Los Grupos Armados Organizados y los sistemas de amenaza persistente, como amenazas cibernéticas en el siglo XXI

Harold Enrique Cabrera Cornelio
Pinzón Diomedes Guzmán A.
Guillermo Eduardo Nova Gómez
Jayson Armando Parra Rojas

Trabajo de grado para optar al título profesional:
Especialización en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2017

TRABAJO DE GRADO

"LOS GRUPOS ARMADOS ORGANIZADOS Y LOS SISTEMAS DE AMENAZA PERSISTENTE, COMO AMENAZAS CIBERNÉTICAS EN EL SIGLO XXI"

BOGOTÁ – COLOMBIA
NOVIEMBRE 2017

Trabajo de grado presentado para obtener el titulo de:

Especialista en Seguridad y Defensa Nacional
ESCUELA SUPERIOR DE GUERRA

MY. HAROL ENRIQUE CABRERA CORNELIO
MY. GUZMÁN A. PINZÓN DIOMEDES
MY. GUILLERMO EDUARDO NOVA GÓMEZ
MY. JAYSON ARMANDO PARRA ROJAS

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Jurado

_____

Jurado

En Honor a Dios por permitirnos estar aquí.

A la Escuela Superior de Guerra por brindarnos la oportunidad de terminar la especialización.

A nuestras familias por su apoyo incondicional.

A cada uno de nuestros docentes que aportaron a nuestra formación

Agradecimiento sincero a la Señora Mayor MILENA ELIZABHET REALPE DIAZ Jefe de Prospectiva del Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia quien por acompañamiento, su apoyo irrestricto durante el desarrollo de esta investigación y trabajo de grado nos ayudó a concluirlo y llevándolo a feliz término.

También profundo agradecimiento al Doctor PEDRO BUITRAGO RINCÓN por su constante seguimiento y orientación sin el cual no hubiese sido posible la consolidación y materialización de este trabajo.

Contenido

Los Grupos Armados Organizados y los Sistemas de Amenaza Persistente como amenazas cibernéticas para el Estado colombiano en el siglo XXI

MY. Jarol Cabrera C.
MY. Diomedes Guzmán P.
MY. Guillermo Nova G.
MY. Jayson Parra R.

Resumen:

El presente artículo pretende aportar al desarrollo de las estrategias del Estado y de las Fuerzas Armadas colombianas, para mitigar las amenazas que representan los Sistemas de Amenaza Persistente (SAP) y los Grupos Armados Organizados (GAO) en el ciberespacio, por lo cual, se propone abordar el ciberespacio en distintos frentes que deben responder a los cuatro niveles principales que componen este campo. Para ello, se analiza el concepto de ciberespacio en términos estratégicos, también se presentan las tendencias mundiales en cuanto a la acción estatal al respecto a la ciberseguridad y la ciberdefens. En adición, se exponen las capacidades que poseen las Fuerzas Armadas para la defensa del ciberespacio haciendo énfasis en el ordenamiento jurídico existente en el país al respecto del ciberespacio.

Palabras clave:

Ciberespacio, Ciberseguridad, Ciberdefensa, GAO, SAP, Colombia, Ciberamenaza.

Abstract:

The next paper pretends to contribute to the improvement of the Colombian Government and The Colombian Armed Forces strategies to mitigate the threats that the Advanced Persistent Threats (APT) and Organized Armed Groups (GAO) represent to that end, it is proposed to address the cyberspace in different fronts each of one must be related to the four different levels that compose the cyberspace. To that purpose, the concept of cyberspace is analyzed from a theoretical perspective, also the global trends regards the governmental action regarding

cybersecurity and cyberdefense are presented. In addition, the capabilities that the Armed Forces have for the defense of the cyberspace are lay out, emphasizing in the internal legal system.

Keywords:

Cyberspace, Cybersecurity, Cyberdefense, GAO, APT, Colombia, Cyberthreat.

1. Introducción

El avance y el crecimiento exponencial de la tecnología en los últimos años han conducido a cambios drásticos en la sociedad actual y en la forma en la que interactúan los actores dentro de esta. Tal proceso impone retos de gran complejidad en todas las áreas de acción de las instituciones y organizaciones, tanto estatales como privadas que, sin lugar a duda, tienen dificultades al momento de responder a los problemas al mismo ritmo que estos surgen.

En este sentido, el presente texto se propone estudiar la acción estatal al respecto del ciberespacio, centrándose en las amenazas que los Sistemas de Amenaza Persistente (en adelante: SAP) y, específicamente, los Grupos Armados Organizados (en adelante: GAO), representan para el Estado colombiano. Lo anterior se hace con el fin de aportar al desarrollo de las estrategias en torno al cibercrimen, y de impulsar el posicionamiento de Colombia como actor clave en la ciberseguridad y la ciberdefensa en el ámbito internacional. De este modo, con este trabajo se busca sustentar que el Estado colombiano, así como las fuerzas armadas, debe abordar el ciberespacio en distintos frentes que deben responder a los cuatro niveles principales que componen este campo.

Para tal fin, el presente trabajo se desarrolla a partir de cuatro núcleos: el primero tiene como objetivo sentar las bases teóricas sobre las cuales se erigirá el análisis y también analiza las tendencias mundiales en cuanto a las estrategias puestas en práctica por otros actores, y con esto, mostrar en el segundo núcleo las repercusiones que las amenazas cibernéticas tienen en

Colombia. De esta manera, el tercer y cuarto núcleo, tienen como objetivo exponer las capacidades que poseen las fuerzas armadas para la defensa del ciberespacio enfatizando en el ordenamiento jurídico existente en el país al respecto del ciberespacio.

Por último, a modo de conclusiones del proceso investigativo, se realizan unas recomendaciones especiales para cada falencia encontrada al respecto de la mitigación de los GAO y los SAP como amenazas cibernéticas.

2. Importancia del ciberespacio, la ciberseguridad y la neutralización de amenazas

Para empezar, es necesario aclarar que la manera en que se han abordado las amenazas y las estrategias de ciberseguridad con respecto a los GAO y los SAP, implican, en primer lugar, definir el espacio de interacción entre estos actores y el Estado: el ciberespacio, y con ello profundizar sobre el desarrollo del concepto de ciberseguridad. En segundo lugar, requiere examinar cómo se han definido las amenazas en el campo de la ciberseguridad en general, haciendo énfasis en los actores mencionados; de tal forma que, en tercer lugar, se identifican las estrategias concebidas en el ámbito académico, así como las tendencias llevadas a cabo por los diferentes países alrededor del mundo.

La conceptualización de ciberespacio es de suma importancia para abordar de manera asertiva los problemas que surjan dentro del mismo; no obstante, elegir una definición de ciberespacio no es tarea simple, ya que en este se conjugan diversos niveles de abstracción. Este concepto puede ser definido a priori como todo lo que se pueda ver en un teléfono inteligente, o un computador conectado a internet (Whittaker, 2004, p. 20), y se puede argüir que por su sencillez gran parte de la población tiene esta noción del concepto.

Sin embargo, el ciberespacio se constituye en más que la combinación entre hardware e internet, ya que el ciberespacio no solo es la red de nodos y redes que tienen su base en varios computadores conectados a través de distintos medios (Whittaker, 2004, p.21), porque en estas redes se forman lugares simbólicos en dónde las personas pueden construir nuevos mundos (Bell, 2001, p. 7), y en donde los cuestiones como la privacidad, la seguridad, los delitos y la guerra adquieren nuevas connotaciones (Abebe, 2016).

Lo anterior, abre la puerta a una multiplicidad de definiciones que pueden hacer el concepto ininteligible y ambiguo, pese a esto, dentro de la literatura académica se encuentran diversas formas de categorizar las definiciones de ciberespacio, una de las primeras caracterizaciones contempla tres órdenes o niveles de complejidad (Strate, 1999, 384): Un nivel cero o de ontología de ciberespacio, un primer nivel de *bloques de construcción*, y un segundo nivel, el cual es una síntesis de los elementos básicos de los anteriores niveles.

La categorización hecha por Strate, permite comprender y sistematizar las definiciones o tipos de ciberespacio, ya que cada orden de complejidad abarca diferentes formas y permite hacer una taxonomía de las definiciones.

A saber, en el orden cero se encuentran las nociones que se tienen de ciberespacio, por un lado, se encuentra quienes consideran el ciberespacio como una simulación, es decir, un espacio que es ficticio o imaginario (Strate, 1999, p.384); por otro lado, se encuentra quienes, haciendo uso de la teoría de la relatividad, consideran al ciberespacio como un aspecto del *ciberespacio-tiempo*, en donde toman lugar relaciones entre computadores, entre humanos, y entre computadores y humanos.

En cuanto al primer orden, hace referencia a un espacio virtual, que se encuentra compuesto por tres bloques: el primero, relacionado con la *base física*, referente al hardware necesario y a los usuarios que hacen uso del mismo; el segundo es el *aspecto conceptual,* que tiene que ver con la manera en que ese tiene una noción generada en la mente mientras se interactúa con tecnología de computación; dentro de esta categoría se encuentran ciberespacios, lógicos, retóricos, o metafóricos. El último bloque es la percepción, que permite hacer un puente entre el bloque físico y el conceptual donde "la noción de espacio es generada por la interfaz del hardware y el usuario mediante uno o más sentidos del ser humano" (Strate, 1999, p.385).

Con respecto al segundo orden, este se basa en el anterior, y debido a ello es una *síntesis* entre transacciones simbólicas entre humanos y un proceso de transmisión y recepción de información.

En congruencia con esta categorización conviene afirmar, como lo hace Clark, que el ciberespacio se puede caracterizar por cuatro capas: la primera es *la base física*, en la que se apoyan los elementos lógicos, como, por ejemplo: el hardware necesario o los lugares de donde se operan los computadores o demás. La segunda es referente a los *bloques lógicos*, entre ellos el código, que crea los servicios y apoya la naturaleza de la plataforma del ciberespacio. La tercera capa, tiene que ver con la *información* que es almacenada, transmitida y transformada en el ciberespacio. Y la última capa, está compuesta de *las personas* que participan, toman decisiones y transforman la naturaleza del ciberespacio (Clark, 2010, pp. 2-3).

Como se hace evidente, al revisar las diversas definiciones de ciberespacio, intentan focalizarse en uno u otro aspecto de este. En términos prácticos, esto puede llevar a grandes insuficiencias en cuanto a la adaptación y respuesta de las instituciones a los problemas que surgen dentro del mismo.

Por ello se hace imperativo entender al ciberespacio:

> (...) como un dominio global dentro del entorno de la información cuyo carácter distintivo es dado por el uso de aparatos electrónicos y el espectro electromagnético para crear, modificar, cambiar y usar información a través de redes interdependientes e interconectadas usando tecnologías de la información. (Kuehl, 2009; p. 28)

Además de ello, tiene unas dimensiones y capas que requieren ser atendidas transversalmente al momento de abordar cualquier asunto de políticas públicas.

Antes de continuar, cabe aclarar que el internet hace parte de esas redes que permiten tal interconexión, empero, existen algunas particularidades en este sentido. Para empezar, dentro de las redes se pueden encontrar niveles de profundidad, generalmente se representa su estructura como un Iceberg, en donde la superficie alberga contenidos indexados por motores de búsqueda como lo son Google, Yahoo!, Bing y demás. A mayor profundidad se encuentran archivos que no se encuentran indexados por los motores de búsqueda, es decir, como bases de datos, credenciales o enlaces directos que se encuentran dentro de un dominio o sitio web particular, por lo cual, la única forma de interactuar con este contenido es accediendo al sito o dominio que lo alberga, a esta parte de la red se le denomina *Deep Web* (Bright Planet, 2014); como parte de esta, se encuentra la *Dark Web,* que ha sido escondida intencionalmente y es inaccesible a través de navegadores convencionales. El contenido, y las páginas de esta última se encuentra en los *Darknets*, redes restringidas como TOR o I2P (Yubal, 2017).

Con lo anterior, es posible afirmar que el ciberespacio se hace más complejo, ya que no solo tiene unas capas específicas, sino que dentro de las mismas se encuentran variables, tales como, el nivel de la accesibilidad a los elementos contenidos en estas. Lo anterior, conlleva a una

proliferación de riesgo, ya que un problema puede ser iniciado desde cualquier capa, pero puede afectar a todas las capas e incluso a las personas en su vida cotidiana por fuera del ciberespacio.

Estos riesgos, han despertado la preocupación de casi todos los Estados alrededor del mundo, por ello en 2004 la Organización de las Naciones Unidas comenzó a promocionar la creación de una cultura global de ciberseguridad y de protección de infraestructuras de información crucial. En ese sentido, la ciberseguridad empieza adquirir cada vez más relevancia dentro de la agenda de políticas públicas en los Estados, debido a que la estructura del ciberespacio tiene un vínculo con las infraestructuras de los países utilizadas para administrar y distribuir la energía, el transporte aéreo y los servicios financieros, entre otros (Naciones Unidas, 2004. La resolución 58/199 de la Asamblea General. *Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales*. En adelante: A/RES/58/199).

De esta forma el concepto ciberseguridad depende de la definición de ciberespacio, ya que, según diversos autores y organizaciones, esta contiene dentro de sí varias dimensiones tales como: el cibercrimen, ciberespionaje, ciberterrorismo, y ciber-hacktivismo (Di Camillo y Miranda, 2011), (Christou, 2016, p. 6) y la ciberguerra (Clarke y Knake, 2010), (Libicki, 2009). De tal forma, es pertinente asirse a una definición amplia que aborde la complejidad del ciberespacio y las amenazas que en este surgen, para esto conviene definir la ciberseguridad como la salvaguarda a través de acciones para proteger el ciber dominio, tanto en el campo civil como en el militar, incluyendo las amenazas que puedan afectar las redes interdependientes y la infraestructura de información. La ciberseguridad pretende preservar la disponibilidad y la integridad de redes, como también, la infraestructura y la confidencialidad contenida en la misma (Unión Europea, 2013. Comunicación conjunta al parlamento europeo, al consejo, al comité

económico y social europeo y al comité de las regiones. *Hacia una asociación renovada para el desarrollo UE-Pacífico*. En adelante: JOIN(2012) 6 final).

Entender la ciberseguridad de esta forma permite vincular todas las capas que la componen, y con ello, comprender todos los niveles de acción que se deben tener en cuenta para abordar el cibercrimen. Con respecto a esta categoría, es evidente que ha sido abordada de diferentes formas en función de la jurisdicción de cada país, incluso algunos autores se reúsan a definirlo como tal (Ferreyros, 1996, 407).

A pesar de ello, las organizaciones internacionales se han esforzado por reconocer las particularidades de este tipo de delito, para con ello actuar de manera efectiva sobre el mismo, aunque en el derecho internacional público no exista ningún tipo de regulación explicita sobre los ciberdelitos o sobre la ciberguerra entre sujetos del derecho internacional (Schhmitt, 2013).

En general las definiciones de cibercrimen consideradas alrededor del mundo se pueden incluir dentro la siguiente interpretación de la misma:

> Un rango amplio de actividades criminales donde los computadores y los sistemas de información están involucrados como herramienta primaria o como objetivo primario. El cibercrimen reúne todas las acciones punibles tradicionales, las acciones y hechos punibles relacionados con contenidos, como la distribución de pornografía infantil, o el fomento al odio racial, y conductas punibles que se dan solamente en los computadores y sistemas de información, por ejemplo, ataques en contra de sistemas de información o malware. (JOIN(2012) 6 final).

Definir cibercrimen con amplitud permite abarcar los diversos tipos de actores que se pueden vincular a esta actividad, además de ello permite que las jurisdicciones y los desarrollos

teóricos se adapten al cambio vertiginoso de características y al surgimiento de nuevas acciones criminales.

Pero el cibercrimen, como toda acción dentro del ciberespacio, es transversal a todas sus capas, y por lo tanto son personas las que lo ejecutan. Por la investigación de los diversos centros académicos y gobiernos, se han identificado diseñado varias categorías a fin de entender y prevenir la acción de cibercriminales. Entre estos actores se encuentran los Estados que pueden sostener hostilidad con algún otro, como es el caso de China, Rusia, y EEUU, también se encuentran actores no estatales cuya proliferación se ha acelerado en el último lustro.

Entre estos últimos se encuentran los *hackers individuales*, que pueden ser actores autónomos y, en algún momento, ser utilizados por parte del Estado; estos individuos pueden poseer información valiosa, como lo son las vulnerabilidades de los sistemas, un ejemplo de cómo estos pueden ser reclutados es la unidad 61398 del Ejército Chino, ó unidad 8200 de las fuerzas de defensa israelís (Bussolati, 2015, p. 105-106).

Continuando con el planteamiento anterior, un segundo grupo son *las organizaciones ciber criminales*, cuya estructura es similar a los sindicatos criminales, cuyo fin es delinquir a fin de obtener réditos económicos, en ese sentido pueden vincularse a cualquier actor que garantice ganancias, generalmente tienen una capacidad muy amplia en términos de infraestructura física, digital y ciber capacidad.

Una tercera categoría, son los *cibermercenarios,* que son grupos compuestos de hackers muy capacitados que se especializan en ataques de alta complejidad, su fin es ofrecer sus servicios a entidades públicas o privadas a fin de lucrarse. A diferencia de las organizaciones

criminales, el único interés de estos es económico y siempre actúan en consonancia a un acuerdo con un contratista determinado.

La cuarta categoría, los *hacktivistas,* son grupos de hackers con afiliaciones políticas o ideológicas, estos pueden ser pequeños grupos locales o grandes organismos transnacionales, generalmente son descentralizados y su acción es coyuntural.

Por último, se encuentran los *"hackers patrióticos"*, que son similares a los Hacktivistas estructuralmente y operacionalmente, son creados de manera coyuntural y pretenden en cada ocasión defender los intereses de un país específico. Estos pueden tener conexiones con grupos terroristas, cuando las motivaciones de estos grupos están relacionadas con reivindicaciones geopolíticas basadas en la religión. (Bussolati, 2015, p. 108).

Antes de continuar, es pertinente precisar que los ciberdelitos entre Estados Nación, u organizaciones con estatus de beligerancia son parte de la denominada ciberguerra. Ello implica que un ataque de una de las partes puede tener consecuencias físicas, y puede que a futuro la mayoría de conflictos físicos, estén acompañados de ciberguerra (Clarke y Knake, 2010, p.31-32), dicha combinación es conocida bajo el nombre de Ciberguerra Operacional (Libicki, 2009, p. 139).

Relativo a la ciberguerra, se encuentran tanto la ciberdisuasión y la ciberdefensa. Esta incluye todo lo necesario con el fin de evitar que los atacantes logren sus objetivos (Libicki p.137), mientras que aquella se refiere a la creación estímulos para desincentivar la escalada de los ataques, o desincentivar que la otra parte lleve a cabo un ataque (Libicki, 2009, p. 7).

Con lo anterior es posible afirmar que la acción de los Estados debe ser centrarse en las organizaciones *cibercriminales*, sin descuidar a los *hackers individuales* y a los *cibermercenarios* en tanto que estos pueden ser parte de un SAP.

Con respecto a los SAP, también conocidos en el ámbito internacional como Advanced Persistent Threats, se puede decir que son unos de los actores que representan mayor amenaza para los actores del ciberespacio. Por tanto, es preciso aclarar a que se refiere este término y cuál es su manera de actuar.

Inicialmente su nombre se refiere a: *Sistema* (Advanced por sus siglas en inglés) debido a que el adversario puede operar en cualquier tipo de intrusión al sistema computacional o a la red, pueden así mismo hacer uso de *exploits,* conocidos comúnmente para perpetrar alguna intrusión por medio de cualquier vulnerabilidad, o pueden desarrollar nuevas piezas de código a fin de buscar y aprovecharse de nuevas vulnerabilidades. *Amenaza*, ya que es una persona u organización que tiene intereses y un propósito definido, generalmente es la perpetración de crímenes, es necesario insistir que las amenazas no son simples piezas de código, ya que estas serían inútiles sin un operador, en este sentido, la amenaza es en conjunto tanto la organización, persona, como el malware. *Persistente*, ya que la organización, o persona, se ha propuesto a cumplir una determinada misión de acuerdo a sus intereses. Es decir, no son intrusos coyunturales, sino que pueden llegar a mantener un nivel de interacción con el sistema, la red o la organización objeto de ataque con el fin de lograr sus objetivos (Bejtlich, 2010).

En general estas tienen distintas motivaciones o intereses, pueden ser políticos, es económicos, técnicos o militares, y distintos objetivos de ataque como lo son firmas de salud, universidades, instituciones financieras o entidades estatales.

Las instituciones miembros del Joint Universities Computer Centre (JUCC) han organizado una clasificación al respecto que es necesario tener en cuenta en el contexto del presente trabajo. Estos definen:

Tabla 1. Organizaciones vulnerables a ataques de Sistemas de Amenaza Persistente

	Crimen Organizado	**Afiliados al Estado**	**Activistas**
Industria o Sector Víctima	Finanzas Ventas Comidas	Manufactura Profesional Transportes	Información Público en general Otros servicios
Región común de	Europa Oriental Norte América	China	Europa Occidental Norte América
Acciones o herramientas usadas comúnmente	Modificación desautorizada de datos Tampering Brute Force Spyware Captura de datos almacenados RAM Scrapping	Pishing Controles de comandos Exportación de datos Descifradores de contraseñas Credenciales robadas	SQL Credenciales robadas Brute Force RFI Backdoor
Objetivos materiales específicos	Cajeros Bases de datos Computadores de escritorio Terminales de venta	Portátiles/Computadores de escritorio Servidores de archivos Servidores de correo Servidores de directorio	Aplicaciones Web Bases de datos Servidores de E-mail
Datos que desean obtener	Tarjetas de pago Credenciales Información de	Credenciales Datos internos de la organización	Información general Credenciales Información de

Cuentas de Bancos	Secretos de negociación Información del sistema	datos de la organización

Nota: Elaboración propia con base en. (JUCC, 2016, p. 1).

El cibercrimen lleva a que diversos actores, tanto gubernamentales como no gubernamentales, se den a la tarea de construir unas estrategias para prevenir, responder y mitigar las amenazas que surgen en el contexto mundial. Esto se hace evidente en cada uno de los planes de seguridad implementados por los Estados y las empresas.

A modo general, las organizaciones internacionales intentan aproximarse al asunto mediante una *defensa a profundidad*, con la que pretenden proteger las redes y las características del ciberespacio a todos sus niveles. Esta estrategia se centra en la medición de tres variables: la primera, *técnica*, en donde se mide la infraestructura y el ciclo de respuestas; en segundo lugar, el *retorno de seguridad de acuerdo a la inversión,* que es un análisis de costos sobre los beneficios de implementar nuevas políticas o instalar nueva tecnológica; por último, se realiza una *Postura de Riesgos* que analiza el impacto de hipotéticos ciberincidentes a la organización.

2.1. Estrategias internacionales

A nivel específico, cada país ha determinado unas estrategias particulares donde se perfila frente a las amenazas que consideran relevantes para su contexto. A continuación, se analizan las estrategias propuestas por Estados Unidos, la Unión Europea y China.

2.1.1. Estados unidos.

En Estados Unidos se empezaron a realizar avances, en cuanto a las estrategias, a partir de la Estrategia de Seguridad Nacional (National Security Strategy) en 2010, con este documento

se intentan comprender las diferentes amenazas cibernéticas para un ciberespacio seguro. En términos generales, el gobierno estadounidense define amenazas generales, desde hackers hasta organizaciones criminales, asimismo, trata de evaluar las amenazas de los grupos terroristas y los Estados que puedan significar riesgos, entre los que se encuentran China y Rusia, entre otros (Casa Blanca, 2010).

En este sentido la estrategia que se adopta es *mitigar*, *prevenir*, *encontrar*, *defenderse y recuperarse* de las intrusiones cibernéticas, para ello, el gobierno decide invertir en las personas y en tecnología con el fin de proteger y mejorar la resiliencia de las redes más importantes de la industria y del gobierno. Otra medida que se toma, es fortalecer las alianzas internacionales y las alianzas con el sector privado. Estas estrategias toman como eje neurálgico la infraestructura critica, es decir la más importante, pauta que es continua en todas los desarrollos regulatorios y estratégicos del gobierno. De hecho, la revisión del plan cuadrienal de seguridad insiste en la protección de la infraestructura para prevenir eventos con consecuencias muy graves (Departamento de Defensa de EEUU., 2010).

Además de lo anterior, se han propuesto trabajar internacionalmente para promover una infraestructura segura de datos, construir un entorno donde las normas que promuevan una acción responsable guíen las acciones de los Estados, promoviendo el imperio de la ley en el ciberespacio. Así las cosas, la estrategia propuesta pretende fortalecer la colaboración multilateral o bilateral, la colaboración con el sector privado. En términos de defensa pretenden disuadir a los Estados u organizaciones de acometer ciberdelitos u hostilidades en el ciberespacio, tales como el robo de datos. En cuanto al desarrollo, la intención es construir capacidades técnicas, y capacidades en ciberseguridad (Casa Blanca, 2011, p. 7-14).

En el aspecto militar, la estrategia se propone adaptarse a los retos del Siglo XXI. Alcanzar la gobernanza del internet promoviendo estructuras efectivas e inclusivas. Y promover y permitir la libertad en internet asimismo como proteger la privacidad (Casa Blanca, 2011, p. 20).

2.1.2. Unión europea.

En la unión europea existe una gran divergencia en cuanto a la Ciberseguridad, sin embargo, dentro de la misma organización existe un liderazgo de buenas prácticas como es el caso del Reino Unido y Países Bajos (JOIN(2012) 6 final). Todos los países tienen una necesidad distinta.

La estrategia interna de seguridad ISS (2010) y la agenda digital por Europa (2010) han dado las pautas para el desarrollo de actividades en esta área. Pero también, se encuentran propuestas específicas a través de la estrategia europea para la seguridad en internet ESIS (2011) y la estratégica de ciberseguridad para la unión europea EUCSS (2013). Quien coordina la acción es el servicio europeo de acción externa, mientras que el equipo de respuesta a emergencias computacionales (CERT) se encarga de los aspectos técnicos a nivel internacional.

La política de común de seguridad y de defensa (PCSD) sentó las bases para la estrategia de la UE. En esta última se reconoce el cambio que las sociedades en torno a una nueva fase de desarrollo, donde la ciudadanía, y la industria tienden a utilizar en mayor medida las TIC y por lo tanto la utilización de redes de comunicación electrónica se hace cada vez más significativa. En este sentido, es clave contemplar la ciberseguridad como eje central a fin de garantizar el desarrollo (Consejo de la Unión Europea, 2006, p. 9).

En este orden de ideas, la protección de ataques, incidentes, utilizaciones irregulares y malintencionadas de ciberespacio requiere que la burocracia de cada uno de los países de la UE garantice la custodia y la promoción de un ciberespacio que sea libre, pero a su vez seguro. Sin embargo, la UE reconoce el liderazgo del sector privado en lo que respecta a la ciberseguridad (Consejo de la Unión Europea, 2006, p, 11), y en este sentido promueve alianzas entre este sector y los gobiernos.

Específicamente existen cinco pilares y prioridades estratégicas:

La primera, es *lograr resiliencia cibernética*, por esta razón se da la creación de la política de seguridad de las redes de la información y en conjunto se forma la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

La segunda, es *reducir la ciberdelincuencia*, para ello se adoptó el convenio de Budapest, que versaba sobre la Ciberdelincuencia del Consejo de Europa, en este se adopta medidas como la persecución de la pornografía infantil en todo medio, lo cual incluye al ciberespacio (Unión Europea, Directiva 2011/93/UE).

La tercera, es desarrollar *estrategias y capacidades de ciber defensa* vinculadas a la PCSD, por ello se adoptan tres frentes: la detección, la respuesta y la recuperación frente a las amenazas complejas que pueden surgir en el ciberespacio.

La cuarta, es *crear y mejorar los recursos industriales y tecnológicos de ciberseguridad,* como se mencionó anteriormente, la UE reconoce su rezago con respecto al sector privado y aunado a esto, se encuentra que la mayoría de firmas expertas en ciberseguridad se encuentran en países terceros, no perteneciente a la UE (Comisión Europea, ,2016, p. 30); por lo cual, el objetivo es que se pueda compensar el atraso con respecto otros países en cuanto a la presencia

de empresas de ciberseguridad, y de esta manera, se pretende evitar que la UE sea dependiente de la capacidad de las TIC en otros países (Comisión Europea, 2016, p. 32).

Y la quinta, es *establecer una política internacional del ciberespacio promoviendo los valores de la UE,* es importante recalcar que en este aspecto la UE pretende promover sus valores esenciales en el ciberespacio, esto es la defensa de la dignidad humana, la libertad, la democracia, la igualdad, y la promoción del Estado de Derecho. En términos diplomáticos, se pretenden promover las alianzas con organizaciones como la OTAN, la ASEAN y en especial se pretende tener una cooperación bilateral con EEUU.

2.1.3. China.

La ciberseguridad es un asunto central para el gobierno chino, pues en este país se reconocen no solo las amenazas técnicas que implica dicho medio, sino también ideológicos. Por ese motivo la acción del Estado pretende poner un marco legal a todas las acciones dentro de este medio.

Por ello, el gobierno chino a través de la comisión XVIII pretende fomentar la orientación de la opinión pública a través de las redes sociales del gobierno, y también pretenden garantizar el orden en el flujo de información de la red (Comité central del Partido Comunista, 2013). Nótese que el programa y la estrategia del gobierno chino distan de ser similares a los de EEUU o la UE, esto por la diferencia con sus principios básicos.

Además de ello la Ley de Ciberseguridad proferida en 2015 (Consejo de Relaciones Exteriores, 2015), pretende garantizar la soberanía del ciberespacio, aunque esto parezca contra intuitivo ya que el ciberespacio es global antes que local, el gobierno chino tiene una estrategia muy peculiar al respecto ya que generan estímulos para tal propósito.

Uno de ellos es ordenar que toda la infraestructura física necesaria para almacenar los datos se encuentre dentro del territorio continental chino (Consejo de Relaciones Exteriores, 2015), de esta forma los delitos relacionados con los datos chinos implican, implícitamente, una acción en contra de infraestructura china, lo cual puede tener implicaciones diversas en el derecho internacional.

Claro está que el Estado también pretende promover es el desarrollo tecnológico y en especial de tecnologías de la seguridad, a fin de garantizar el liderazgo de la nación en el ciberespacio. En cuanto a la prevención, el Estado, mediante la misma ley, ordena que todas las partes y secciones del Estado a todos niveles se encarguen de capacitar a todos los funcionarios para que sean conscientes de la importancia del ciberespacio, y que extiendan la estrategia de ciberseguridad a todos los niveles.

Ahora bien, un aspecto interesante en términos penales es que el gobierno chino ordena que el aparato judicial consulte a los operadores de red para que proporciones ayuda técnica y colaboren con la formulación de leyes y reglamentos (Consejo de Relaciones Exteriores, 2015). Y en ese sentido, se abre la puerta a una mutua colaboración entre los jueces y los especialistas en temas cibernéticos, lo cual puede generar una capacitación de los primeros en cuanto a temas de ciberseguridad.

En términos de respuesta a amenazas la solución del gobierno contempla la posibilidad de desconectar temporalmente la infraestructura de diferentes lugares, esto con el fin de garantizar el orden (Consejo de Relaciones Exteriores, 2015). Lo particular de esta decisión es que esta respuesta puede ser puesta en marcha incluso en momentos donde la amenaza no surja en el mismo ciberespacio como por ejemplo en caso de disturbios.

En suma, se puede afirmar que en estos países la preocupación que existe por formar estrategias ha sido abordada, en primer lugar, mediante la colaboración con las organizaciones y empresas que tienen experiencia en el campo, a fin de desarrollar mejores capacidades dentro de las burocracias de cada país. En segundo lugar, la ciberdefensa se ha centrado en la prevención de las amenazas, en este sentido, los países han adaptado sus legislaciones y sus infraestructuras con el fin de minimizar cualquier amenaza; un ejemplo prominente es China, que a pesar de su controversial perspectiva se ha empeñado en mitigar los riesgos mediante restricciones al uso del ciberespacio. Por último, se encuentra que todos los países se esfuerzan para innovar en este aspecto, un ejemplo claro de esta intención es la inversión realizada para incentivar la creación de firmas de ciberseguridad en la UE, así como la capacitación de la burocracia China en este sentido.

En este sentido, es necesario profundizar en las particularidades que adquieren tanto las amenazas como las estrategias para el caso colombiano y, en especial, el papel que juegan los GAO y los SAP como amenazas para el Estado colombiano.

3. Repercusiones de las amenazas cibernéticas en colombia.

Como es evidente, las ciberamenazas son un fenómeno que ocurre a nivel mundial, por esto se requieren esfuerzos multilaterales para mitigarlas. Además, es necesario categorizarlas, a fin de hacer la acción estatal más efectiva frente a las amenazas más frecuentes en cada contexto. Para el caso de la presente investigación se realiza una categorización de amenazas según quien las ejecute con el fin de identificar la relación de los SAP y los GAO en el caso colombiano.

En desarrollo de lo anterior, es preciso empezar con la categoría más general, los SAP, los cuales abarcan una amplia gama de actores y acciones, que son pertinentes para analizar en el caso colombiano:

Hackers individuales: en el contexto colombiano no se cuenta con una estimación del número de estos actores. Sin embargo, es clave aclarar que los hackers criminales individuales, pueden ser parte de diversos grupos, y tener varios intereses. Por lo cual, no es conveniente, ni posible, hacer una categorización de estos, en tanto pueden variar sus intereses. Al respecto, se puede decir que estos pueden trabajar para otros actores, o unirse a otros grupos como, por ejemplo: a grupos de hacktivismo, defender intereses de su patria, a grupos de Organizaciones Cibercriminales, como los GAO o GDO, o ser parte de firmas de cibermercenarios.

Hacktivistas: un ejemplo de la presencia de estos grupos en Colombia, es la existencia de miembros de grupos como Anonymus en el país, cuyo actuar es coyuntural y, por lo general, tienen un fin ideológico. De tal forma que su interés no es, per se, criminal, empero, pueden incurrir en ciberdelitos bajo la legislación colombiana a fin de lograr sus objetivos, ya que pueden obstaculizar el tráfico de un sitio Web, o hacer cambios en las características del software de una entidad pública.

Hackers patrióticos: la existencia de estos hackers a nivel mundial es prominente en casos como el ruso, el chino o el estadounidense. Pese a ello, en Colombia no se han identificado grupos de especialistas cibernéticos que protejan o abanderen los intereses del Estado sin hacer parte de su burocracia. Sin embargo, es necesario que el Estado prevenga la acción de estos actores en caso de la intrusión de otros países en las redes nacionales y estatales, además, que impulse la regulación de este tipo de ataques. Este tipo de actor, garantiza a los Estados una

cierta impunidad delante del derecho internacional debido, como es evidente en el caso ruso (Clarke y Knake, 2010, p. 20).

Cibermercenarios: el uso de estos en el contexto internacional es de conocimiento por diferentes Estados. Consecuentemente, es posible que delincuentes se hagan a los servicios de los cibermercenarios para alcanzar sus fines, esto no excluye a ninguna organización, lo cual quiere decir que los GDO o los GAO pueden hacerse a los servicios de estos grupos. De hecho, estos grupos mercenarios son considerados como el mayor riesgo para los Estados Nación (Despasquale y Daly, 2016), por lo cual es imperativo tener en cuenta estrategias de mitigación de este riesgo.

Organizaciones cibercriminales: en el contexto que nos atañe, pueden ser conformadas de los GAO o Grupos Delictivos Organizados, que son los grupos que bajo una dirección de un mando responsable, ejercen control sobre un territorio que les permita realizar operaciones militares sostenidas y concertadas. A su vez, estos se relacionan con los Grupos Delincuenciales Organizados (GDO) que "son grupos de más de tres personas que exista durante cierto tiempo y actué con el propósito de cometer delitos graves para obtener un beneficio económico o de orden material" (Ministerio de Defensa Nacional, Directiva 0015/2016, p. 5). Con lo anterior, se puede afirmar que los GAO pueden hacer parte de las organizaciones cibercriminales siempre que se valgan del ciberespacio para ejercer y ejecutar sus labores.

Otros Estados: hasta el momento no hay evidencias de la intención de intromisión de otros Estados en la infraestructura de datos en Colombia. A pesar de esto, es necesario que la nación se prevenga de incidentes como los ocurridos en Georgia, Estonia o Estados Unidos, donde otro país (Rusia o China) intentó instruirse en el ciberespacio de otro país con el fin de

obstaculizar el funcionamiento normal del mismo, y con ello causar un caos económico, social y político (Clarke y Knake, 2010, p. 16).

Para complementar el análisis, es necesario tener en cuenta que cada uno de estos grupos tiene la intención de afectar o incidir en el normal funcionamiento de las cuatro capas que componen el ciberespacio. En general, todos los SAP tienen la capacidad y la intención de afectar la capa de bloques lógicos, pues a nivel general la estrategia que más se usa entre estos con respecto al Estado es la Negación Distribuida de Servicio (DDOS por sus siglas en inglés) cuyo objetivo es obstaculizar el tráfico normal en diferentes sitios web.

Ahora bien, en general una de las más prominentes causas de debilidad del ciberespacio se encuentra en la última y más importante parte del mismo, la referente a los usuarios. En general, las personas que usan y manipulan el software o el hardware del Estado son vulnerables a la ingeniería social, sin que ellos lo sepan, lo cual hace que todos los actores mencionados puedan hacer uso de esta debilidad.

Además de ello, todos los ataques terminan por afectar a los usuarios, sin embargo, unos los hacen en mayor medida que otros. Como ilustración de ello, los ataques de los hacktivistas no tienen la misma intención o intensidad de ataque que los de una organización cibercriminal, ya que estas organizaciones pueden dedicarse a la trata de personas, o tráfico de armas, lo cual es una verdadera intención de afectar a los usuarios del ciberespacio, mientras que los activistas no pretenden causar mayor daño a la integridad de las personas.

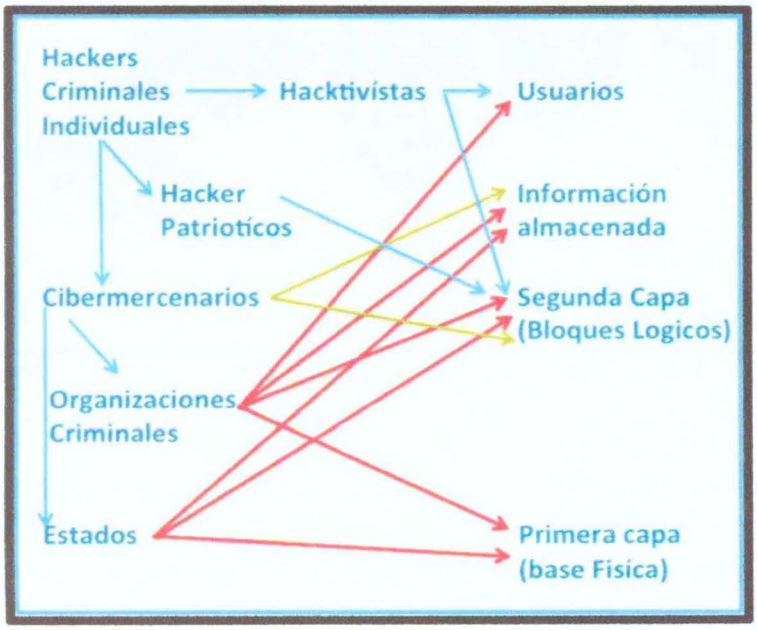
En ese sentido, es necesario mencionar que también los Estados pueden tener una intención de afectar directamente a los usuarios, cuando, por ejemplo, llevan ataque dirigidos a

través de un sistema operativo con el fin de realizar un ataque que pueden involucrar vidas de personas.

Con respecto a la información que se almacena dentro de los servidores se puede decir que los más interesados en esta parte del ciberespacio son los Estados, y las organizaciones cibercriminales con fines políticos, en conjunto con los cibermercenarios, quienes pueden ser contratados para obtener algún tipo de información específica de determinada red.

Por último, los Estados y las organizaciones cibercriminales con potencial armamentístico pueden atentar en contra de las instalaciones donde se albergan y funcionan los servidores, y en este sentido, tienen la capacidad de afectar las cuatro capas del ciberespacio de otro Estado, lo cual los convierte en los más peligrosos actores en cuanto a la afectación del ciberespacio.

Figura 1. Actores como amenaza directa para capas del ciberespacio

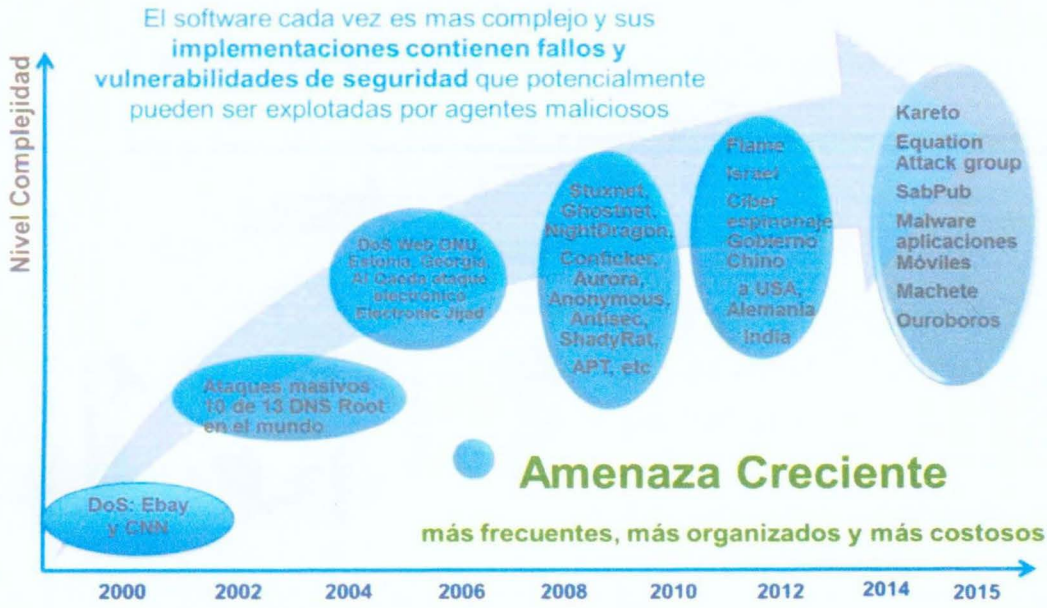


Nota: Elaboración propia. 2017.

En la anterior figura se puede ver la intencionalidad y capacidad que tienen los actores para afectar a las diferentes capas del ciberespacio. Asimismo, en la parte izquierda se encuentra la relación entre los actores específicos.

Ahora bien, las anteriores nos son las únicas variables que el Estado colombiano y las FFAA tienen que tener en cuenta a la hora de adaptarse en el ciberconflicto, esto debido a que la amenaza se amplifica y complejiza cada vez más, en tanto los software tienden a vincular más bloques de código y eso conlleva a que, asimismo, aumenten los huecos de seguridad (Figura 2).

Figura 2. Diagrama cualitativo sobre la evolución de la amenaza cibernética a lo largo de los últimos años



Nota: Extraído del *Diplomado de Ciberseguridad y Ciberdefensa en el ámbito jurídico*, 2015, p. 28.

Con esto en mente, es evidente que para abordar la amenaza que representan los SAP y los GAO, se requiere conocer que conductas pueden llevar a cabo para afectar el funcionamiento del aparato estatal. Para esto, es oportuno relacionar los ataques que se realizan en contra de cada

una de las capas del ciberespacio colombiano, de esta forma es posible establecer una relación entre los actores, las partes del ciberespacio y las amenazas más frecuentes en cada parte.

Inicialmente, es posible afirmar que existen características de amenazas en cada nivel del ciberespacio. Así, los *ataques a la infraestructura física*, son característicos en el primer nivel o capa, ya que es la única forma de vulnerar y afectar esta parte del ciberespacio de una nación; en cuanto a la segunda capa, esta es afectada mayormente por el *sabotaje*, mediante conductas como el DDoS; la tercera capa es afectada mayormente por el *espionaje*, ya que esta conducta pretende hacerse a los datos del Estado; la cuarta capa, las personas son afectadas tanto por *fraudes* como *ingeniería social*, que es la extracción de información importante de la red mediante manipulación.

Figura 3. Relación partes del ciberespacio y ataques más frecuentes a las mismas.

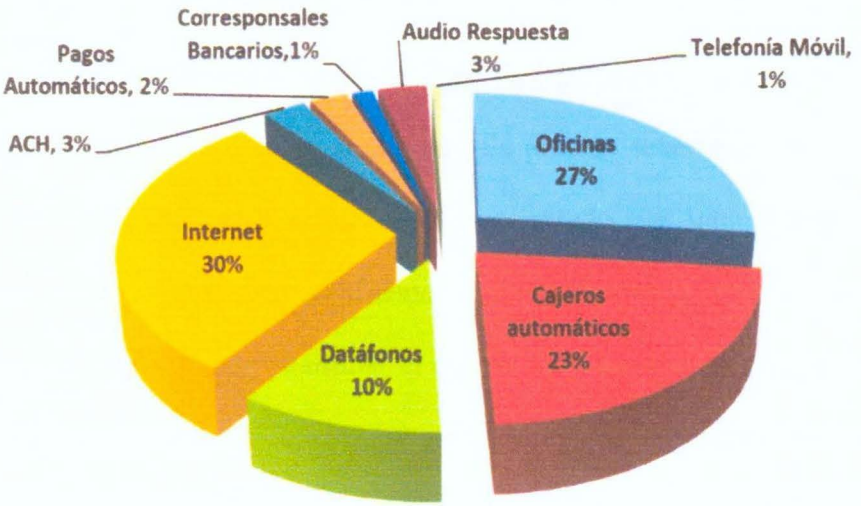
Nota: Elaboración propia, 2017.

Con lo anterior, es posible afirmar que los SAP en conjunto pueden afectar a todas las partes del ciberespacio colombiano. Tal es el caso de los Estados, y de los GAO, pues estos

últimos pueden afectar todas las capas, y en ese sentido, utilizar cualquiera de los ataques o amenazas mencionadas previamente debido a que poseen control parcial del territorio, y comenten crímenes en contra de la convención de Palermo, tales como el tráfico de armas, la trata de personas o el tráfico ilícito de inmigrantes (Ministerio de Defensa Nacional, Directiva 0015/2016, p. 5).

Con respecto a los GDO, aunque en teoría están vinculados con los GAO[1], no tienen la capacidad de afectar los ataques a la infraestructura, ya que no poseen potencial armamentístico de los GAO. En cambio, están más interesados en realizar fraudes y hacer uso de la ingeniería social para manipular a las personas y lograr cometer sus fines delictivos. Por ende, no pueden estar interesados en espiar, o en sabotear los sitios web del Estado.

Figura 4. Operaciones Monetarias y no Monetarias por Canal



Nota: Informe de Transacciones y Operaciones Superintendencia Financiera de Colombia. 2010

[1] Ya que un grupo delictivo puede transitar de una categoría a otra. (Ministerio de Defensa Nacional, Directiva 0015/2016).

Pero lo anterior no significa que los GDO son una amenaza insignificante, pues estos grupos al pretender hacer fraude pueden afectar en gran parte la estabilidad y seguridad económica ya que el 30% de las transacciones monetarias para 2010 fueron realizadas por internet, y si a esto se le suman los canales que están vinculados al ciberespacio, como los datafonos y los cajeros automáticos, sería el 63 % de las transacciones las que estarían en riesgo de sufrir daños por la acción de estos grupos (Figura 4).

Por tal motivo, es necesario tener en cuenta las amenazas que pueden representar los SAP en sus diferentes modalidades, esto sin descuidar dentro de las mismas a los GAO y los GDO, ya que ambos representan riesgos significativos para la ciberseguridad en diferentes partes o componentes del ciberespacio colombiano, lo cual puede traer consigo consecuencias indeseables tanto para el gobierno como para la ciudadanía.

4. Capacidades de las fuerzas armadas para la defensa del ciberespacio

Una vez expuesta la situación de amenazas en Colombia, es necesario evaluar la preparación del Estado ante las diferentes amenazas. Es preciso tener en cuenta que tanto los Estados Nación y las organizaciones multilaterales han optado por intensificar su trabajo en cuanto a la ciberseguridad y al cibercrimen principalmente en dos perspectivas: una estratégica y una jurídica, por lo cual, es pertinente examinar el estado de estas dos dimensiones para el caso colombiano. Cabe anotar que la división anterior no tiene como propósito hacer una distinción excluyente entre ambas dimensiones, sino que pretende enfatizar en la importancia del campo jurídico dentro de la estrategia de disuasión en el ciberespacio.

Por ello, el presente aparte se ocupa de las capacidades estratégicas y militares para la defensa del ciberespacio. En este sentido, es importante tener en cuenta como se articulan las

organizaciones estatales y su respectivo campo de acción, por eso se revisan las diferentes agencias estatales conformadas para desarrollar la acción estatal en el ciberespacio y sus diferentes funciones.

En términos generales, la estrategia colombiana para abordar las amenazas del ciberespacio se asemeja a lo planteado por Estados Unidos o por la Unión Europea. De hecho, los esfuerzos del país se han centrado en fortalecer la cooperación internacional y ha procurado adoptar algunas de las buenas prácticas que se llevan a cabo a nivel mundial.

Por esta razón, es necesario reconocer que la fuerza Pública con todas sus instituciones se encuentra en la búsqueda de generar y desarrollar una *política en seguridad cibernética,* estructural sostenible a largo plazo, con el ánimo de degradar y enfrentar en buena medida los ataques cibernéticos que puedan realizar los GAO en el ciberespacio. Para contribuir sustancialmente a la estabilidad, la seguridad y defensa en contra de las amenazas comunes a la región.

Para mantenerse a la altura de las nuevas circunstancias, Colombia está tomando medidas importantes para enfrentarse a las amenazas cibernéticas, un flagelo relativamente nuevo que está creciendo de manera vertiginosa y que sienta las bases para un nuevo campo de conflicto potencial en el siglo XXI.

Esta política se genera desde la institucionalidad del Estado colombiano principalmente con el Ministerio de Defensa y el Ministerio de las Tecnologías de Información y Comunicación; también procura el fortalecimiento de las relaciones interinstitucionales con los países líderes en la lucha contra los delitos cibernéticos, guías y puntos de referencia en relación

a desarrollo tecnológico de vanguardia para afrontar los conflictos de quinta generación de carácter hibrido y también como referente en la educación teórica práctica en esta área del saber.

Sin embargo, esto es algo reciente, ya que antes de 2011 el país carecía de unidades articuladas que se dedicaran exclusivamente a la vigilancia electrónica o a actividades propias del ciberespacio, antes de este año hubo esfuerzos por parte del sector privado con fin de mitigar este tipo de amenazas en su campo, sin embargo, la cultura de ciberseguridad era débil en su difusión tanto para el sector privado y en mayor medida en el sector público (CONPES 3701, 2011).

En consecuencia, es clave afirmar que los lineamientos de la política de ciberseguridad consignados en el CONPES 3701 son el origen de la ciberdefensa institucional del Estado, siendo el Comando Conjunto Cibernético (CCOC) el ente central para la protección y defensa del ciberespacio colombiano, en especial de la ciber-infraestructura militar, en cuanto a la ciberseguridad también se destaca el papel del ColCERT y del CCP (Tabla 2). En cuanto a acciones específicas, el CCOC, es el encargado de liderar el proceso de elaborar los informes e infraestructura critica junto con el ColCERT, además de ello es el encargado de liderar el proceso de creación de mecanismos para el fortalecimiento de las entidades de ciberdefensa (CONPES 3854, 2016, p. 60).

Además, dentro del Comando existe un Centro de Operaciones de Seguridad (SOC), el cual presta sus servicios tanto a propietarios como operarios de infraestructura crítica cibernética, lo cual lo convierte en un enlace importante entre el sector de defensa público y el sector privado. Este centro, también es un importante punto de retroalimentación con respecto a los avances en ciberseguridad a nivel global, esto debido a que el SOC del CCOC pertenece al Foro

para Respuesta a Incidentes y Equipos de Seguridad al cual también pertenecen los CSIRT de la Policía Nacional, de la Empresa de Telecomunicaciones de Bogotá y de Claro.

Otra de las organizaciones fundamentales para la mitigación de riesgos en el ciberespacio es el grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), el cual coordina la acción de los diversos CSIRT y promueve una cultura de ciberseguridad entre los diferentes entes. Esta labor, sin embargo parece no ser suficiente para que la promoción de una cultura ciberseguridad y de auto gestión sea eficaz a la hora de lograr formar unas buenas prácticas en todas las organizaciones por lo que varias instituciones, incluso estatales, parecen restarle importancia a la prevención de daños en sus estructuras cibernéticas.

Tabla 2. Agencias de ciberseguidad y ciberdefensa.

Nombre de la agencia	**Sigla**	**Misión**
Grupo de Respuesta a Emergencias Cibernéticas de Colombia	ColCERT	Ente articulador intersectorial a nivel nacional encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y ciberseguridad y Ciberdefensa
Departamento Administrativo Dirección Nacional de Inteligencia	DNI	La Dirección Nacional de Inteligencia tendrá como objeto desarrollar actividades de inteligencia estratégica y contrainteligencia para proteger los derechos y libertades de los ciudadanos y de las personas residentes en Colombia, prevenir y contrarrestar amenazas internas o externas contra la vigencia del régimen democrático, el orden

		constitucional y legal. La seguridad y la defensa nacional, así como cumplir con los requerimientos que en materia de inteligencia le hagan el Presidente de la República y el Alto Gobierno para el logro de los fines esenciales del Estado, de conformidad con la ley.
Comando conjunto cibernético de las fuerzas militares de Colombia	CCOC	Es una unidad militar fundada el 10 de octubre de 2012 con la misión de direccionar planea, coordinar, integrar y sincronizar a través de unidades y dependencias que podrán desarrolla, ejecutar y conducir actividades para dirigir las operaciones cibernéticas conjuntas, combinadas, coordinadas e interagenciales a fin de defender la infraestructura critica cibernética.
Comando Cibernético Policial	CCP	Encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en Ciberseguridad y trabajará de forma coordinada con el colCERT.
Equipos de Respuestas ante Incidentes de Seguridad Computer Security Incident Response Team de la Policia Nacional	**CSIRT PONAL**	Encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos

	nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT.

Nota: Elaboración propia. 2017.

Con lo anterior en mente, es necesario aclarar que la acción de los GAO como actor de los SAP hacen parte de las preocupaciones de ciberseguridad del Estado, pero específicamente son una amenaza central para la ciberdefensa, pues estos son una amenaza directa a la estabilidad del Estado, y por ende, la entidad que está encargada de mitigar los riesgos que estos representan es el CCOC porque este es el eje central de la ciberdefensa nacional. (Ministerio de Defensa Nacional, Directiva 0015/2016).

Ahora bien, estos organismos teóricamente deben cumplir una labor muy extensa que requiere la cualificación técnica que no es fácil de llenar, lo que lleva a preguntarse sobre la capacidad que tiene el país en el reclutamiento o la formación de especialistas en ciberseguridad y en ciberdefensa. Con respecto a esta cuestión, es inexorable tener en cuenta que la mayoría de especialistas en estas áreas se forman en los centros de educación superior. A pesar de ello, según el observatorio laboral en 2015 solo 2.052 estudiantes se matricularon en especializaciones de ciencias computacionales y afines, 6.861 en pregrados de la misma área, 502 en maestrías y 18 en doctorados (Ministerio de Educación, 2017). Como es evidente, estas cifras no corresponden a la demanda que el sector de ciberseguridad tiene en la actualidad, en especial si se tiene en cuenta que el total de estudiantes de pregrado es de 178.379, en este sentido, solo un 3.8% de los estudiantes se ocupan de esta área, esta es una cifra mínima si se tiene en cuenta que no todos los graduados de esta área se dedicaran a la ciberseguridad y la ciberdefensa. Todo esto nos permite afirmar que el país está propenso a depender de la producción científica y militar de otros países, lo cual puede ir en detrimento del liderazgo de las FFAA colombianas en esta área.

5. Ordenamiento jurídico existente en el país al respecto del ciberespacio

Ahora bien, el reto técnico también se presenta en relación al campo jurídico, puesto que el aspecto estratégico está estrechamente ligado con el campo jurídico, ya que, para evitar y regular las amenazas cibernéticas toda acción estatal requiere un sistema normativo, que sea capaz de disuadir a los potenciales perpetradores de este tipo de conductas.

En términos normativos hay que destacar el esfuerzo del Estado colombiano y de sus diferentes órganos para abordar las diversas amenazas que surgen en un contexto cada vez más dependiente del ciberespacio. Aunque este esfuerzo haya sido concretado hace poco tiempo, ya que, la primera ley que incluyo el ciberdelito como conducta punible en el sistema normativo colombiano fue la ley 1273 de 2009, seguida de la ley 1336 del mismo año, la cual se ocupaba regular delitos como la distribución de pornografía infantil. Estos fueron pasos muy importantes en tanto sentaron las bases para generar estímulos disuasivos entorno a conductas que afectaran el patrimonio, la integridad de los ciudadanos, y en general conductas en detrimento de la ciberseguridad en Colombia.

Sin embargo, el Estado también se vio obligado a adaptarse a un contexto cada vez más dependiente a la TIC y, con el fin de aprovechar la eficiencia del tránsito de información en el ciberespacio, vinculó el uso de medios electrónicos en el proceso administrativo. Estas acciones traen consigo grandes beneficios para la ciudadanía, pero también representan un riesgo latente para el Estado. La principal razón es que, entre más dependientes del ciberespacio sean los procedimientos y las funciones administrativas del Estado, es más posible que un ataque en contra de estas infraestructuras signifique consecuencias más graves, es decir entre más dependa el Estado a las TIC las amenazas cibernéticas significaran más riesgos para la estabilidad del Estado.

Como es evidente, la digitalización de los procedimientos del Estado ha avanzado notoriamente desde 2009, año en que estas leyes fueron promulgadas. La que más contribuyó a la aceleración de este proceso de digitalización fue la ley 1341 de 2009, ya que esta propuso los principios para generar el uso eficiente de las tecnologías de información, pues esta definía en su artículo 4 que era tarea del Estado masificar el programa de Gobierno en Línea (Colombia, Congreso de la República, 2009, Ley 1341, Art. 4), esto trajo consigo la irrupción y promulgación de normas en relación al ciberespacio en Colombia y en especial a la digitalización de la acción estatal, esto se puede observar en la promulgación de normativa sobre el tema ya que después de esta ley se aceleró la producción legislativa al respecto (Anexo 1).

Ahora bien, en términos de la disuasión que puede generar un ordenamiento jurídico entorno a la ciberseguridad es preciso afirmar que existe una brecha entre la promulgación legislativa, aunque esta no sea suficiente (CONPES 3701, 2011, p. 14), y la ejecución de la misma. Esto es causa de, por un lado, la falta de capacitación de los diferentes jueces encargados de juzgar sobre hechos relacionados a ciberdelitos, y por otro, de la difusión masiva y la creación en la práctica de una cultura de ciberseguridad.

En cuanto a la falta de capacitación de jueces y fiscales es necesario mencionar que ello conduce a que la disuasión no sea efectiva en tanto que la incapacidad de probar y juzgar un delito conlleva a que los criminales no teman a ser judicializados puesto que conocen estas falencias del sistema jurídico. Con respecto a este problema, se requiere que se empiecen a promocionar la creación de programas de especialización de derecho relacionados con estos temas, ya que en términos probatorios la preparación jurídica actual de la mayoría de jueces y fiscales, no se equipara a las necesidades que surgen a partir de problemas técnicos en términos de la primer, segunda y tercer capa del ciberespacio, esto es todo lo relacionado con el hardware,

los códigos de fuente y las particularidades que adquiere la información dentro de los sistemas cibernéticos.

Ahora bien, en términos penales es muy difícil que se pueda judicializar a algún ciberdelincuente sin pruebas, o con pruebas que no sean plenamente válidas. Esto es un problema en la legislación colombiana ya que "el número de fiscales capacitados para lograr construir un caso validado sobre pruebas electrónicas es limitado" (CONPES 3854, 2016, p. 42), lo cual permite afirmar que el problema de la cultura de la ciberseguridad se extiende incluso a la propia rama judicial.

En este mismo sentido, es necesario señalar que la ley 1273/09 se constituye en una base para perseguir el ciberdelito (Colombia, Congreso de la República, 2009, Ley 1273); aunque la falta de capacitación en aspectos técnicos y tecnológicos de la fiscalía y los jueces para discernir sobre las pruebas de estas clases de delitos hacen que el juez no pueda exigir las pruebas adecuadas para tales delitos a la hora de juzgar sobre casos de ciberdelitos. Esto conduce que el criminal quede libre por la falta de capacitación del juez o el fiscal.

Por esto la capacitación de las instituciones nacionales en aspectos como la ciberseguridad es uno de los retos y metas más importantes por alcanzar. Aunado a esto es necesario, promover las competencias y capacidades del talento humano nacionales del sector público, con participación de los funcionarios públicos y empleados del sector privado, para con ello formar profesionales que sean capaces de asumir los retos que implican el uso de las tecnologías de la Información y las Comunicaciones (TIC) en función del mejoramiento de la gestión pública, para consolidar un Estado eficiente, transparente y eficaz en seguridad cibernética.

Es por ello que el principal objetivo es implementar mecanismos que capaciten masivamente al sector judicial, y en general a todos los funcionarios estatales en una cultura de ciberseguridad para con ello subsanar las diferencias existentes entre doctrinas de comando y control de las diferentes instituciones públicas que tienen relación con el ciberespacio.

6. Conclusiones

Con lo anterior se reconoce que es necesario atender a las estrategias de los GAO, pero de igual forma los GDO, puesto que puede haber un tránsito de un grupo determinando entre ambas categorizaciones, de tal forma que la disuasión debe ser dirigida tanto a GDO como a GAO, ya que, como se expuso con anterioridad, la magnitud del ataque en el ciberespacio puede no ser necesariamente proporcional al tamaño del grupo, en tanto que un grupo reducido puede hacer más daño en la segunda y tercera capa del ciberespacio. Entretanto, si puede haber una relación proporcional entre el tamaño y organización del grupo con los ataques realizados a la capa física, y a las personas que hacen uso del ciberespacio, como es el caso de los Estados, las organizaciones criminales y los grupos terroristas.

Por otro lado, es recomendable hacer un análisis en cifras al respecto de cada una de estas capas del ciberespacio para así definir las diferentes estrategias en cada uno de estos niveles: el nivel de protección de la infraestructura física que sostiene el ciberespacio Colombiano, la vulnerabilidad de los bloques de código que sostienen y albergan las bases de datos e información del país, es pertinente saber que cuanta información alberga el Estado en el ciberespacio, así como la dependencia del Estado a las TIC.

Por otro lado, identificar la ubicación de la infraestructura física que sustenta, contiene los datos y estructura de las redes usadas por el Estado colombiano. Esto, con el fin de elaborar

un concepto de soberanía digital, tal como lo hacen países como Rusia o China, a fin de tipificar, gestionar y mitigar las diversas amenazas cibernéticas, y los ciberdelitos cometidos tanto por actores nacionales como actores internacionales, esto con el fin de blindar a Colombia en un caso de afectación a su estructura cibernética.

Para lo anterior, el ordenamiento jurídico y las instituciones encargadas de formular las estrategias entorno a la ciberseguridad deben reconocer las dimensiones que conforman el ciberespacio, y generar estrategias que, frente al derecho internacional, puedan tener en cuenta que la primera capa está estrechamente relacionada con las demás capas, y si se considera de esta forma, es posible que se considere un ataque a una infraestructura de datos como una intrusión en la soberanía de la nación, lo cual permite que la acción del Estado sea más amplia y legitima en relación al derecho internacional.

Se puede evidenciar que las ciberguerra no es una guerra convencional ya que no se encuentran los mismos niveles de violencia, no hay acciones bélicas físicas y no hay muertes de personas de forma directa por los diferentes actores involucrados en el ciberespacio, pero puede generar daños e importantes afectaciones a la infraestructura cibernética del Estado.

La ciberguerra es una nueva forma para generar conflictos a nivel mundial, por ende, es importe que el Estado con todos sus elementos constitutivos e instituciones preste especial atención y priorice los esfuerzos en la gestión de los riesgos para prevención de amezas presentes en el ciberespacio.

La cultura de seguridad digital junto con el balance entre los diferentes niveles (físico, bloques lógicos, información y usuarios) se constituyen en la mejor arma para enfrentar las diferentes amenazas cibernéticas y los ciberataque dentro de la ciberguerra.

La cultura de seguridad digital es una necesidad del país para de reducir los riesgos cibernéticos.

7. Recomendaciones

A la rama judicial del Estado: profesionalizar y especializar a juristas, jueces y fiscales en materia y crear la Ley para Asuntos del Ciberespacio en Colombia, sobre delitos informáticos y manejo adecuado de evidencia y material digital.

Al gobierno nacional: buscar la estandarización y la difusión de los protocolos de seguridad informática en todos los sectores del Estado a fin de minimizar los riesgos y amenazas cibernéticas, y promover la participación del sector público, privado y educativo, para generar iniciativas, proyectos, planes, reglamentaciones y leyes que promuevan la seguridad digital.

Al Comando General de las Fuerzas Militares: fortalecer las capacidades de los diferentes comandos y agencias que atienden y observan la ciberseguridad al interior de cada una de la Fuerzas Militares y la Policía Nacional para enfrentar la guerras de cuarta y quinta generación, con énfasis en la ciberguerra.

Referencias

Abebe, D. (2016, Invierno). Cyberwar, International Politics, and Institutional Design. En *Law Review*. Estados Unidos: The University of Chicago. Vol. 83, Núm. 1, pp. 1-22.

Bejtlich, R. (2010. Enero, 16). What Is APT and What Does It Want? *TaoSecurity*. Recuperado el 4 de julio de 2017, de: https://taosecurity.blogspot.com.co/2010/01/what-is-apt-and-what-does-it-want.html

Bell, D. (2001). *An Introduction to Cybercultures*. Londres y Nueva York: Routledge.

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. En: Ohlin, J. D., Govern, K. & Finkelstein, C. (eds), *Cyber War: Law and Ethics for Virtual Conflicts*. Inglaterra: Oxford University Press. Pp. 102-126.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. United Kingdom: Palgrave Macmillan.

Clark, D. (2010). *Characterizing cyberspace: past, present, and future*. Boston: CSAIL. Massachusetts Institute of Technology (MIT).

Clarke, R., y Knake R. (2010). *CYBERWAR: The next threat to national security and what to do about it*. New York: Harpercollins.

Clearing Up Confusion – Deep Web vs. Dark Web. (2014. Marzo, 27). *Bright Planet*. Recuperado el 4 de Julio de 2017 de: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

Comisión Europea. (2016) *Study on EU positioning an analysis of the international positioning of the EU using revealed comparative advantages and control of key Technologies*. Recuperado el 4 de julio de 2017, de: http://ec.europa.eu/research/innovation-union/pdf/expert-groups/rise/final-report_eu-positioning.pdf#view=fit&pagemode=none

Comité central del Partido Comunista. (12 de noviembre del 2013). *Documentos de la III Sesión Plenaria del XVIII*. Beijin. Recuperado el 4 de julio de 2017, de: http://www.politica-china.org/imxd/noticias/doc/1389789646Documentos_de_la_III_Sesion_Plenaria_del_XVIII_Comite_Central_del_Partido_Comunista_de_China.pdf

Colombia, Congreso de la República (2009) Ley 1273 de 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Bogotá: En Diario Oficial, Núm. 47.223, 5 de enero de 2009.

Colombia, Congreso de la República (2009) 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 de Espectro y se dictan otras disposiciones*. Bogotá: En Diario Oficial, Núm. 47426, 30 de julio de 2009.

Consejo de la Unión Europea. (2006. Diciembre, 11-12) *Transporte, Telecomunicaciones y Energía*. Bruselas. Recuperado el 4 de julio de 2017, de: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/trans/92382.pdf

Consejo de Relaciones Exteriores. (2015. Julio, 6). *Cybersecurity Law of the People's Republic of China*. Recuperado el 4 de julio de 2017, de: http://dev-www.cfr.org/internet-policy/cybersecurity-law-peoples-republic-china/p36788

Departamento de Defensa de los Estados Unidos. (2010). *Quadrennial Defense Review Report*. Washington, Estados Unidos: Casa Blanca. Recuperado el 4 de julio de 2017, de: https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf

Departamento Nacional de Planeación. (2011, 14 de julio). *Lineamientos de política para ciberseguridad y ciberdefensa Política Nacional de Seguridad digital* (Documento CONPES 3701). Bogotá D.C., Colombia: DNP.

Departamento Nacional de Planeación. (2016, 11 de abril). *Política Nacional de Seguridad digital* (Documento CONPES 3854). Bogotá D.C., Colombia: DNP.

Despasquale, S. y Daly, M. (2016. Diciembre, 10). The growing threats of cybermercenaries. *Politico Website.* Recuperado el 15 de julio de 2017, de: http://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221

Di Camillo, F. y Miranda, V. (2011. Septiembre). Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward. *IAI Working Papers*. Vol. 11-26. Italia: recuperado de: http://iaitestnew.asw.bz/sites/default/files/iaiwp1126.pdf

Escuela Superior de Guerra. (2015). *Diplomado en Ciberseguridad y Ciberdefensa en el ámbito jurídico*. Bogotá D. C., Colombia: Escuela Superior de Guerra.

Estados Unidos, & Obama, B. (2010). *National Security Strategy of the United States*: Casa Blanca. Recuperado el 4 de julio de 2017, de: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Estados Unidos, & Obama, B. (2011). *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*: Casa Blanca. Recuperado el 4 de julio de 2017, de: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ferreyros, C. (1996) Aspectos metodológicos del delito informático. En *Revista Iberoamericana de Derecho Informático*. Mérida: Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura. Núm. 9-11, pp. 407-412.

Joint Universities Computer Centre Limited (JUCC). (2016). Advanced Persistent Threat. En: *Information Security Newspaper*. Hong Kong: The University of Hong Kong. Vol. 2- IT Professional. Núm 2.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. En Kramer F., Starr S., & Wentz L. (Eds.), *Cyberpower and National Security*. Estados Unidos: University of Nebraska Press. Pp. 24-42.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Estados Unidos, Santa Monica: RAND corporation.

Ministerio de Defensa Nacional. (22 de abril de 2016). Directiva 0015/2016. Asunto: *Expedir los lineamientos del Ministerio de Defensa Nacional para caracterizar y enfrentar a los Grupos Armados Organizados (GAO)* y *Derogar la directiva permanente 014 de 2011 que establece la estrategia nacional de lucha contra las BACRIM*. Colombia.

Ministerio de Educación Nacional. (2016. Mayo, 24) *Oferta educativa en Colombia*. Recuperado el 15 de julio de 2017, de: Página del Observatorio Laboral Graduados Colombia. http://bi.mineducacion.gov.co:8380/eportal/web/men-observatorio-laboral/oferta-regional Consultado 24/05/2016

Naciones Unidas. (20 de enero de 2004). La resolución 58/199 de la Asamblea General. *Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales*. A/RES/58/199. Recuperado el 4 de julio de 2017, de: http://www.un.org/es/comun/docs/?symbol=A/RES/58/199

Schmitt, M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Nueva York, Estados Unidos: Cambridge university press.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. En *Western Journal of Communication*. Estados Unidos: Western States Communication Association. Vol. 63, Núm. 3, pp. 384-412.

Unión Europea. (13 de diciembre de 2011). Directiva 2011/93/UE del Parlamento Europeo y del Consejo. Asunto: *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.*

Unión Europea. (2013). Comunicación conjunta al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. *Hacia una asociación renovada para el desarrollo UE-Pacífico*. JOIN(2012) 6 final. Bruselas. Recuperado el 4 de mayo de 2017, de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012JC0006&from=ES

Whittaker, J. (2004). *The Cyberspace Handbook*. Londres y Nueva York: Routledge.

Yubal Fm (2017. Febrero, 10). Deep Web, Dark Web y Darknet: éstas son las diferencias. Recuperado el 4 de julio de 2017, de: https://www.xataka.com/aplicaciones/deep-web-dark-web-y-darknet-cuales-son-las-diferencias

Anexos

Anexo 1. Normativa nacional relacionada con asuntos de seguridad digital

Norma	Contenido
Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. Ley.
	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2° y 5°), el principio de equivalencia funcional (artículos 6°, 8°, 7°, 28°, 12° y 13°), la autenticación electrónica (artículo 17°), la firma electrónica simple (artículo 7°), la firma digital (artículo 28°), y la firma electrónica certificada (artículo 30°, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el

	aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información
Ley 906 de 2004 (Código de Procedimiento Penal	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004)
Ley 962 de 2005 (racionalización de trámites y procedimientos	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de lo´ 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 1032 de 2006 (derechos de autor y conexos	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración y documentos y haga notificaciones por medios electrónicos para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley 1273 de 2009 (Delitos Cibernéticos)	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC

Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños	A través de esta ley se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC, en primer lugar establece en el artículo 4 (autorregulación de café internet códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario
Ley 1341 de 2009 (Sector TIC	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 1727 de 2009 (Habeas Data	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información
Decreto 2952 de 2010 (Habeas Data)	Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial
Ley 1437 de 2011 (Uso de medios electrónicos Procedimiento Administrativo Electrónico)	Consagra la utilización de medios electrónicos en el procedimiento administrativo permitiendo adelantar los trámites y procedimientos administrativos por medios electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes

Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1474 de 2011 (Uso de medios tecnológicos	Esta norma permite la utilización de medios tecnológicos en los trámites y procedimientos judiciales, en las diligencias, práctica de pruebas y notificaciones de las decisiones
Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad	Se incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico. El artículo 26 de esta Ley, consagra que la SIC determinará las condiciones mínimas bajo las cuales operar la información pública de precios de los productos que se ofrezcan a través de cualquier medio electrónico.
Ley 1564 de 2011 (Uso de las TIC	Permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Resolución CRC 3066 de 2011	Se establece el régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones. En particular, se establece que los proveedores de servicios de comunicaciones deberán implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor
Resolución CRC 3067 de 2011 "por a cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"	Está Resolución establece en el artículo 2.3, que los proveedores que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo
Resolución CRC 3502 de 2011 (Neutralidad de Internet)	A través de la Resolución CRC 3502 de 2011, se establecen condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011 (PND 2010 2014). Se contempla en el artículo 3 los principios de libre elección, no discriminación,

	transparencia e información, que deben aplicar los proveedores que prestan el servicio de acceso a internet
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios
Ley 1712 de 2012 (Uso de las TIC	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
Decreto 1704 de 2012 (Interceptación legal de comunicaciones	Este Decreto determina que la interceptación legal de comunicaciones, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional, deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.
Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del Viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente le encarga a la Dirección de seguridad pública y de infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el

	sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa
Decreto Ley 019 de 2012 (Entidades de Certificación Digital	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999, entre otras.
Resolución SIC No. 76434 de 2012 (Habeas Data	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países
Decreto 2364 de 2012 (Firma electrónica)	Establece la reglamentación del artículo 7° de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Se definen algunas características que benefician el uso de los medios electrónicos, tales como la definición de los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación, la fijación de la relación de género y especie entre firmas electrónicas y firmas digitales, señalando las diferencias en su tratamiento probatorio, pues en el último mecanismo existe una inversión probatoria, y el uso de la firma electrónica mediante acuerdo de las múltiples partes de una relación jurídica, entre otras.
Resolución 3933 de 2013 del Ministerio de Defensa Nacional (Crea y organiza grupos internos de trabajo)	Creó el Grupo colCERT y asignó funciones a la dependencia de la Dirección de seguridad pública y de infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.

Decreto 1377 de 2013 (Habeas Data)	Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados
Ley 1621 de 2013 para la función de inteligencia y contrainteligencia en Colombia)	Esta ley expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.
Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el Documento CONPES 3701, creo a través de este Decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.
Decreto 333 de 2014 (Habeas Data)	Se reglamenta el artículo 160 del Decreto 019 de 2012), definiendo el régimen de acreditación de las entidades de certificación abierta, en desarrollo de lo que define el artículo 160 del Decreto 019 de 2012 y se deroga el Decreto 1747 de 2000, que reglamenta de manera parcial la Ley 527 de 1999, referente a las entidades de certificación digital, certificados y firmas digitales, de manera que las entidades que deseen seguir prestando los servicios de certificación digital, deberán iniciar la correspondiente acreditación, ya no ante la Superintendencia de Industria y Comercio, sino ante el Organismo de Acreditación en Colombia (ONAC).
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los

	responsables del tratamiento
Decreto 2573 de 2014 (Gobierno en Línea)	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto compilatorio 1070 de 2015	Por medio del cual se reglamenta la Ley estatutaria 1621 de 2013, que establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos.
Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo)	Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012, 333 de 2014, entre otros.
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector.
Circular Externa SIC 02 del 3 de noviembre de 2015	Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015.

Nota: Elaboración propia con base en CONPES 3854.