vez más grupos considerados terroristas están haciendo uso de tecnologías informáticas, principalmente para el reclutamiento, la difusión de propaganda, la provocación, la planificación de operaciones, etc.

4.1.4. Infiltrados.

Esta categoría es diferente a las anteriores debido a que los actores deben infiltrarse y promover el acceso a las redes o sistemas de información. Sus acciones se caracterizan por que buscan interrumpir, destruir o manipular.

Según Iasielo (2013), la última categoría es la fuente principal de los delitos cibernéticos. Asimismo, los volúmenes de los ciberataques varían según los intereses particulares de actor, precisamente dependen de las capacidades y recursos con las que cuenten los actores.

En resumen, Colombia enfrenta grandes desafíos en materia de seguridad cibernética por la implementación de nuevas tecnologías de la información y de las comunicaciones. Por ello, se hace necesaria una estrategia de ciberdefensa para la protección de intereses estratégicos nacionales, particularmente acciones interinstitucionales articuladas para la defensa de la infraestructura crítica vulnerable a amenazas provenientes del ciberespacio.

Por lo tanto, Colombia debe establecer una estrategia de contención de las amenazas cibernéticas para la defensa de la infraestructura crítica mediante la actualización permanente de las políticas públicas relacionadas al manejo de la información y telecomunicaciones. Esta estrategia debe contemplar la acción conjunta de las diferentes instituciones de seguridad para el control y regulación del ciberespacio hasta donde los medios y recursos lo permitan.

5. Política pública de ciberseguridad en Colombia

Las políticas públicas son acciones y herramientas del Estado para brindar respuestas a situaciones concretas sociales, con las cuales se busca definir, inducir y/o modificar un orden en un espacio social particular operante (Roth, 2018). Para André Roth (2018), la política pública parte de la concepción de un Estado de derecho el cual comprende "la adopción de una reglamentación jurídica autoriza y legitima la implementación de su estrategia" (p. 34). Por tanto, la definición de estrategias implica la movilización de ciertos recursos, actores públicos y privados.

Dicho lo anterior, y como ya se había mencionado, las primeras regulaciones frente a los sistemas de información y comunicación se materializan con la Ley 1273 de 2009, referente a la protección de la información y de los datos (Ley 1273, 2009). Entre los aspectos más relevantes se encuentra la reestructuración del hoy conocido MINTIC. Sin embargo, es la Ley 1341 de 2009 la que establece las funciones del ministerio, y entre las cuales se pueden destacar el diseño, la adopción y promoción de las políticas, programas, planes y proyectos referentes al sector de las Tecnologías de la Información y las Comunicaciones (MINTIC, s.f).

Actualmente, el MINTIC se articula con otras instituciones del Estado como el Ministerio de Defensa Nacional (En adelante: MDN), el Departamento Nacional de Planeación, el Consejo Nacional de Política Económica y Social, entre otras instituciones, para coordinar políticas, normas, procedimientos y estándares relacionados con la ciberseguridad y la ciberdefensa. A continuación, se identifican algunas de las políticas públicas referentes al manejo del ciberespacio.

5.1. El Consejo Nacional de Política Económica y Social: CONPES 3701/11 y 3854/16.

Los CONPES son documentos proferidos por el Consejo Nacional de Política Económica y Social -CONPES-, el máximo organismo asesor del Gobierno Nacional creado en 1958 para coordinar y orientar proyectos de desarrollo económico y social en el país (Departamento Nacional de Planeación, s.f). Hasta la fecha, el Consejo Nacional de Política Económica y Social ha proferido dos documentos referentes al fenómeno en cuestión: CONPES 3701 del año 2011 y el CONPES 3854 del año 2016.

5.1.1. CONPES 3701 del año 2011.

Para el año 2011, se establecen los lineamientos de la política en ciberseguridad y ciberdefensa mediante el CONPES 3701 del 2011. El fin último del documento es contrarrestar las amenazas cibernéticas que atentan contra el país mediante una serie de recomendaciones a las entidades involucradas para la aplicabilidad de una estrategia de prevención y control, además de identificar las fortalezas y debilidades de las capacidades con la que cuenta el país (CONPES, 2011).

De los apartados encontrados en el documento se destacan tres aspectos claves de la estrategia: primero, la implementación

de iniciativas para prevenir, coordinar, atender, controlar y regular los incidentes o emergencias cibernéticas; segundo, el aumento de capacitación especializada en seguridad de la información, buscando ampliar las líneas de investigación sobre los aspectos relacionados con la ciberdefensa y ciberseguridad; y tercero, buscar el fortalecimiento de la legislación nacional en materia de ciberseguridad y ciberdefensa, haciendo uso de la cooperación internacional y de los diferentes instrumentos internacionales relacionados con el problema en cuestión.

Producto de CONPES se estableció el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (en adelante; ColCERT), el cual tiene el objetivo la coordinación de acciones necesarias para la protección de la infraestructura critica: el Comando Conjunto Cibernético, integrado por el Ejército Nacional de Colombia, la Armada Nacional de Colombia y la Fuerza Aérea de Colombia; y el Centro Cibernético Policial (CONPES, 2011).

5.1.2. CONPES 3854 del año 2016.

Un segundo documento se realizó en el año 2016. El CONPES 3854 estableció la Política Nacional de Seguridad Digital con el objetivo de identificar, gestionar, tratar y mitigar los riesgos de las amenazas sobre las actividades socioeconómicas en el entorno digital (CONPES, 2016).

Continuando con lo establecido en el documento anterior, el nuevo CONPES profundizó en la estrategia para la ciberseguridad y ciberdefensa. Entre los apartados a destacar se encuentran: primero, el establecimiento de un marco institucional para la seguridad digital; segundo, la creación de una serie de condiciones para que los actores y/o partes interesadas gestionen el riesgo de seguridad digital; tercero, el fortalecimiento de la seguridad de los individuos y del Estado en el entorno digital; cuarto, el fortalecimiento de la defensa y soberanía nacional en el

entorno digital; y quinto, la gestión de mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital. Todos los apartados, y en general la estrategia, articulados a un enfoque de gestión de riesgos (CONPES, 2016).

Entre las sugerencias del documento se destaca la integración interinstitucional del Departamento Administrativo de la Presidencia, el Ministerio de Educación Nacional, el Ministerio del Interior, el Ministerio de Justicia y del Derecho, el Ministerio de Relaciones Exteriores, el Departamento Administrativo Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación, recomiendan al Consejo Nacional de Política Económica y Social (CONPES, 2016).

Los mencionados documentos CONPES establecieron las bases de una serie estrategias conjuntas e interinstitucionales para la seguridad y defensa de las amenazas provenientes del ciberespacio, destacando el interés gradual de las demás instituciones para generar una coordinación conjunta en cuanto a la implementación de nuevas tecnologías.

En consecuencia de lo anterior, hoy podemos encontrar cada vez una mayor coordinación en los diferentes niveles del gobierno en una suerte de consolidación de una "cultura estratégica"[27] en materia de seguridad y defensa nacional.

5.1.3. Plan Nacional de Desarrollo 2014-2018.

Una de las características del Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país" es la implementación

27 Se refiere a una serie de costumbres, valores, formas, hábitos, creencias y prácticas de una organización o institución.

de nuevas tecnologías, el uso responsable y el aumento de las mismas a lo largo del territorio colombiano. Por lo tanto, una de las preocupaciones del gobierno, justamente como se menciona en el documento, es mitigar los riesgos por las trasformaciones sociales, económicas, y políticas producto de la implementación de nuevas tecnologías y su dependencia (Departamento Nacional de Planeación, 2015b).

Entre los objetivos propuestos en el Plan Nacional de Desarrollo 2014-2018 (en adelante: PND) para el MINTIC, se encuentra enmarcada en la estrategia de fortalecimiento de los roles del Estado, precisamente en el objetivo relacionado con la seguridad y defensa en el territorio nacional (Departamento Nacional de Planeación, 2015a). En este se establece la Estrategia Nacional de Ciberseguridad, la cual busca obtener las ventajas que brinda el entorno digital. Para ello, se busca el fortalecimiento de seguridad cibernética mediante la consolidación del grupo ColCERT, la creación de un Observatorio del Ciberdelito y del Centro de Mando y Control, Centros de Respuesta Cibernética –CSIRT-, el fortalecimiento de los activos digitales a través de las Fuerzas Militares y la Policía Nacional (DNP, 2015a).

Asimismo, el PND se busca el respeto de la soberanía nacional y la protección de los intereses nacionales en los diferentes escenarios de dominio (terrestre, marítimo, fluvial, aéreo, espacial y ciberespacial). Para lo anterior, se precisa el fortalecimiento de las capacidades en ciberdefensa (DNP, 2015a).

5.1.4. Política de Seguridad del Ministerio de Defensa Nacional 2015-2018.

La Política de Seguridad del Ministerio de Defensa Nacional 2015-2018 "Todos por un nuevo país" establece los lineamientos de la política de defensa y seguridad enfocada a la consolidación de la paz en el escenario de posacuerdo. Con respecto al nuevo

escenario, se manifiesta el fortalecimiento de la lucha de fenómenos criminales en el sector urbano, especialmente contra delitos como el homicidio, el microtráfico, la microextorsión, la extorsión, el secuestro y, claramente, los ciberdelitos (Ministerio de Defensa Nacional, 2015).

Una característica de Política de Seguridad del Ministerio de Defensa Nacional es la toma de ciberespacio como eje trasversal, debido a que en cada uno de los apartados se mantiene como primicia el fortalecimiento de la ciberseguridad a raíz de la consolidación de las nuevas tecnologías, recursos digitales e informáticos que son utilizados cada vez más por los delincuentes quienes tienen como objetivo atentar contra el patrimonio económico de empresas e individuos.

Son varios los beneficios del empleo de las tecnologías digitales por parte de los criminales. En principio, el ciberespacio ofrece, entre otras cosas, el anonimato de las acciones, el empleo de bajos recursos materiales, humano y económico y, sobre todo, la infinidad de modalidades delictivas que se encuentran fuera de la regulación y control de las autoridades. En 2017, la Dirección de Investigación Criminal e Interpol –DIJIN-, manifestó el incremento del cibercrimen en un 28%, cifra que representó pérdidas económicas cercanas a 50.000 millones de pesos ("El cibercrimen en […]", 2017).

En resumen, Colombia se encuentra en la consolidación de una estrategia de prevención y control de las amenazas provenientes del ciberespacio mediante políticas públicas interinstitucionales encaminadas al fortalecimiento de la ciberseguridad y ciberdefensa durante los últimos 10 años. Esto a raíz de la sistemática implementación de nuevas tecnologías de la información y comunicación. En consecuencia, el Estado ha optado por conformar, estructurar y direccionar a un conjunto de instituciones competentes en el tema de ciberespacio para afrontar los nuevos desafíos y amenazas que, en términos

estadísticos, seguirán posiblemente en aumento en la medida en que la red de tecnología siga creciendo.

6. Arquitectura del sistema en Colombia

Hasta este punto, se ha realizado una aproximación conceptual de los conceptos ciberseguridad y ciberdefensa en Colombia y cómo estos han generado una serie de políticas públicas motivadas por una estrategia hacia la prevención de las amenazas provenientes de un campo de dominio de Quinta Generación relativamente nuevo para las autoridades del Estado.

En este sentido, y profundizando un poco más con el tema tratado en el aparatado anterior, a continuación se realiza una breve descripción de la arquitectura institucional que orienta, coordina y ejecuta los lineamientos establecidos para la seguridad y defensa del ciberespacio en Colombia.

6.1. Fuerzas Militares de Colombia.

6.1.1. Comando Conjunto Cibernético.

El Comando Conjunto Cibernético (en adelante: CCOC), mediante la Resolución 7436 del MDN, es el responsable de la ciberseguridad en Colombia. En este comando, participan todas las Fuerzas Militares para la ciberdefensa de la infraestructura critica nacional frente a amenazas: la Dirección de Seguridad Cibernética del Ejército Nacional, Dirección de Ciberdefensa Fuerza Aérea Colombiana y la Unidad Cibernética de la Armada de la República de Colombia que, coordinadas con la Unidad de Gestión General -UGG- del MDN y el Grupo Social y Empresarial de la Defensa –GSED-, se articulan para orientar, detectar, observar, prevenir, contener, decidir, responder y mejorar todo aquello relacionado con el sistema general de ciberdefensa (Siegert, 2015).

Entre las capacidades operativas del comando, se encuentra la gestión de eventos de seguridad de la información, la respuesta en línea a incidentes de ciberseguridad, visibilidad y análisis de tráfico en tiempo real, la protección de bases de datos, la protección de portales web, el análisis de malware, la implementación de esquema de protección de intrusos, el análisis de vulnerabilidades y el análisis forense (Henao, 2016).

Referente a la protección de infraestructura critica, el CCOC estableció un comité ejecutivo que se reúne para debatir aspectos relacionados con las amenazas y ciberdefensa. En este comité, participan representantes de sector eléctrico, financiero, gobierno, tecnologías de la información y la comunicación y defensa (Henao, 2016).

6.2. Policía Nacional de Colombia.

El Centro Cibernético Policial (en adelante: CCP) es una unidad encargada de investigar el cibercrimen, es decir, todos aquellos delitos generados en el ciberespacio como fraudes, extorsiones, sabotaje, robo de información, interceptaciones, entre otros delitos. Actualmente, el Centro cuenta con cuatro grandes grupos: el primer grupo de investigación referente a delitos financiaros –GIDAT-, el segundo grupo de investigación referente a delitos ciberterroristas –GICIB-, el grupo de investigación referente a delitos pornográficos infantiles –GRUPI-, y el cuarto grupo relacionado con el manejo de la plataforma virtual de denuncias (CAI Virtual), el cual coordina los reportes y denuncias con los grupos de investigación (Policía Nacional de Colombia, 2016).

En el informe del año 2017 realizado por el CCP, se confirma el aumento del cibercrimen en un 28% en relación con el año anterior. Entre los delitos se encuentran ciberinducción, (tipo de delito que incita al daño físico), estafa por suplantación, tráfico de datos financieros personales, estafas, ciberpirámides y ataques gubernamentales.

Para finalizar, desde el año 2016, se encuentra en construcción el Centro de Comando y Control para la Ciberseguridad en Colombia. Se espera ampliar las capacidades con que cuenta la Policial Nacional de Colombia para combatir el cibercrimen. Se espera que este centro entre en operación a finales del 2018 (Policía Nacional de Colombia, 2016).

6.3. Sector Privado.

La Cámara Combinada de Informática y Telecomunicaciones (en adelante: CCIT) es una entidad del sector privado fundada en 1993. Esta entidad agrupa a empresas del sector de la informática y telecomunicaciones para promover el crecimiento acelerado y sostenible del sector TIC en coordinación con entidades del Estado (CCIT, s.f).

Para el año 2017, la CCIT estableció una estrategia encaminada a fortalecimiento de la política pública TIC, fomento de la legalidad, generar estabilidad jurídica, incentivar la inversión y trasformación digital (CCIT, s.f).

Esta entidad privada, de la mano con el CCP, publicó un informe conjunto realizado en el año 2017. En este informe se destacan tres puntos importantes: 1) el incremento en el año 2016 de ataques de malware; se registró un aumento cercano del 114 %; 2) se registraron cerca de 13.774 denuncias por violación a la ley de protección de datos entre los años 2014 y 2017; y 3) se registró la captura en el año 2016 de 18 ciudadanos de nacionalidades extranjeras, dejando una pérdida total por ciberataques en ese mismo año de $130 mil dólares (CCIT, 2017).

Por otra parte, se encuentra el Grupo Social y Empresarial de la Defensa (en adelante: GSED), una organización que agrupa 18 entidades, entre las cuales se encuentran:

> 8 Establecimientos Públicos, 3 Sociedades de Economía Mixta, 2 Entidades Industriales y Comerciales del Estado, 2 Entidades Descentralizadas Indirectas, 1 Superintendencia con personería jurídica, 1 Entidad Privada sin Ánimo de Lucro y 1 Entidad Dependencia del Ministerio de Defensa Nacional. (GSED, s.f., párrafo 1)

El GSED tiene como objetivo orientar y dirigir el fortalecimiento de las empresas que la componen en tres ámbitos: el apoyo logístico, el apoyo a la seguridad y el bienestar, con el fin último de que las empresas sean modernas, eficientes y competitivas (GSED, s.f).

7. Conclusiones

La Revolución Tecnológica, impulsada por la globalización, ha generado que el mundo inicie una era de digitalización del trabajo, de la información y de la comunicación, todo esto ha significado la transformación de las relaciones sociales, políticas y culturales, pues el mundo contemporáneo en que vivimos cada vez se inclina al desarrollo de nuevas tecnologías, particularmente el desarrollo e innovación del sector relacionado con la información y de la comunicación, aspectos que marcan una fuerte dependencia digital. En consecuencia, nuevos actores y amenazas convergen en un escenario lejos de los alcances del control de cualquier Estado.

Al respecto, Colombia se encuentra en la consolidación de una estrategia de prevención y control de las amenazas provenientes del ciberespacio mediante políticas públicas interinstitucionales encaminadas al fortalecimiento de la ciberseguridad y ciberdefensa, optando por conformar, estructurar y direccionar a un conjunto de instituciones competentes en el tema de ciberespacio.

Si bien hoy el país evidencia un aumento sistemático del crimen organizado y de las amenazas a medida de la implementación de las nuevas tecnologías, cabe resaltar que existen grandes esfuerzos estatales para afrontar las nuevas amenazas materializadas a través de políticas públicas. En este sentido, Colombia debe continuar en sus esfuerzos por fortalecer los campos ciberdefensa y ciberseguridad, con el objetivo de proteger al país y a las instituciones de los delitos producto de las nuevas amenazas transnacionales de la Quinta Generación. El Ministerio de Defensa, las Fuerzas Armadas y la Policía deben continuar trabajando conjuntamente en la protección de la seguridad y las libertades cibernéticas de los ciudadanos y la nación, para defender a los colombianos de delitos como el fraude electrónico, las estafas por suplantación, el hacking, entre otros.