Análisis comparativo de la estrategia ciber de Colombia vs estrategia ciber de Estados Unidos

Bernardo Antonio Rozo Delgado
Jose Miguel Obando
Miker Macareno Chacón
Jhon Jairo Segura Valencia

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

2019

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra

Análisis comparativo de la estrategia ciber de Colombia vs estrategia Ciber de Estados unidos

MY. BERNARDO ANTONIO ROZO DELGADO
MY. JOSE MIGUEL OBANDO
MY. MIKER MACARENO CHACON
MY. JHON JAIRO SEGURA VALENCIA

Director

JAIRO ANDRES CACERES GARCIA

Trabajo De Grado
Bogotá – Colombia
2019

Tabla de Contenido

ANALISIS COMPARATIVO DE LA ESTRATEGIA CIBER DE COLOMBIA VS ESTRATEGIACIBER DE ESTADOS UNIDOS

Resumen

En las sociedades globalizadas actuales, el índice de desarrollo es el principal indicador de un Estado, y cuanto mayor es el índice de desarrollo, mayor dependencia se tiene de los sistemas de información y comunicaciones. Cualquier interrupción de dichos sistemas o de las redes de infraestructura que usan de soporte, puede afectar al funcionamiento de los mismos, y sus efectos pueden llegar a ser catastróficos. Teniendo en cuenta la anterior acepción, este trabajo se centra en un análisis comparativo de la estrategia ciber de Estados Unidos frente a la estrategia de Colombia. En ese orden de ideas, este análisis parte del hecho que mientras que en los conflictos tradicionales existen fronteras y límites, en el *ciberespacio* no. Por esta razón, la descripción de las estrategias de ambos países parte del hecho que para realizar un *ciberataque* no es necesario desplazarse, moverse o tener que pasar una frontera. Ya que, esta es una de las principales características de este tipo de fenómeno. El *ciberespacio* es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser fácilmente clandestino. De la misma manera, se analizará como las estrategias de ambos países actúan para contrarrestar el grado de conocimiento que necesita un atacante para realizar una agresión a los sistemas de información. Por último, se describirá la calidad y disponibilidad de herramientas ofensivas para hacer frente a la amenaza, partiendo del hecho que actualmente es relativamente fácil encontrar en Internet multitud de herramientas de *hacking* que se intercambian en los diferentes foros dedicados a esta materia.

Palabras clave: ciberataque, hacking, ciberespacio, estrategia, asimétrico.

Abstract

In today's globalized societies, the development index is the main indicator of a State, and the higher the development index, the greater the dependence on information and communications systems. Any interruption of these systems or of the infrastructure networks that they use as support can affect their operation, and their effects can become catastrophic. Taking into account the previous acceptance, this work focuses on a comparative analysis of the cyber strategy of the United States versus the strategy of Colombia. In that order of ideas, this analysis starts from the fact that while in traditional conflicts there are borders and limits, in cyberspace no. For this reason, the description of the strategies of both countries is based on the fact that it is done to fulfill the obligation, it is not necessary to move, move or have to cross a border. Since, this is one of the main characteristics of this type of phenomenon. Cyberspace is a unique environment, without geographical boundaries, anonymous, asymmetric and can be easily clandestine. In the same way, analyze how the strategies of both countries act to counteract the degree of knowledge that an attacker needs to make an attack on the information systems. Finally, the quality and availability of offensive tools to deal with the threat is described, based on the fact that it is currently relatively easy to find on the Internet a multitude of piracy tools that are exchanged in the different forums dedicated to this matter.

Keywords: cyberattack, hacking, cyberspace, strategy, asymmetric.

Introducción

La rápida y constante evolución de la tecnología y los nuevos retos y amenazas existentes para cada uno de los estados ha revolucionado la visión y los alcances en las estrategias políticas y económicas, pero en especial en las militares entendidas como la defensa de los estados en un nuevo escenario como la Cibernética y dentro de ella la ciberseguridad y ciberdefensa, términos que ocupan hoy el primer lugar en la generación de estrategias de seguridad y avance de un país.

En esta etapa, Colombia no ha sido ajeno a esta nueva era de la tecnología y ha iniciado los pasos lógicos de planear, instaurar, verificar y continuar mejorando las políticas, procedimientos y análisis de riesgos ante la amenaza cibernética con el propósito de garantizar la seguridad de los ciudadanos, la economía del país, la infraestructura crítica y obviamente la seguridad y defensa del Estado, pero aun, con los esfuerzos dados, el ciberdelito está creciendo y siendo cada vez más real en el intento de sus propósitos. Por esto, se hace imperativo que el sistema ciberseguridad y ciberdefensa del país, sea analizado y mejorado con el firme propósito de estar en la vanguardia a nivel regional y mundial. Para ello, Colombia ha contado con el apoyo de la más desarrollada tecnología y capacitación por parte de los Estados Unidos como país referente en el tema cibernético.

Siguiendo esa línea, Colombia ha expedido dos Documentos COMPES[1] y ha establecido una organización a nivel multisectorial para la prevención y defensa del ciberespacio contando con una serie de avances que mantienen un nivel de protección sobre las amenazas. Es así, que las

[1] El Consejo Nacional de Política Económica y Social (CONPES) fue creado por la Ley 19 de 1958. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. Para lograrlo, coordina y orienta a los organismos encargados de la dirección económica y social en el Gobierno, a través del estudio y aprobación de documentos sobre el desarrollo de políticas generales que son presentados en sesión. El Departamento Nacional de Planeación desempeña las funciones de Secretaría Ejecutiva del CONPES.

Fuerzas Militares y de Policía han adquirido capacidades en el campo de ciberdefensa. De la misma manera, con la implementación de estas políticas se ha generado una dinámica integral de las instituciones del Estado, instituciones privadas y los ciudadanos. Quienes, en una visión de protección, prevención y ejecución de las medidas adoptadas, permiten la protección del ciber espacio y garantizan así una fortaleza en el aspecto de ciberseguridad y defensa del país de acuerdo a los nuevos retos que trae consigo el avance indetenible de la tecnología a nivel mundial.

Teniendo en cuenta lo anterior, este trabajo se centrará en describir mediante un análisis comparativo de las políticas estratégicas de Estados Unidos, cómo, la implementación de los documentos COMPES en política ciber, han sido efectivos para crear un ámbito de ciberdefensa estatal. Sin embargo, este avance no es suficiente ante la dinámica de las amenazas emergentes que el mundo globalizado impone diariamente. Todo ello, conforma un escenario de nuevos riesgos para el que es necesario que los distintos gobiernos desarrollen planes o estrategias, y se contemple la ciberdefensa como un riesgo al que es preciso hacer frente para la mejora de la seguridad nacional.

Verbigracia de lo anterior, organizaciones intergubernamentales como La OTAN han definido la ciberdefensa como "la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los *ciberataques*" (MC0571 - NATO *Cyber Defence Concept*). Partiendo de esta premisa, se puede evidenciar que el termino define en términos generales la estrategia de defenderse de ataques de un ambiente complejo, dado que influyen factores muy diversos. Uno de ellos, es el hecho de que muchos de los objetivos susceptibles de ser atacados se encuentran en manos de empresas privadas, por lo que su seguridad depende en gran medida de las acciones que toman estas para salvaguardar sus

sistemas, debiendo asumir unos costes que en ocasiones no son asumidos y así se concreta el riesgo (Cáceres, 2017).

De la misma manera, otro factor importante es la falta de conciencia en seguridad en algunas partes de la sociedad, lo que dificulta tomar medidas eficaces, medidas que, en todo caso, debería coordinar el gobierno. La Ciberdefensa es, por tanto, un ámbito de la seguridad nacional en el que los estados deberán tomar determinadas medidas, que deberán ejecutarse en coordinación con los sectores público y privado, ser compatibles con los derechos y libertades individuales, ser coordinadas con otras acciones tomadas para responder a otras modalidades de agresión, establecer sistemas de respuesta a los ciberataques y fomentar la cooperación internacional (Cano, 2017).

Por todo lo anterior, en la presente monografía se han recogido las iniciativas de Colombia en materia de ciberdefensa y se han comparado con las estrategias de Estados Unidos como punto de referencia. Este trabajo, constituye un intento de recopilación de información y de referencias que sirve de punto de partida para comprender el concepto de ciberdefensa, y para valorar su alcance y su influencia en la estrategia de seguridad nacional.

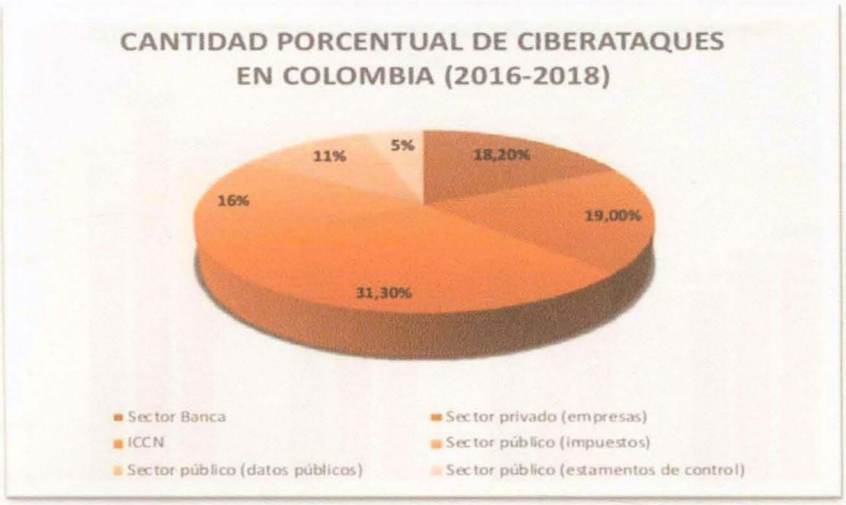
Descripción del problema

Amenazas con naturalezas complejas han salido a luz gracias al concepto de globalización. El intercambio fluido en redes de comunicación y demás criterios asociados el modelo "ciber" ha requerido la construcción y estructuración de nuevas formas estratégicas para dar garantía al prototipo de seguridad y defensa nacional.

No obstante, a pesar de que el Estado colombiano cuenta en la actualidad con el documento CONPES No 3701 donde se conforma la Comisión Intersectorial, con representación del Ministerio de defensa Nacional, ColCERT (El término CERT se deriva de las siglas en inglés "Computer Emergency Response Team" y está conformando por un equipo de personas dedicadas a la gestión de incidente con el objetivo de mitigar el riesgo y dar respuesta a incidentes de tipo cibernético), el Comando Conjunto Cibernético en el Comando General de las Fuerzas Militares y finalmente el Centro Cibernético Policial estamentos que conducen actividades propias a fin de controlar, disminuir y neutralizar todo tipo de acción "ciber" que intente afectar la Infraestructura Crítica Cibernética de la Nación (ICCN), de ahí el papel del estado se ha visto en la obligación de afrontar diferentes etapas en las que ha existido un aumento de los ciber ataques que se aproxima al 37,2% en referencia a la cantidad de ciber ataques recibidos durante el periodo de tiempo que comprendió a los años 2002-2010. (2,337,251).

El aumento de los ciberataques deja en claro, que si bien la comisión intersectorial ha sido útil para contrarrestar gran parte los ataques generados de modo ciber, los efectos y alcances inmediatos que puedan contrapesar el crecimiento numérico de los ciber ataques, mucho más de los que reposa en las "ciber-ofensas a la ICCN". (Gráfica 1)

Gráfica 1 Cantidad porcentual de ciber ataques a 2018



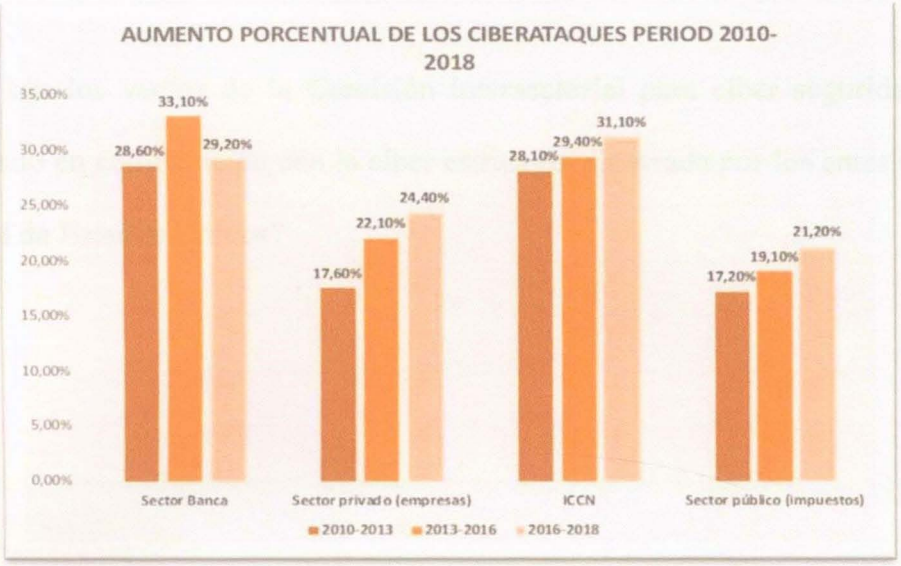
Fuente: información extraída de ISIC (2019)

Esta situación, es decir, la capacidad efectiva de la Comisión Intersectorial diseñada, demanda un análisis que se pueda utilizar en varios medios es decir intermodal que genere aspectos a favor y en contra del modelo funcional y estructural empleado por el Comando Conjunto Cibernético de las FF.MM.

Esto, teniendo en cuenta que, aunque la estrategia ya existe y se encuentra en funcionamiento, esta podría carecer de elementos o de fases primordiales capaces de garantizar el cumplimiento propio del objetivo propuesto, en este caso, ligada a la proposición político-pública exigida en el CONPES 3701 "Lineamientos de política para Ciberseguridad y Ciberdefensa" del 14 de julio de 2011 y el CONPES 3854 "Política Nacional de Seguridad Digital".

Es de recalcar, que a pesar de haber iniciado una campaña en términos de ciber seguridad y ciber defensa desde el año 2011, la estrategia no ha satisfecho el lineamiento intersectorial para la ciber seguridad ya que, si se observa la gráfica 2 pueden ser advertidos dos patrones diferentes: la constante evolución de los ciberataques y la cantidad numérica en aumento.

Gráfica 2 Aumento porcentual de los ciber-ataques 2010-2018



Fuente: información extraída de ISIC (2019)

Por consiguiente, el problema en descripción surgiría de una aparente insuficiencia de los alcances efectivos de parte de la Comisión Intersectorial, lo que exige un análisis de la estrategia del Comando Conjunto Cibernético de las FF.MM. que pueda demarcar cuáles serían las falencias funcionales de la estrategia planteada en comparación con proposiciones estratégicas internacionales altamente efectivas, funcionales e intersectoriales, para el caso de la presente investigación, haciendo referencia a la estrategia de Ciberseguridad y Ciberdefensa diseñada por el Gobierno de EE.UU., publicada en el año 2018.

Pregunta de investigación

¿Cuáles son los vacíos de la Comisión intersectorial para ciber seguridad defensa del Estado colombiano en comparación con la ciber estrategia planteada por los entes de seguridad y defensa nacional de Estados Unidos?

Justificación

Esta investigación esboza un análisis primario de las diferencias y necesidades contenidas en la estrategia de ciberseguridad y ciberdefensa diseñada por el Comando Conjunto Cibernético de las FF.MM. Su justificación, surge por la necesidad conocer cuáles podrían ser los vacíos funcionales utilizados por las diferentes ciberamenzas que buscan desestabilizar por este medio las entidades del país en lo público y privado.

El desarrollo investigativo concederá a la institución un estudio en el que se pueda analizar la analogía de los conceptos básicos para la seguridad y defensa nacional y la reinterpretación del concepto de "domino y guerra", el cual está encaminado a determinar con amplio detalle que el ciberespacio habría de convertirse en el quinto dominio de interés para los actores en conflicto.

De igual manera, el estudio por desarrollar comparará la capacidad efectiva de la estrategia intersectorial que se encuentra descrita en los Conpes 3701 y 3854, con el alcance práctico que posee la ciber estrategia de seguridad y defensa nacional de Estados Unidos, la anterior, constituida por las entidades encargadas del control para el ciber espacio.

Esta comparación busca un análisis y observación que permita identificar cuáles son las similitudes entre ambas estrategias y cuáles jugarán un rol como elementos de comparación hábiles para demarcar diferencias.

La investigación expondrá de igual manera un resultado mediante el desarrollo de los ejercicios de comparación entre ambas estrategias, el proceder investigativo examinará posibles funciones en las que existan espacios operacionales poco efectivos en comparación con el crecimiento evolutivo de las ciber amenazas.

Finalmente, el motivo principal para justificar el desarrollo de esta investigación hará parte de una búsqueda que identifique vacíos proporcionales, ligados al esquema operativo de la Estrategia Intersectorial. Es importante estimar que esta búsqueda comparará la ciber-estrategia nacional, de alcances moderados, con una ciber-estrategia internacional de alcances óptimos (ciber-estrategia Estadounidense).

Objetivos

Objetivo general

- **Identificar** los vacíos en la función y estructura de la Estrategia Nacional de Ciber seguridad y ciberdefensa del Estado colombiano **a través** de un análisis comparativo entre la estrategia intersectorial y la ciber-estrategia estadounidense.

Objetivos específicos

- **Realizar** un estudio interpretativo de los CONPES 3701 del 2011 y 3854 del 2016 **mediante** el uso de una herramienta de comparación orientada a la relación de objetivos, metas planteadas, herramientas, actores involucrados y sistemas funcionales.

- **Desarrollar** un análisis de observación directa sobre la estrategia intersectorial planteada por el Comando Conjunto Cibernético de las Fuerzas Militares **mediante** un análisis que permita identificar propósitos, métodos y alcances.

- **Efectuar** un ejercicio de comparación de los sistemas de función de la estrategia intersectorial colombiana y de la ciber estrategia estadounidense desarrollando un estudio paralelo de conceptos y sistemas empleados por ambas proposiciones ciber-operacionales.

Marco metodológico

En esta investigación se utilizarán los direccionamientos metodológicos de autores como Camacho & Rodríguez (2015). Estos investigadores explican que una investigación debería estar direccionada mediante la materialización de cuatro títulos primarios: el enfoque de la investigación, el tipo de estudio de la investigación y fuentes de información.

Enfoque de la investigación

Esta investigación posee un enfoque cualitativo. Este enfoque facilita la búsqueda y análisis de información mediante el uso de métodos inductivos y recurrentes. Estos métodos incluirán el desarrollo de análisis fundamentados en los que la comparación entre ambas ciber-estrategias (colombiana y norteamericana) podrá arrojar al final de la investigación una serie de resultados amparados en un marco metodológico caracterizado por los puntos convergencia del entorno en el tema ciber.

Tipo de estudio

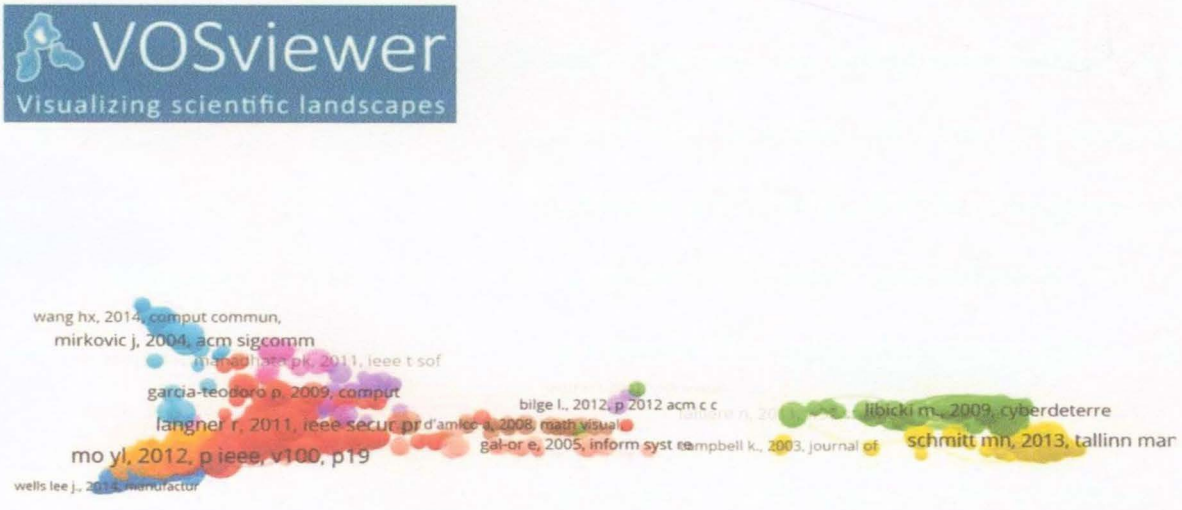
El tipo de estudio para esta investigación pertenece a la categoría propositiva, lo que significa que los marcos metodológicos para la búsqueda de la información corresponderán a la orientación de variable parecidas, desarrollando de esta manera categorías cualitativas de estudio. Para esta investigación, las categorías harían parte de la siguiente línea: ciberseguridad, ciberdefensa, ciberataques y ciber estrategias.

Tipo de muestra

La muestra a utilizar por la investigación hace parte de la clasificación: análisis tipo-caso de categorías teóricas o conceptuales. Para esta investigación, la conceptualización, descripción, entendimiento e interrelación de las fuentes de información harán más efectiva la triangulación de los datos objetivos a recolectar.

Fuentes de información

Para identificar las fuentes de información necesarias durante el desarrollo de la investigación es utilizado en primera instancia el software Vos Viewer. En este son buscadas las referencias investigativas requeridas para la construcción de las bases teóricas y conceptuales del marco referencial. Los resultados son los siguientes:



El 78,4% de la información referencial se encuentra ubicada en autores anglosajones, pertenecientes a universidades como Harvard, MIT o Yale. El porcentaje restante hace parte de un clúster académico procedente de la China y de la Unión Europea. La investigación cuenta con un

número amplio de referencias temáticas empleables en la construcción de las distintas fases teóricas.

Asimismo, las fuentes secundarias para la recolección de la información son:

- CONPES temáticos, referentes a las problemáticas "ciberseguridad y ciberdefensa"
- Estrategia de ciber seguridad y ciberdefensa norteamericana. Cabe aclarar que esta política es pública y no posee ningún grado de confidencialidad

Estado del arte

Hablar de Ciberdefensa y Ciberseguridad es hablar de un paradigma innovador, el cual permite analizar la caracterización internacional de nuevas formas y tipologías de amenazas impactantes para el concepto de seguridad y defensa nacional.

Desde 1998, de acuerdo a Furnell (2002), el acceso masivo a internet ha facilitado a los piratas informáticos el desarrollo de tendencias complejas, todas estas correlacionadas a la ruptura determinista de una paz intangible, cualificada por el precepto de estabilidad manifestado por los estamentos de seguridad y defensa nacional. Investigar la naturaleza existencial del cibercrimen, sin analizar la evolución cuántica de los nichos poblacionales hacia el uso de internet ad hoc, sería desvariar ante un precepto intersectorial, cuya función primaria surge en la concurrencia y materialización de acciones delictivas, todas estas derivadas de la intención objetivista de la amenaza.

En concordancia con Ciardhuáin (2004), la masificación del acceso a internet significaría para la estructura de defensa y seguridad internacional un reto de características multidimensionales, puesto que la no tradicionalidad del método permitía a los actores ilegales confluir y converger en un cúmulo de propuestas ilegales praxeológicas, útiles en la desestabilización de la razón antropocéntrica del Estado. Por ende, afirma Ciardhuáin (2004):

> (...) existe una relación directa entre internet, acceso, objetivos criminales y nuevas formas de interdicción. Es decir, desde 1998 la característica criminal dejo de lado al remanente tradicional, mientras que adaptaba nuevas formas de intervención subjetivistas. Dichos métodos, facilitarían al esquema criminal un ingreso directo e indetectable a formas de desestabilización sobre el esquema del statu quo nunca antes imaginadas. (p. 63)

La posición de Ciardhuáin (2004), es imprescindible para demostrar que si existió un dinamizador en la naturaleza transmutativa de las amenazas. Este catalizador permitiría explorar un ciberespacio del que dependerían, con posterioridad, el 91,7% de los sistemas co-existenciales a nivel mundial. Desde una perspectiva reflectivista el acceso a internet se convertiría a un canal de nuevas formas de crimen, las cuales, para 1998, no poseían un marco institucional jurídico o incluso público que permitiría a los gobiernos tipificar el hecho desde el axioma jurídico. Frente a esta ponencia, McQuade (2006) expone que:

> (...) no solo existió un paramento correlacional entre internet y nuevas formas de crimen, sino también un paradigma holístico que integraba, por primera vez en la historia, tres variables de afección, las cuales involucraban a: objetivos ilegales, ser humano y tecnología. (p. 114)

El aporte de McQuade (2006), es claro para describir una ecuación estatocéntrica, cuya funcionalidad radica en la evolución paralelista de dos variables divergentes: el acceso a internet y el aumento de los ciberataques. (Ver figura 1)

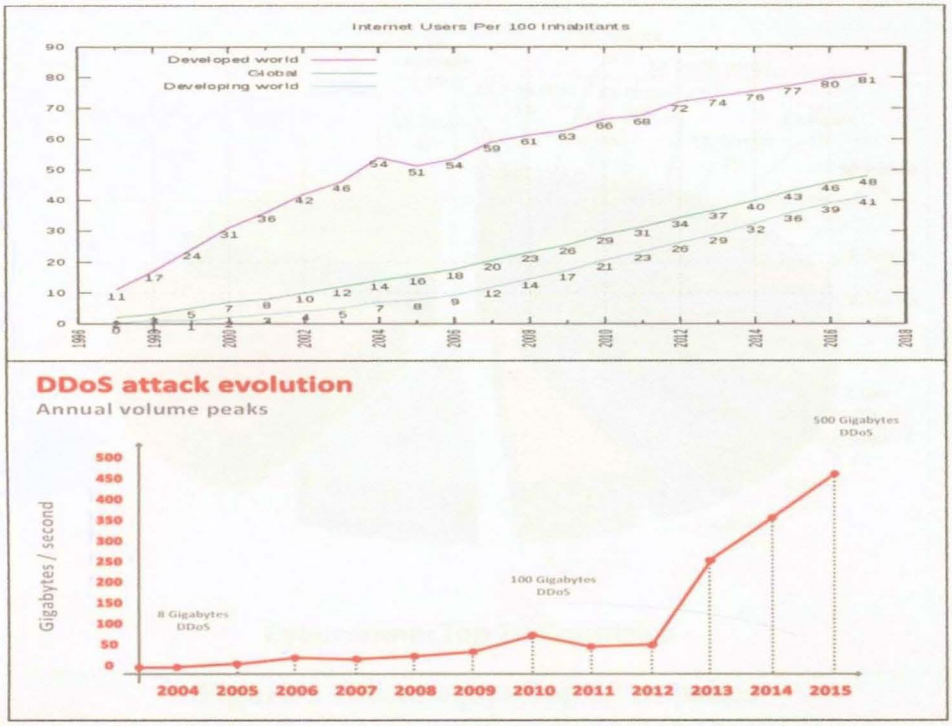


Figura 1 Correlación entre acceso a internet y evolución de ciberataques
Fuente: información recuperada de IMND (2017)

La figura anterior, facilita la realización de un análisis transeccional puesto que es notable un patrón paralelista entre el acceso a internet y el crecimiento anual de ciberataques a nivel mundial. Sin embargo, afirma Waxman (2011), la atomización de ataques cibernéticos es desigual, ya que el acceso a internet es diferencial, dinámico y no masificado. Dicho de otra forma, no se podría esperar un ciberataque de impacto sobre el rendimiento gubernamental y público de una nación que no posea acceso inter-variado, masificado y constante a la red. Este factor ha delimitado la acción criminal de las amenazas, puesto que no todos los Estados poseen la misma capacidad instalada. Sin embargo, la constante mencionada permite entrever una distribución de ciberataques altamente interconectada a la masificación de internet como medio o herramienta de comunicación. Es decir, en las naciones en las que existe un mayor acceso a internet, existe también un riesgo propenso e inminente.

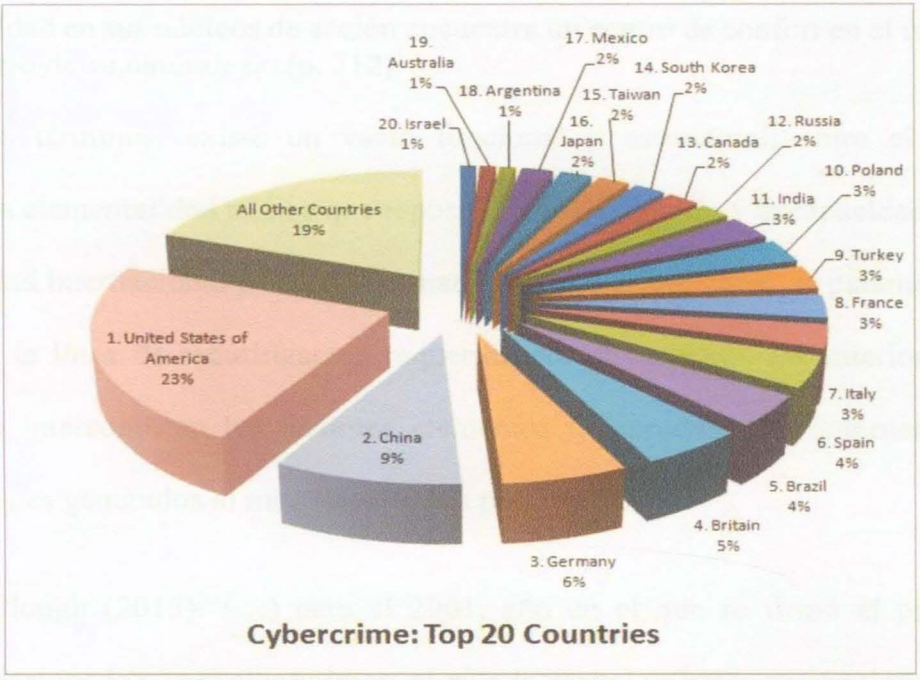


Figura 2 Ciberataques Top 20 en países
Fuente: información recuperada de IMND (2017)

En relación con la ponencia de Mc Quade (2006), Anderson, Barton, Böhme, Clayton, Van Eeten, Levi & Savage (2013) aportan al debate una nueva concepción investigativa, la cual propicia la utilización de los conceptos de ciberdefensa y ciberseguridad a partir de una matriz de ataques sobre los sistemas de seguridad nacional, los sistemas interdependientes y los paradigmas interestatales. Es decir, la presunción de Anderson et al. (2013) sería explicita sí se entendiera que la prevención del cibercrimen surge de una necesidad gubernamental relacionada con la disminución de impactos sociopolíticos, socioeconómicos y socioculturales derivados de la acción tangible de un ente antes desconocido. De esta forma, la estructuración epistemológica de Anderson et al. (2013) expone a ciberseguridad y a ciberdefensa como a dos herramientas complejas, pero útiles en la desarticulación de actividades criminales caracterizadas por un alto nivel de clandestinidad e intangibilidad. De acuerdo con Anderson et al. (2013):

> El cibercrimen es aún un paradigma, cuya fenomenología no solo es inentendible, sino también altamente transformacional y evolutiva. La

> volatilidad en sus núcleos de acción encuentra un centro de confort en el carácter complejo de su naturaleza. (p. 212)

En otros términos, existe un vacío funcional y estructural; entre el entendimiento pragmático de la elementalidad ad hoc que reposa en el cibercrimen y la capacidad de los Estados y de la comunidad internacional per se relacionada con la configuración de parámetros y políticas adecuadas para la línea de secutirización requerida por el contexto. La anterior afirmación es analizable sí se interconectan los distintos elementos jurisprudenciales internacionales con la cantidad de ataques generados al momento de sus publicaciones.

Según Clough (2015):"(...) para el 2001, año en el que se firmó el primer consenso internacional relacionado con el cibercrimen, el mundo digital ya había presenciado un sin número de ciberataques provenientes de, al menos, 2.311.437 piratas informáticos" (p. 94). De acuerdo con el mismo autor, una de las bases del Convenio sobre Ciber-criminalidad de Budapest correspondía a la imperiosa necesidad que los Estados poseían en ese momento para hacerle frente a una dinámica delictiva, indescriptible e inentendible para la tradicionalidad de los métodos de acción procedentes de los estamentos de seguridad y defensa nacional. Por lo tanto, establecer una dinámica internacional que contrarrestara el impacto bidimensional – económico y militar- de los ciberataques traería condigo la reunión formal de las principales potencias afectadas, en este caso, Estados Unidos, Japón, Inglaterra, Francia, España y Alemania (Slattery, 2014).

Ahora bien, una vez establecido el CCCB (Convenio sobre Ciber-criminalidad de Budapest) y teniendo en cuenta el impacto generado por el código criminal Moonligth Maze- el cual afectó de manera colateral al 11.3% de los sistemas bancarios en Norte América y en la U.E. (Slattery, 2014)- la OEA tomó la determinación de crear una resolución que pudiera establecer un sistema de seguridad cibernética hemisférica, con el propósito de disminuir los porcentajes

evaluados durante la VI Conferencia para la Seguridad Intersectorial realizada en el año 2004. De acuerdo con el análisis circunstancial y con las ponencias investigativas de Ron (2016):

> (...) se hacía fundamental para las Américas establecer un sistema de seguridad que pudiera controvertir el creciente impacto de amenazas intangibles, no materiales, cibernéticas, capaces de desarticular el concepto funcional de los diferentes sistemas que conformaban el estándar democrático de los Estados. (p. 52)

Por tal razón, la OEA daría vida a la Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores – CSIRT, la cual tendría como función objetiva el diseño y configuración de una red interestatal encargada de prevenir y disminuir el riesgo interdinámico derivado del accionar delictivo por parte de los piratas informáticos. Para Ron (2016), dicha red era ineficiente ya que la misma fue creada a partir del análisis descriptivo de los contextos retrospectivos correlacionados con la tecnología y con el mundo digital, no considerando de esta forma que la criminalidad cibernética no solo era transmutativa sino altamente evolutiva, ya que su naturaleza crecería a la par con los últimos desarrollos investigativos en materias cibernéticas.

La argumentación de Ron (2016), es lógica si se tiene en cuenta que para el 2004 el riesgo estipulado radicada en un porcentaje no mayor al 24,1%, siendo que para el 2007 el riesgo proyectado se acercaría al 48,6%. (Ver figura 3)

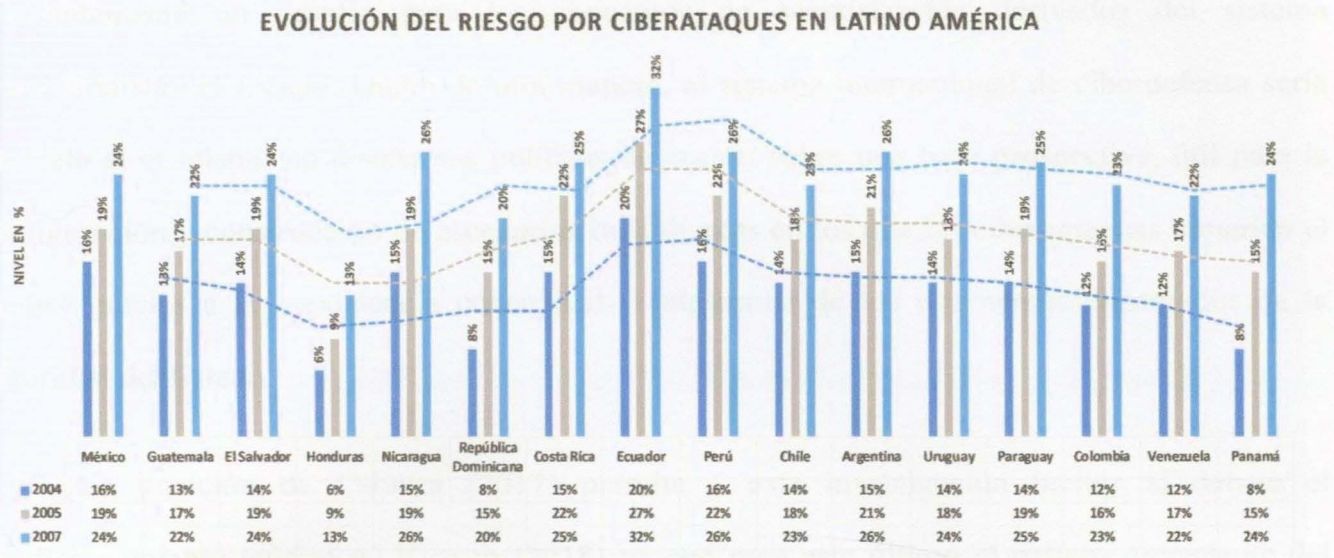


Figura 3 Evolución del riesgo por ciberataques en Latinoamérica
Fuente: elaboración propia con información recuperada de OEA (2017) e IDMN (2015)

Frente a esta ponencia, Cabrera (2017) establecería entonces una nueva forma de analizar el paradigma de seguridad y defensa nacional, el cual sugeriría a los Estados el establecimiento de organismos especiales, todos estos micro-focalizados hacia la conceptualización, contextualización y entendimiento hermenéutico y praxeológico de la ciberamenzas. La posición de Cabrera (2017) expone que:

> (…) el cibercrimen obedece a una nueva clase de acción delictiva, la cual no puede categorizarse o neutralizarse a través de la tradicionalidad operativa militar estatal. Los desafíos impuestos por un ciber pirata exigen a los estamentos de seguridad nuevas formas de intervención e interacción en las que la estrategia no depende únicamente de la capacidad física y efectiva del concepto operacional, ya que la naturaleza intangible de la acción demandada a los actores la desarticulación de la intencionalidad objetiva a partir de un esquema de seguridad correlativo al direccionamiento tecnológico, digital y ciber-dinámico de los estamentos para la seguridad nacional e internacional. (p. 53)

Por tal razón, el cibercrimen pasaría a ser considerado, según Cabrera (2017), una manera de interdicción ilegal, la cual no posee barrera alguna, pues su tipología evolutiva contraería

constantemente un desafío para los conceptos de secutirización derivados del sistema proteccionista del Estado. Dicho de otra manera, el sistema internacional de ciberdefensa sería obsoleto si el mismo no diseña sus políticas de acción sobre una base prospectiva, útil para la configuración y construcción de escenarios delimitantes en los que las ciberamenzas tomarían el control gracias a la inexistencia conceptual e intelectual de los estamentos encargados de la seguridad del Estado.

La posición de Cabrera (2017) permite a esta investigación incluir al debate el condicionamiento teórico de Kirwan (2018) ya que para este último el peligro procedente del impacto ciber criminal obedece a una sistematización constructivista, puesto que sus efectos involucran a ambos actores: el Estado ad hoc y la empresa privada. Dicha ponencia, deduciría entonces que el sentido natural de una ciberamenaza no es estatocentrista, es reflectivista y busca desarticular el paradigma de control en cada uno de los factos que conforman al conglomerado social. Una muestra de lo anterior, según Kirwan (2018), puede verse desde la siguiente figura. En ella se exponen los principales campos del concepto social atacados por el accionar delictivo del cibercrimen.

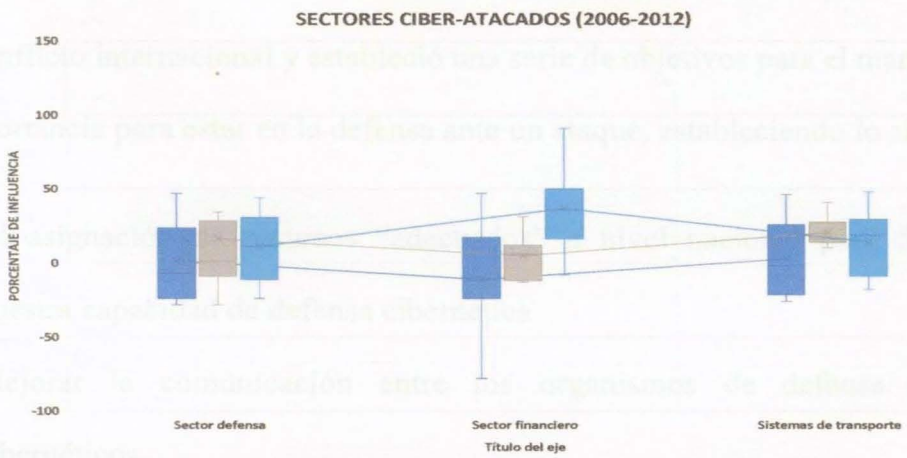


Figura 4 Estadística general de sectores ciber atacados
Fuente: elaboración propia con información recuperada de OEA (2017) e IDMN (2015)

La figura expuesta permite analizar que el sector defensa, a nivel mundial, es el área funcional con más impacto por el accionar constante del cibercrimen. Sin embargo, es menester recordar que el sector defensa cuenta con una serie de sistemas alineados para la conformación de defensas cibernéticas, útiles en la neutralización de afecciones o efectos dirigidos por cualquier clase de ciberamenzas (Malwares, Worms, trojan horses, Blended Threats, Spy-eyes o inclusive spams). La ponencia expuesta daría a entender que las áreas más afectadas durante la primera década del siglo XXI estarían asociadas con: sistemas financieros y banca internacional y transportes públicos.

De igual manera se deben contextualizar los nuevos retos vistos desde la óptica de la OTAN bajo el concepto de la diferenciación de las guerras del siglo XXI las cuales ya no se desarrollan únicamente por tierra, mar y aire se maneja ahora el florecimiento del internet que puso al ciberespacio como un nuevo escenario para todos los Ejércitos del mundo donde se debe poner ante todo la protección de los intereses estratégicos, digitales, infraestructura critica.

Basado en estos criterios la OTAN ha puesto en la pirámide de importancia la ciberdefensa en un hipotético caso de conflicto siendo este anexo al llamado dominio operacional y esencial en caso de un conflicto internacional y estableció una serie de objetivos para el manejo de este nuevo factor de importancia para estar en la defensa ante un ataque, estableciendo lo siguiente.

1. La asignación de recursos "adecuados" a nivel nacional para fortalecer nuestra capacidad de defensa cibernética
2. Mejorar la comunicación entre los organismos de defensa nacional cibernéticos

3. Mejorar la comprensión de las amenazas informáticas, incluyendo el intercambio de información y sus evaluaciones
4. Mejorar las habilidades y el conocimiento de la "salud cibernética fundamental" a través de las defensas cibernéticas más sofisticadas y robustas
5. Mejorar la educación en seguridad cibernética, la formación y los ensayos estratégicos.
6. Acelerar la ejecución de los compromisos de ciberdefensa, incluyendo aquellos sistemas nacionales de los que la OTAN depende. (Edición revista digital OTAN)

Es así, como dentro del nuevo papel de Colombia como único país latinoamericano vinculado a como socio estratégico en la OTAN, conjuntamente desarrollaran en el país unos aportes a la estrategia en materia de ciberseguridad de acuerdo al anuncio del Presidente Iván Duque y el señor Jens Stoltenberg en Bruselas. Esta estrategia conjunta, busca la disminución del riesgo en cuantos ataques y exposición de los ciudadanos, las instituciones del estado y las instituciones privadas ante los ataques cibernéticos.

Marco teórico

Ciberdefensa, relación objetiva entre el concepto de seguridad y defensa nacional

La interconexión que existe entre ambos conceptos es un derivado hermenéutico que proviene de la relación epistemológica existente entre: seguridad integral, defensa nacional y seguridad intersectorial. Para analizar el concepto de ciberdefensa es fundamental incluir en el debate la definición de Geers (2011) quien afirma que:

> La defensa y seguridad cibernética ha evolucionado rápidamente de una disciplina técnica a un concepto estratégico. La globalización e Internet han otorgado a las personas, organizaciones y naciones un nuevo poder increíble, basado en la tecnología de redes en constante desarrollo. Para todos, estudiantes, soldados, espías, propagandistas, piratas informáticos y terroristas: la recopilación de información, las comunicaciones, la recaudación de fondos y las relaciones públicas se han digitalizado y revolucionado. (p. 09).

La ponencia de Geers (2011), es útil para demarcar nuevamente que si existe una relación dinámica entre; acceso a internet, ciberdefensa y ciberataques. Sin embargo, la exposición de Geers (2011), no está completa si se tiene en cuenta que el acceso a internet no es razón suficiente para afirmar que dicho facto es el dinamizador primario del cibercrimen. Contrario a esto, y exponiendo el concepto teórico de Kirwan (2018), es imprescindible afirmar que para que exista un concepto criminal debe existir, primeramente, un paradigma intencional, un precepto objetivo y un catalizador ideológico. En algunos casos, explica el autor, no es requerida la conjunción o convergencia de las tres, lo que significaría entonces que la red sería considerada únicamente una herramienta de acceso, y no el dinamizador primario.

A partir de la conceptualización teórica de Kirwan (2018) podría ser redefinido el precepto funcional de ciberdefensa y ciberseguridad, proponiendo al primero como el mecanismo general,

radicado en la universalidad del concepto intrafronterizo de "defensa", mientras que el segundo pasaría a ser considerado el esquema principal, conformado por mecanismos interdinámicos, correlacionados con la intención de los Estados, el acceso a la red y la protección continua de la misma.

Ahora bien, a diferencia de Geers (2011) y Kirwan (2010), Choo (2011) interconecta las tres dialécticas; ciberdefensa, internet y objetividad a una sola estructura, la cual analiza el cibercrimen como a una respuesta pronta a dos factores de interés colectivo. La primera de ellas hace alusión al carácter subjetivo y anárquico. Es decir, las estadísticas demuestran, en EE.UU. por ejemplo, que no todos los ataques generados en el ciberespacio buscan extraer el elemento financiero de las organizaciones, ya que su intención principal no es otra que desestabilizar el esquema organizacional del banking en general. Frente a esta ponencia, el investigador diseña la figura que se relaciona a continuación. En ella pueden observarse, de acuerdo a la información recolectada en Statistics (2018), que las razones – valores porcentuales- por las que un cibercriminal ataca estamentos financieros no siempre están relacionados con la actividad del hurto per se.

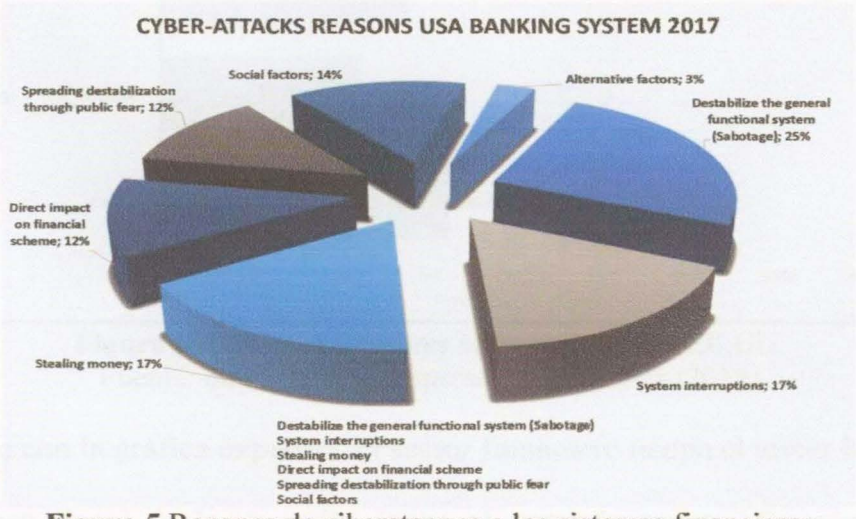


Figura 5 Razones de ciberataques a los sistemas financieros
Fuente: elaboración propia con información recuperada de Statistics (2018)

La figura anterior permite analizar que, efectivamente, no todos los ataques – durante el 2017- tuvieron como objetivo principal la extracción ilegal de dineros. Contrario a esto, la interrupción sobre el sistema y la desestabilización de los componentes funcionales en las entidades financieras ocuparon los puestos con mayor porcentaje. Esto permitiría analizar la existencia de una relación sistémica entre desacuerdo, insatisfacción, ciberataques y sistema financiero. Aunado a la estadística expuesta, Nykodym, Taylor & Vilela (2005) interponen una presunción teórica, la cual afirma que no solo existe dicha relación, sino que, desde un espectro paradigmático, el cibercrimen pasaría a ser un tipo de muestra social, la cual manifiesta un inconformismo general referente a la temática de banking y fluctuación financiera. Por otro lado, la afirmación de Nykodym et al. (2005) pierde validez una vez que se analizan los principales segmentos impactados por el cibercrimen durante el año 2018 en los Estados Unidos.

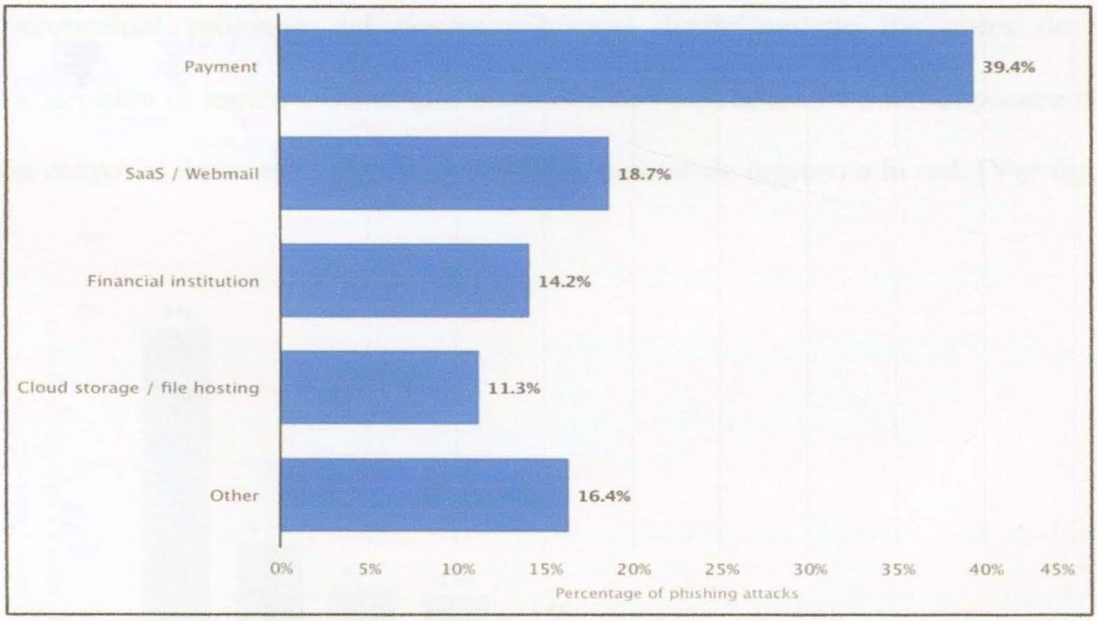


Figura 6 Principales sectores ciber atacados en EE.UU.
Fuente: información recuperada de Statistics (2018)

De acuerdo con la gráfica expuesta, el sector financiero ocupa el tercer lugar, mientras que el intento al acceso ilegal de los e-mails ocupa el segundo puesto. De una u otra forma, la

ciberseguridad, respuesta inmediata para contrarrestar el impacto venidero de los ciberataques, se convierte a la vez en una herramienta privada, puesto que los organismos de defensa no poseen la tecnología, el concepto prospectivo o incluso el recurso humano adecuado para hacerle frente a la interdicción ilegal practicada por los cibercriminales. Si bien, afirma Broadhurst (2006) "(...) la ciberdefensa se ha convertido en un canal secundario, ya que las empresas y economías privadas no están dispuestas a permitir el daño sobre los conceptos estructurarles, materiales o procedentes de la propiedad intelectual" (p. 71).

La posición del anterior autor expondría la categorización de una función social y empresarial determinística que no solo pondría en peligro la información privada de los usuarios, sino también cuestionaría de forma colateral la efectividad de los recursos cibernéticos empleados por el esquema gubernamental atacado. Si bien, argumenta Broadhurst (2006), la exposición al riesgo cibercriminal proviene del desconocimiento disciplinar de los entes de seguridad encargados, también es lógico afirmar que los países con más acceso a internet poseen un nivel de vulneración mayor al de otras naciones con escasas fuentes de ingreso a la red. (Ver figura 7)

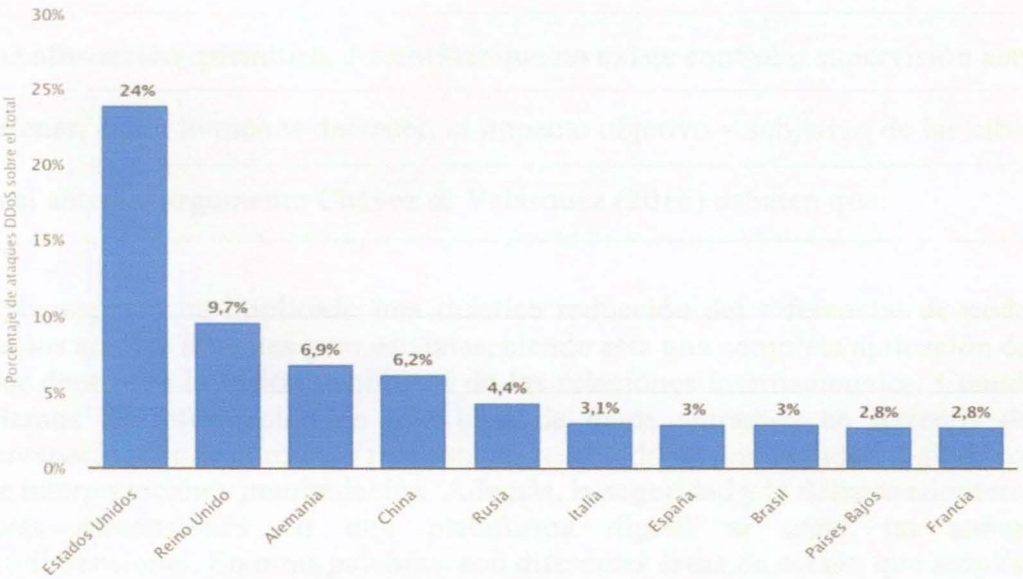


Figura 7 Principales países víctimas de ataque.
Fuente: información recuperada de Statistics (2018)

Como se puede observar, el porcentaje total de ataques DDoS durante al año 2017 correspondió a una subdivisión casi continental puesto que Norte América recibió el 24% de los ciberataques, mientras que el Reino Unido, Italia, España y Francia sumarían casi el 32% entre todas. Así mismo, y a pesar de ser una nación pionera en ciberseguridad, Rusia tuvo que afrontar el 4.4% de todos los ataques cibernéticos. Finalmente, el Brasil haría contrapeso al 3.3% de los ciberataques lanzados.

Todas estas naciones tienen tres factores en común. Primero, son hegemones competentes, cuyas naturalezas estatocéntricas mantienen a la mismas en un estado de continua competencia. Segundo, son naciones con extensas densidades poblacionales, y, por ende, con un amplio estándar de acceso a internet. Tercero, todas ellas compiten por el control de los diferentes sistemas internacionales asociados con el mercado. A pesar de poseer grandes sistemas de seguridad y defensa nacional todas estas poseen falencias reflejadas en las constantes violaciones a fuentes de información gubernamental o secuestro activo de datos de identificación procedentes de las diferentes fuentes diseñadas por entidades comerciales.

Esta última afirmación, permitiría determinar que no existe control o supervisión actual alguno que pueda detener, o por lo menos decrecer, el impacto objetivo y subjetivo de las ciberamenzas. Con relación al anterior argumento Chávez & Velásquez (2016) debaten que:

> El ciberespacio ha implicado una drástica reducción del diferencial de poder entre los actores estatales y no estatales, siendo esta una completa aplicación del poder dentro de la visión neoliberal de las relaciones internacionales. Cuando hablamos de información en una base de datos entramos en terrenos del ciberespacio, donde el mundo real está representado en una realidad digital, con libre interpretación y manipulación. Además, la seguridad y la defensa adquieren nuevas dimensiones en una plataforma digital al crear un campo multidimensional. En otras palabras, son diferentes áreas de acción que amplían el contexto habitual limitado, por lo general, por ambientes geográficos y

> pasando a ambientes virtuales en los cuales las ciberguerras ya se entienden como una realidad virtual, y donde obtener información es el factor más importante y el de la victoria. (p. 239)

La ponencia de estos investigadores incluye en la descripción de la relación que existe entre ciberdefensa, ciberseguridad y objetividad cibercriminal un elemento conceptual, el cual permite re-direccionar la intención subjetiva interpuesta por la hermenéutica axiomática asociada con la ciberdefensa, buscando de esta forma integrar en la definición del poder cibernético a los actores estatales y no estatales. Los actores involucrados a la presunción desarrollista de la esencialidad del núcleo de la ciberdefensa no siempre corresponden a la naturaleza estatocéntrica. Todo lo contrario, gran parte de los entes encargados de suministrar las constantes cutting edge en ciberseguridad hacen parte de una línea de firmas privadas que convierten la ciberdefensa en un sector de naturaleza público-privada. Para Carr (2016):

> A pesar de la centralidad en las estrategias de seguridad cibernética derivadas de los EE. UU. y del Reino Unido, la asociación público-privada es un arreglo nebuloso, que es especialmente problemática en el contexto de la protección de infraestructura crítica. La infraestructura crítica de propiedad y operación privada que se considera como una vulnerabilidad potencial de seguridad nacional plantea preguntas sobre la asignación de responsabilidades y la responsabilidad en términos de ciberseguridad. (p. 03)

La preocupación de Carr (2016) no surge únicamente de la insuficiencia de los alcances provenientes por ambos actores: firmas privadas y estamentos gubernamentales, sino también de la intervención directa que generan los sectores privados ante temáticas sensibles como datos, fuentes y elementos de acción que convertirían al sujeto, usuario o individuo en un ente vulnerable a la violación masiva y sistémica de sus derechos fundamentales, en especial sobre aquellos que reposan en la ley universal de Habeas Data. Apoyando la idea de Carr (2016), Rowe (2016) plantea que:

> (...) numerosas organizaciones compilan bases de datos de vulnerabilidades e información de parches y rastrean el número de incidentes reportados por las organizaciones de los EE. UU. De manera continua, muchas de estas son organizaciones privadas, como la empresa de seguridad contemporánea, que proporcionan dicha información solo a clientes y / o la utilizan para brindar la mejor seguridad a grandes personalidades jurídicas. Sin embargo, muchas organizaciones y consorcios privados y públicos también recopilan información sobre los tipos de ataques y su frecuencia y, en algunos casos, proporcionan soluciones generales o específicas para el producto. No obstante, los análisis actuales indican que esta información no puede usarse para predecir con precisión los ataques futuros en una red específica. (p. 04)

Por tanto, la ciberseguridad, herramienta principal para la estructura de ciberdefensa, no estaría bajo el total dominio de los estamentos públicos, convirtiendo la misma en un componente biparticionado, cuyo acceso es público y privado, desestructurando y desarticulando el alcance constitucional o jurisprudencial de los actores estatales encargados del precepto general de seguridad nacional. Otro de los aportes claves para entender el concepto de ciberdefensa, visto este como un paradigma subsecuente procedente de la actividad internacional relacionada con la seguridad informática y digital yace en la proposición conceptual de Rowe (2016). Para este investigador existe un elemento catalizador, cuya función principal busca entregar a la estructura funcional de la ciberdefensa una visión prospectiva y proactiva que genera al espectro aplicativo la posibilidad de anticiparse al impacto de las acciones cibercriminales generadas por la objetividad ideológica o intereses lucrativos de los piratas informáticos. A través de la proactividad, argumenta el autor, un estamento de seguridad focalizado hacia las problemáticas cibercriminales no podría únicamente anticiparse a la acción, sino también identificar los patrones binarios y la consulta informática realizada antes de consolidar la acción criminal.

Visto desde la consideración de Rowe (2016), la ciberdefensa sería entonces un concepto de seguridad nacional, encargado de prevenir, para posteriormente contrarrestar, el accionar e

impacto generado por la parcialización de los efectos cibernéticos ante campos inherentes al espectro social; sectores financieros, sectores médicos, sectores de defensa y sectores educacionales.

Similar a la proposición de Rowe (2016), pero describiendo la capacidad que considera a la aproximación de ciberdefensa como a un ente sistémico, de características intersectoriales, Tokunaga & Aune (2017) incluye en el ciclo exploratorio una concepción holística, la cual permite observar el comportamiento de dicho paradigma como a un organismo conformado por varios sectores, todos ellos diseñados para consolidar la idea abstracta de secutirización.

Por tanto, para este autor, la seguridad informática, la seguridad digital y las garantías de resguardo hacia un sistema universal asociado con flujos constantes de datos son variantes que hace parte de la misión constitucional de cualquier Estado, independiente a que su regulación esté o no estipulada en un marco jurisprudencial. De esta forma, la exposición de Tokunaga & Aune (2017) sería útil para describir el siguiente acápite desde la perceptibilidad legal que ofrecen los estamentos de seguridad relacionados con el diseño de políticas jurisprudenciales empleadas para regular la acción ciber criminal, la defensa en contra de ciberataques y la disponibilidad activa de los actores encargados de materializar el concepto objetivo de seguridad y defensa nacional general, específico e integral.

NORMATIVIDAD VIGENTE EN COLOMBIA EN CIBERSEGURIDAD Y DEFENSA

De acuerdo al análisis y la revisión hecha en la investigación, vemos el enfoque de la política de seguridad en Colombia a través de la legislación existente con sus conceptos y antecedentes propios de la ciberseguridad, teniendo en cuenta que el estado presenta un interesante avance vanguardista en el ámbito de ciberseguridad teniendo como referencias las tareas y procesos que permitan implementar la aplicación y uso de las políticas para la detección y prevención de ataques cibernéticos protegiendo los sectores amenazados desde diferentes ámbitos.

La aplicación de las políticas y legislación existente ha permitido disminuir y detectar a tiempo las diferentes clases de amenaza que surgen del ciberdelito, para esto el surgimiento de los siguientes documentos y leyes que buscan detener y controlar a la ciberdelincuencia.

Para esto se inicia con la elaboración del Consejo Nacional de Política Económica y Social CONPES que se aplica como un asesor del gobierno en los aspectos relacionados con lo concerniente al desarrollo económico y social del país y es la máxima autoridad a nivel Nacional respecto a la planeación donde se integran, coordinan y orientan los organismos encargados de la dirección económica y social del gobierno para hacer los estudios, documentos y políticas que se someten a la aprobación en una serie de secciones al ser presentados por el Departamento Nacional de Planeación que cumple su función como la secretaria ejecutiva del Conpes

Conpes 3701 como política pública nacional dio claridad a los lineamientos para ciberseguridad y ciberdefensa con el fin explícito de contrarrestar las amenazas que aumentaban desmedidamente y a su vez tener un marco normativo sobre el mismo asunto basados en los diferentes ataques presentados inclusive en la Presidencia de la Republica y sus instituciones (DNP, 2011), de allí era urgente afrontar estas situaciones para fortalecer las capacidades del

Estado en defender y aplicar el uso de la Ciberseguridad y ciberdefensa para la defensa y seguridad nacional estableciendo tres aspectos de importancia 1.implementacion de normatividad en pro de proteger el Estado en temas de ciberseguridad y ciberdefensa. 2. Generar espacios de capacitación e investigación en ciberdefensa y ciberseguridad. 3. Legislación y alineación a los estándares internacionales surgidos sobre la cibernética. (Conpes 3701, 2011)

Estos objetivos dieron el cumplimiento en la creación de organismos que iniciaron el proceso de defensa de ciberseguridad y ciberdefensa del estado como los siguientes mencionados Grupo de Respuesta emergencias Cibernéticas de Colombia (colCERT) de Min defensa, Comando Conjunto Cibernético (CCOC) del CGFM, el Centro Cibernético Policial (CCP) de la Policía siendo los principales símbolos de la institucionalidad en el tema además de la Comisión Nacional Digital y de Información Estatal con el decreto 32 de 2013 del MINTIC que realizaría las funciones de coordinación, control y ejecución de los servicios públicos, infraestructura tecnológica de información para los ciudadanos y así mismo el uso adecuado de la información en el país

Las actividades de capacitación y fortalecimiento de se desarrolló desde cada uno de los entes creados siendo objetivos primordiales desde los niños hasta las instituciones del estado con campañas de conocimiento, sensibilización, educación y formación de servidores públicos, respecto a sectores privados se generó concientización en la población y suministro de internet, con el CCOC llegaron las unidades cibernéticas enfocadas a la protección de la defensa, soberanía, independencia, integridad del territorio y el orden constitucional, la CCP además de la sensibilización en la población enmarco su esfuerzo a la ciberseguridad para atacar los delitos cibernéticos y a esto sumado el aumento de la educación en instituciones formales y no formales con especializaciones técnicas y maestrías, la creación de la Comisión Nacional digital y de

Información estatal, la regulación para proteger los menores de edad y toda la población de los delitos sexuales en todas sus formas de explotación, abuso, turismo y pornografía que tanto afectaba al país. (Conpes 3701, 2011)

La terminología estableció unos conceptos básicos y claros del tema como los siguientes:

Ciberseguridad es el conjunto de respuestas que un estado adopta para enfrentar las conductas que perjudican el aspecto social esto para proteger los intereses y derechos de la población y las instituciones protegidos por el Estado es decir su objetivo es gestionar los riesgos del ciberespacio, relacionados con información digital y sus sistemas interconectados, donde hay vinculo del ciberespacio y el internet. (MicTc, 2014)

Este concepto se complementa con una serie de parámetros como es la confidencialidad, la integridad, el riesgo de seguridad digital.

Delito informático: lo que concierne a lo ilegal sin autorización y que no permita procesar datos en un sistema informático.

El ciberdelito: se aplica en las tecnologías que manejan el internet como base de funcionamiento y se realizan en el ciberespacio.

Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. (Conpes 3701,2011).

Estos llamados ciberdelitos se caracterizan por unos aspectos principales de acuerdo a las muchas maneras que permite el internet y su utilización donde las más ejecutadas son estas:

Ataques de denegación de servicios, ataque por cambio de la página web, alteración de protocolos de comunicación y modelo de ciberataque que a su vez maneja cuatro pasos para su ejecución y los cuales dan el punto de partida principal en la secuencia delictiva, estos son:

- Investigar y obtener la información
- Conocer la disponibilidad de herramientas
- Conocer los sistemas disponibles para el manejo de la información
- La fachada, alias o identidades digitales falsas para evitar ser detectado o que detecten el punto de origen y así proteger su identificación y ubicación real.

Además de este Conpes también contamos con otra normatividad aplicable a la Ciberseguridad y Ciberdefensa como los siguientes:

Constitución política de Colombia de 1991

Artículo No15 define que todas las personas tienen derecho a tener su intimidad personal, familiar y su buen nombre donde el estado debe velar por el respeto y que se le respeten, así mismo el derecho a conocer, actualizar y corregir o rectificar la información que se tenga en los bancos de datos y los archivos de entidades públicas y privadas.

Artículo No20 en este artículo se les garantiza a las personas la libertad de expresar y difundir lo que piensan y opinan, así como dar y recibir información cierta, veraz y de manera imparcial, también de fundar los medios de comunicación, también habla de la no censura.

Ley 527 / 1999 esta nos define el comercio electrónico y reglamenta el acceso y uso de mensajes, comercio electrónico, firmas digitales, certificación de entidades y algunas disposiciones adicionales.

Ley 594 / 2000 en esta define la función del archivo con sus principios y regulación.

Ley 679 / 2001 establece las normas de carácter preventivo y sancionatorio, así como las medidas de protección de los delitos como explotación, pornografía, turismo sexual y demás formas asociadas a estos actos.

Ley 962 / 2005 establece el uso de los medios tecnológicos de organismos y entidades del estado, sus incentivos en la disminución de tiempos y costos en los tramites que realizan las personas.

Ley 1032 / 2006 Por la cual se modifican algunos artículos del código penal, sobre la violación a los derechos patrimoniales de autor y derechos conexos.

Ley 1273 / 2009 establece y tipifica delitos informáticos y protección de información y los datos poniendo penas en prisión y multas.

Consiente el estado de las necesidades y la evolución de las nuevas mutaciones del tema y los ataques cibernéticos en los ámbitos del estado económicos, sociales y contra la ciberseguridad y ciberdefensa del país inicio el camino de modificación de la normatividad hacia una política nacional de Ciberseguridad trabajo del cual se estableció con el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), el Ministerio de Defensa (MINDEFENSA) y el Departamento Nacional de Planeación los cuales presentaron un nuevo documento CONPES, que

articula y describe una Política Nacional de Seguridad Digital y a partir de este nuevo documento se reemplaza o substituye el Conpes 3701 del 2011 que su política estuvo vigente hasta el año 2015.

Como fin primordial del nuevo documento se vincula no solo las fuerzas Militares y la Policía para hacer frente a este riesgo de seguridad informática, también se vinculan y obligan a todos los entes del estado a iniciar un fuerte trabajo direccionado a la capacitación, prevención y disminución de los riesgos cibernéticos, creando el CONPES 3854 en el mes de abril del 2016.

CONPES 3854, el cual establece una política en ciberseguridad y a su vez se convierte en el inicio de una estrategia para prevenir y luchar contra la amenaza y los riesgos cibernéticos siendo esta la Política Nacional de Seguridad Digital formada por seis capítulos desde la introducción, los antecedentes justificados y basados en cifras y estadística del crecimiento a nivel mundial, el marco conceptual referenciado y alineados con la OCDE, el diagnostico de nuestro país, una definición clara de la política y las recomendaciones para el establecimiento y funcionamiento de la misma dando unos parámetros claros en la concepción y asimilación que garanticen la inmediata puesta en marcha de su finalidad.

Esta Política nacional de Seguridad Digital presenta unos aspectos de enfoque como son:

Vinculación de los entes gubernamentales, los conceptos y esquemas que permitan tener los riesgos respecto al tema de seguridad digital e interpone un marco de protección de los valores fundamentales y la preservación los derechos humanos.

Relaciona los antecedentes de la temática, diagnosticando el estado de la ciberseguridad en el país.

Proyecta dentro de la política la gestión de riesgos, las partes interesadas, los mecanismos y fortalecimiento de la defensa en medios digitales en concordancia con los estándares internacionales y concluyendo con la afectación económica de su funcionamiento.

Lo anteriormente descrito nos permite apreciar los avances en lo concerniente a ciberdefensa enfocado a la protección de la inf4raestructura critica del país para así evitar su afectación y funcionamiento, además de la integración de las entidades públicas y privadas que permitan el conocimiento de los ciudadanos sobre los riesgos informáticos a los que están expuestos generando conciencia y prevención sobre el manejo adecuado de la información y de la misma manera el establecimiento de organizaciones que completen el engranaje de funcionamiento de la política de ciberseguridad como lo es el Grupo de Respuestas a Emergencias Cibernéticas (ColCERT) y el CSIRT-CCIT Centro de Coordinación de Atención a Incidentes de Seguridad Informática.

En el engranaje que lleva el proceso de organización también se resalta como el único estamento funcional la creación de la Comisión Intersectorial donde interviene el ministerio de Defensa Nacional por medio del Grupo de Respuesta a Emergencias Cibernéticas de Colombia, el Comando Conjunto Cibernético en el Comando General de las Fuerzas Militares y el Centro Cibernético Policial a cargo de la Policía Nacional.

ColCERT es el responsable de coordinar dos conceptos ciberseguridad y la ciberdefensa bajo el direccionamiento del Ministerio de defensa con el propósito de las medidas necesarias para proteger la infraestructura critica del estado ante ataques o emergencias que atenten contra la seguridad de la nación, para esto presenta un numero de funciones que consolidan todo tipo de coordinación Nacional, Extranjera, de entidades públicas, de entidades privadas y los diversos protocolos que debe desarrollar para generar, apoyar y fomentar os instrumentos a su alcance para reaccionar de la manera más eficaz y rápida ante cualquier situación de riesgo para el Estado y su infraestructura.

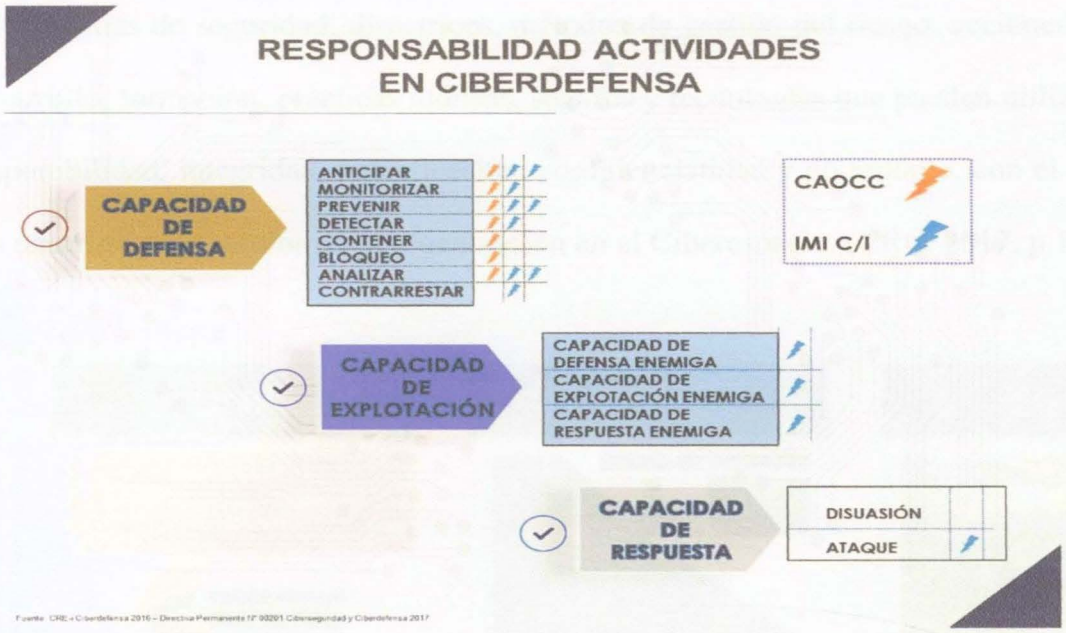
CSIRT-CCIT funciona como un centro de coordinación y atención a incidentes de seguridad informática que permanece en contacto directo con los centros de seguridad de sus

empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas. (ATcsirt-ccit.org.co)

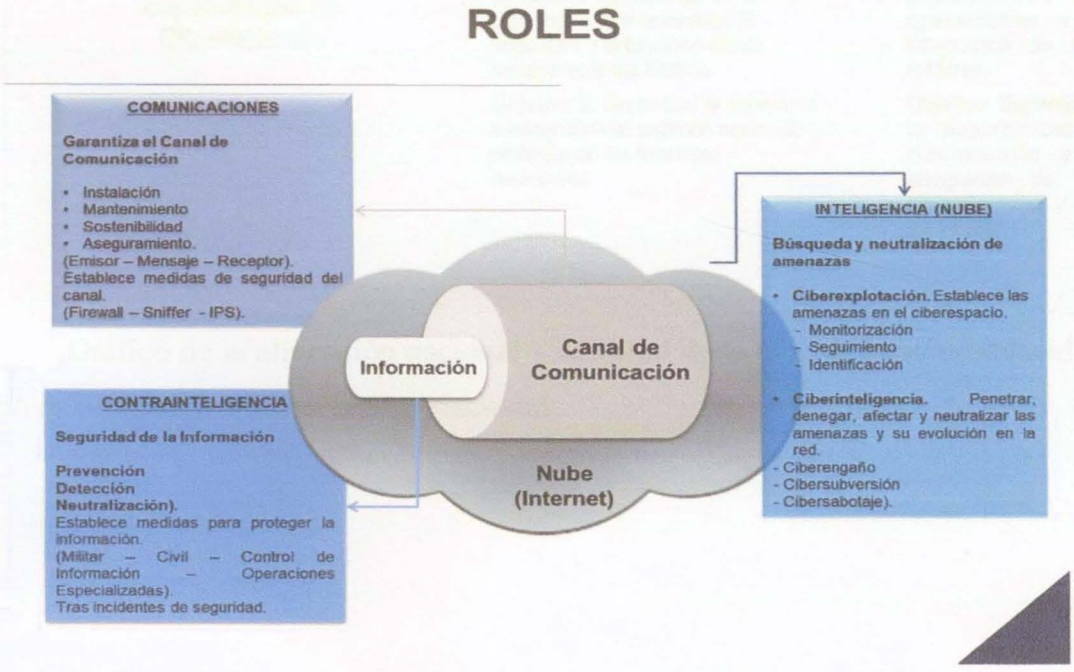
También se están efectuando trabajos en contra del robo de información privada (phishing), la cual es usada posteriormente para sustraer dinero de las cuentas bancarias de las víctimas, estas tareas anti-phishing se están realizando, de forma coordinada, entre las entidades bancarias y las empresas prestadoras del servicio de Internet que están agrupadas en el NAP Colombia y mantiene comunicación constante con organizaciones internacionales que trabajan en el sector de la seguridad informática y hace uso de información especializada entregada por estas, para advertir a los integrantes del CERT Colombia, sobre cualquier tipo de contenido malicioso que pueda tener alojado dentro de sus redes, que afecte directamente su operación, o que amenace la seguridad de sus clientes. (CSIRT-CCIT org, 2018).

Por ultimo veremos en estos gráficos la organización del sistema de ciberdefensa en las Fuerzas Militares con sus roles y sistema de aplicación.

Vemos la descripción del sistema en su entorno principal de capacidades.



Las capacidades y la actividad a desarrollar dentro de cada una de ellas desarrollada.



En Colombia, según la Comisión de Regulación de Comunicaciones, órgano adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones, la ciberseguridad se alinea al concepto anterior y es entendida como: "El conjunto de recursos, políticas, conceptos de seguridad,

salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (CRC, 2017, p.12)

Gráfico de la alineación nacional y sectorial de la ciberdefensa establecido en la visión de análisis prospectivo del gobierno Nacional.

ESTRATEGIA Y LEGISLACION SOBRE CIBERNETICA EN ESTADOS UNIDOS

Al ser el país pionero sobre este tema y en especial de la creación de políticas, normas e instituciones que desarrollaran y previnieran ataques cibernéticos mediante una implementación a todo nivel, es por esto que para Colombia es referente en la creación y conformación de esta capacidad que ahora los Estados deben tener con miras al crecimiento de la tecnología y sus alcances.

De acuerdo con Pernik, Wojtkowiak & VerschoorKirss (2016) su primera estrategia nacional de seguridad cibernética fue publicada en 2003 y luego de estas vienen tres más la publicada en 2010, 2015 y 2018, todas estas encaminadas a la prevenir y responder ante las nuevas amenazas que generen algún riesgo la infraestructura crítica y la estabilidad del estado, cabe resaltar que luego de los atentados delo 11 de septiembre revoluciono muchas de las políticas de seguridad en varios países ante nuevas formas de ataque y dentro de estas nuevas amenazas esta la ciberseguridad.

Los desafíos han llevado a que las autoridades estadounidenses tengan como la mayor de sus amenazas sobre su infraestructura en general a la cibernética siendo atacada en diferentes flancos como el espionaje militar, económico, delitos financieros a través de la red y también varios países que observan y analizan su inf5raestructuura critica buscando vulnerabilidades para desarrollar posibles ataques, esto ha llevado a que se manejen muchos protocolos sobre el tema de la seguridad cibernética y entre los de aspecto militar tenemos:

La estrategia Nacional Militar de los Estados Unidos, en ella se establecen capacidades en la defensa de redes y también la preparación para ser disuasivo en el ciberespacio como lo han hecho en el espacio físico.

Las operaciones de información, en esta se da una doctrina de planear, preparar y ejecutar este tipo de operaciones y además incluyen la ética del jus in bello y jus ad bellum en el tema de ciberespacio.

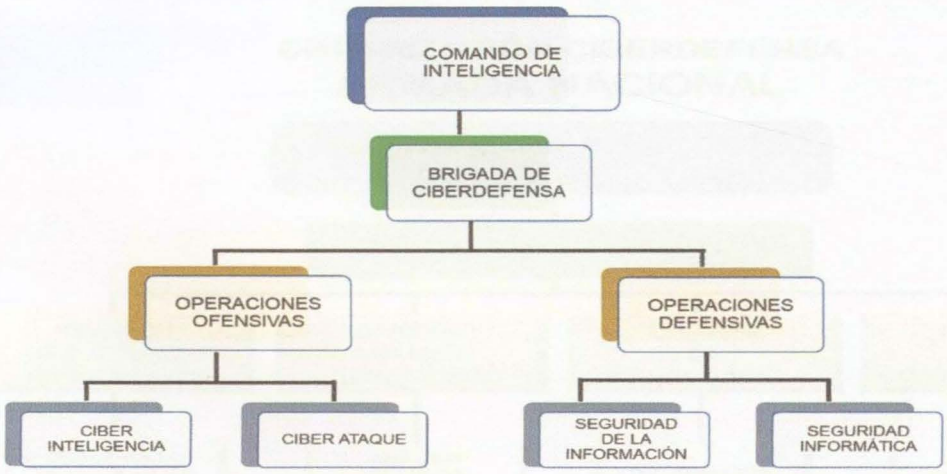
Las actividades cibernéticas electromagnéticas, las cuales están estipuladas en el (FM3-38) del Ejército de Estados Unidos dando la información de desarrollar actividades electromagnéticas y como ponerlas en ejecución con el plan X que es el programa de guerra cibernética que el Departamento de Defensa planea, ejecuta y evalúa sobre la guerra cibernética.

Plan de acción de ciberseguridad nacional, en la que el control será la bandera creada la comisión de mejoramiento de ciberseguridad, inversión para su mejoramiento y las alianzas estratégicas con empresas como Facebook, google, Microsoft y Dropbox que aseguran las cuentas de los usuarios. De acuerdo con Pernik, P., Wojtkowiak, J., & Verschoor-Kirss (2016)

Además de la organización interna de sus fuerzas militares como veremos en los siguientes gráficos.

ORGANIZACIÓN CIBERDEFENSA ESTADOS UNIDOS

ORGANIZACIÓN CIBERDEFENSA



ORGANIZACIÓN CIBERDEFENSA
FUERZA AÉREA

ORGANIZACIÓN CIBERDEFENSA
ARMADA NACIONAL

Como hemos visto el enfoque de las fuerzas militares sobre el tema cibernético es visionario y efectivo ante la magnitud de esta amenaza, algunos lo definen como el Ciberejercito estadounidense.

Además de lo anterior hay una serie de aspectos que están a disposición del gobierno y sus agencias que fortalecen este aspecto desde todos los ámbitos como a continuación veremos.

La ley de intercambio de información sobre la seguridad CISA, la cual es una ley federal entre el gobierno y las empresas que manejan y fabrican tecnología en la que la información personal es obtenida en las siete agencias relacionadas al tema de ciber analizando todo el tráfico de Internet.

CIBERESTRATEGIA DE ESTADOS UNIDOS 2018

Basada en la mantener la supremacía de la cibernética ya que ante tantos competidores que buscan de una manera u otra obtener ventajas de tipo militar, económicas, sociales y de infraestructura de los Estados Unidos ellos generaron esta estrategia con unos objetivos muy claros. (ciber estrategia 2018 EE.UU.)

Primero, debemos garantizar la capacidad del ejército de EE. UU. Para luchar y ganar guerras en cualquier dominio, incluidos ciberespacio. Este es un requisito fundamental para la seguridad nacional de EE. UU. Y una clave para garantizar que disuadimos la agresión, incluidos los ciberataques que constituyen un uso de la fuerza, contra Estados Unidos, nuestros aliados y nuestros socios.

En segundo lugar, el Departamento busca evitar, derrotar o disuadir el objetivo de actividades maliciosas cibernéticas Infraestructura crítica de EE. UU. Que podría causar un incidente cibernético significativo

En tercer lugar, el Departamento trabajará con aliados y socios de EE. UU. Para fortalecer la capacidad cibernética, expandir las operaciones combinadas del ciberespacio y aumentar el intercambio de información bidireccional en para avanzar nuestros intereses mutuos.

Los objetivos del ciberespacio del Departamento de defensa son:

1. Asegurar que la Fuerza Conjunta pueda cumplir sus misiones en un ambiente de ciberespacio disputado;
2. Fortalecimiento de la Fuerza Conjunta mediante la realización de operaciones en el ciberespacio que mejoren los EE. UU. ventajas militares;
3. Defender la infraestructura crítica de los EE. UU. De la actividad cibernética maliciosa solo o como parte de una campaña, podría causar un incidente cibernético significativo.
4. Asegurar la información y los sistemas del Departamento de Defensa contra la actividad cibernética maliciosa, incluido el Departamento de Defensa información sobre redes no pertenecientes al DoD.
5. Expandir la cooperación cibernética del Departamento de Defensa con interinstitucionales, la industria y los socios internacionales (ciber estrategia 2018 EE.UU.)

Se han desarrollado además de lo anteriormente mencionado unas formas desde todos los campos sobre el manejo y control de la cibernética dl país de la siguiente manera.

En lo estratégico, Política y estrategia de ciberseguridad donde la dependencia cada vez más de la dependencia sobre los sistemas genero una nueva dimensión por esto se creó la directiva de decisión presidencial (PDD-63), donde se generan varios puntos como la toma de medidas necesarias en los entes gubernamentales a fin de solventar la amenazas existentes, también creo el coordinador nacional para la seguridad con capacidad de coordinar y dirigir los esfuerzos, fomentar la educación cibernética, el desarrollo de programas, la interacción de los centros federales que realizan operaciones cibernéticas y la elaboración del plan de contrainteligencia cibernética.

CULTURA CIBERNETICA, la generación de campañas de sensibilidad e integración de los estadounidenses con una serie de instancias como es la comisión federal del comercio, el sistema nacional de concientización cibernética, la base de datos nacional sobre vulnerabilidades, Y la alianza de ciberseguridad con el sector privado buscando fomentar la cultura de ciberseguridad en el trabajo y en el uso seguro de dispositivos conectados a Internet. https://www.ftc.gov/system/files/documents/ reports/privacy-data-security-update

EDUCACION Y FORMACION EN SEGURIDAD CIBERNETICA, donde ya existen carreras universitarias con un enfoque estratégico del tema apoyados por el departamento de educación que hace un trabajo de compartir la información académica y tecnológica sobre ciber y asi tener personal capacitado en ciberseguridad es allí donde los planes de estudio los hacen las instituciones educativas o a nivel estatal por lo tanto pasa a ser estrategia Nacional y no federativa. http://www.ponemon.org/ library/2014-a-year-of-mega-breaches

EL MARCO JURIDICO, Estados Unidos no cuenta con la ley global de ciberseguridad, se establece en diversos regímenes que regulan en conjunto con marcos jurídicos establecidos para cada sector como el sistema financiero, sector energético, salud, educación, defensa y seguridad y continúan así todos los aspectos de manera individual pero alineados con la estrategia de ciberseguridad, la normatividad federal con muchas leyes federales sobre delitos informáticos todos relacionados con el Internet donde abarcan una amplia gama como lavado de activos, tarjetas de crédito, pornografía infantil, armas y demás aspectos generales siendo una garantía en la parte de jurisprudencia existente apoyadas por el ejecutivo. https://www.fas.org/sgp/crs/natsec/R42114.pdf

ORGNIZACIONES Y TECNOLOGIAS, que se dividen las responsabilidades cada una con unas funciones y atribuciones designadas para el engranaje de control cibernético, dentro de ellas las más importantes son:

- Departamento de seguridad nacional DHS, como organismo principal en ciberseguridad.
- Departamento de justicia
- Oficina Federal de la Investigación FBI, organismo investigador.
- Departamento de Estado
- Departamento de Defensa
- https://www.us-cert.gov/

RECOMENDACIONES

Con el propósito de establecer una serie de medidas que permitan superar el nivel alcanzado del avance en ciberdefensa y ciberseguridad del Estado colombiano en comparación con el Sistema de Cibernética de Estados Unidos debemos desarrollar una serie de aspectos para mejorar, como los siguientes

Aportar acciones por medio de las capacidades para tener y cumplir con los objetivos de ciberdefensa, por medio de la implantación de nuevas estrategias que prevengan y protejan las vulnerabilidades en el uso de la cibernética en Colombia en organizaciones y empresas público y privado que permita una seguridad altamente verificable.

Desarrollar cultura cibernética con estudio, que ayude a concientizar al ciudadano y a las empresas de los riesgos que tenemos en este nuevo panorama de ciber y que consecuencias trae al país este tipo de ataques contra los recursos y la infraestructura del Estado, lo cual se logra en pequeñas partes con algunos programas ya existentes sobre seguridad informática. Generar conocimiento, capacitación y sensibilización.

Este programa académico debe abarcar desde la primaria hasta el nivel superior de educación como la ESDEGUE que ya maneja especialización y maestría sobre este dominio y tiene acceso a los funcionarios públicos aportando las bases de este proceso.

Implementar plan de contingencia, que permitan seguir estables y condicionados a unas normas básicas de funcionamiento donde como las fuerzas Militares han desarrollado el andamiaje

para que se inicie el proceso con unidades de ciber, protección de datos así mismo deben las empresas públicas y privadas que de hecho ya algunas aplican estos soportes tecnológicos, como lo hacen las instituciones militares y algunas empresas que han implementado. Hacer cumplir la normatividad existente y generar una fuerte campaña de proteger y cuida sobre los delitos informáticos y el manejo de los medios digitales

Asignación de cargos, roles que permitan un efectivo papel de los órganos de control

Establecer roles y responsabilidades en seguridad de la información de un modo coordinado y realmente establecido como en nuestro caso el cual debe extenderse a las grandes empresas en conjunto con el Estado para poder mitigar y disminuir el riesgo de la amenaza.

CONCLUSIONES

Al analizar y conocer la estrategia de los países en comparación para este caso, Colombia respecto de Estados Unidos, se obtiene una serie de consideraciones que llevan a ver los vacíos estructurales que existen en la cibernética colombiana. Estas falencias, se demuestran en un proceso descriptivo en el que se evidencia la necesidad de políticas para generar nuevas estrategias, leyes e instituciones que permitan avanzar y crecer en la implementación de medidas para afrontar estas nuevas amenazas del mundo cibernético actual.

Así mismo, se ha podido evidenciar que Colombia está en un nivel de manejo sobre temas cibernéticos tipo medio, por lo tanto, es el momento de obtener apoyo político para que en futuras decisiones se realicen los ajustes que ayuden a prevenir los efectos de los delitos cibernéticos y a su vez contribuir a la protección de la ciberseguridad y defensa del Estado.

También es necesario, crear una nueva organización y dar responsabilidades que asuman los diferentes ámbitos donde se deben usar de manera diferente los análisis sobre las amenazas de cada sector, puede ser ciberataques a la infraestructura que atenten contra la ciberdefensa y seguridad del Estado. Donde, como se pudo observar en la investigación hay una serie de mecanismos para contrarrestar la amenaza, pero, no son suficientes en la etapa de implementación. Esta conclusión, se deduce del análisis comparativo con las estrategias de Estados unidos mediante su organismo de control ciber, lo que garantiza confiabilidad y seguridad para este tema en el nivel ejecutivo.

Por lo tanto, la elaboración de un soporte jurídico no se puede dejar de último momento, se debe tener establecidos un sin fin de leyes que van desde el delito común de robo hasta llegar a

los que son encaminados al propósito de atacar la ciberseguridad y defensa de la Nación. El establecimiento de este marco jurídico, lleva al soporte más adecuado para mitigar las dudas y los procederes de quienes atacan el Estado, pero también exige deberes de quienes emplean el internet y por ende muchas de las situaciones que podrían poner en amenaza o ser víctima del ciberdelito.

Además, la protección de la infraestructura debe estar definida con responsables, normas y medios. En este orden de prioridades, debe manejarse de acuerdo a la importancia en la vulnerabilidad que pueda afectar al Estado, en este caso, se debe iniciar por la preparación académica especialmente en el uso de la tecnología con seguridad y protección aunado a la preparación de quienes realizan la mano de obra en temas cibernéticos, empezando por las fuerzas Militares contamos priorizando en el fortalecimiento idóneo del área gubernamental y privada. Todo ello, para establecer un vínculo de capacitación en el cual las enseñanzas de la estrategia cibernética de Estados Unidos con su conocimiento y capacidades deben ser ejemplo para el manejo de las estrategias de ciberdefensa en Colombia.

Referencias

Acosta, P., Rodriguez, J., Arnáiz de la Torre, D., & Taboso Ballesteros, P. (2009). Seguridad nacional y ciberdefensa. catedraisdefe. etsit. upm. es/wp-content/uploads/2010/07/CUADERNO-Nº-6. pdf.

Amigo Tossi, A. (2016). Ciberdefensa en las Operaciones Militares. Seminario ACAPOMIL, Tendencias Tecnológicas Asociadas a la Ciberdefensa.

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de infraestructura crítica. Estudios de Seguridad y Defensa, 131-164.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., ... & Ou, X. (2010). Cyber SA: Situational awareness for cyber defense. In Cyber situational awareness (pp. 3-13). Springer, Boston, MA. (s.f.).

Benson, V., McAlaney, J., & Frumkin, L. A. (2018). Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In Psychological and Behavioral Examinations in Cyber Security (pp. 266-271). IGI Global. (s.f.).

Blackwell, A. (2013). Multidimensional Security Perspective. In Conferencia de la OEA, Curasao. Pág (Vol. 1).

Borbúa, R. V., Herrera, L. R., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20), 31-45.

Bolaño, I. M. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 5(9).

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408-433. (s.f.).

Cabrera, E. (2017). The culture of cybercrime in West Africa. Trend Micro blog, March. (s.f.).

Cáceres, J. (2017). Colombia, estrategia nacional en ciberseguridad y ciberdefensa. *Air and Space Power Journal*, 85-89.

Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *SISTEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS)*, *119*, 4-7

Caro, M. (2014). DELINCUENCIA ORGANIZADA E INTERNET. Instituto Español de Estudios Estratégicos , 03.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62. (s.f.).

Casey, N., & Herrero, A. V. (2017). How a Politician Accused of Drug Trafficking Became Venezuela's Vice President. The New York Times.

Centro de Policía Cibernético. (2017). Balance Cibercrimen 207. Bogotá: Publicaciones PONAL.

Chávez, L., & Velásquez, S. (2016). Ejercicio dEl cibErpodEr En El cibErEspacio. Revista Científica de la Escuela de Postgrados de la Fuerza Aérea Colombiana, 236-244.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731. (s.f.).

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), 1-22. (s.f.).

Clough, J. (2015). Principles of cybercrime. Cambridge University Press. (s.f.).

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

Cortés Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia.

Corvalan, F. (2015). Seguridad de Infraestructuras Críticas: Visión desde la Ciberdefensa. In III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires.

Digiware. (2017). Los sectores económicos más impactados por el cibercrimen en Colombia. Dinero, 04-05.

Furnell, S. (2002). Cybercrime: Vandalizing the information society (pp. 3-540). Boston, MA: Addison-Wesley. (s.f.).

Geers, K. (2011). STRATEGIC CYBER SECURITY. En K. GEERS, STRATEGIC CYBER SECURITY (pág. 09). Tallin: NATO Publications.

Graham, D. E. (2010). Cyber threats and the law of war. J. Nat'l Sec. L. & Pol'y, 4, 87.

Feliu Ortega, L. (2012). La ciberseguridad y la ciberdefensa. España: Ministerio de Defensa de España.

Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. Washington, DC: Institute for National Strategic Studies, National Defense University. (s.f.).

Justribó, C. (2014). Ciberdefensa: una visión desde la UNASUR. In VII Congreso del IRI/I Congreso del CoFEI/II Congreso de la FLAEI (La Plata, 2014).

Kirwan, G. H. (2018). Dispelling the pseudopsychology of cybercrime. (s.f.).

Kamlofsky, J., Abdel Masih, S., Colombo, H., Veiga, D., & Hecht, P. (2015, June). Ciberdefensa de infraestructuras industriales. In XVII Workshop de Investigadores en Ciencias de la Computación (Salta, 2015).

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414. (s.f.).

Ramacciotti, B. (2005, March). Democracy and Multidimensional Security: The rising need for citizen security in Latin America. In Seminar on" Security and Democratic Governability: Addressing Challenges in Latin America.

Ramírez, I., Velandia, D., & Orduz, G. (2017). Ciberamenazas, una perspectiva analítica desde el concepto de seguridad multidimensional. International secuirity and economic globalization, 37-45.

Ron, M. (2018, April). Situational Status of Global Cybersecurity and Cyber Defense According to Global Indicators. Adaptation of a Model for Ecuador. In Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International. (s.f.).

Rowe, B. (2016). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. Technology Economics and Policy RTI International, 03.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. (s.f.).

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296-298. (s.f.).

Tokunaga, R. S., & Aune, K. S. (2017). Cyber-defense: A taxonomy of tactics for managing cyberstalking. Journal of interpersonal violence, 32(10), 1451-1475. (s.f.).

Vargas, R., Recalde, I., & Reyes, R. (2016). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. Revista Latinoamericana de Estudios de Seguridad, 20, 31-45.

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2 (4). Yale J. Int'l L., 36, 421. (s.f.).

Zheng, R., Lu, W., & Xu, S. (2018). Preventive and reactive cyber defense dynamics is globally stable. IEEE Transactions on Network Science and Engineering, 5(2), 156-170. (s.f.).

Revista digital OTAN (2019). Donde hablan los expertos. Nuevas amenazas en el ciberespacio

MicTc, M. d. (2014). Agenda Estratégica de Innovación: Ciberseguridad. Bogotá.
Moreno, J. Z. (2015). Ciberdiccionario.

Universidad Cooperativa de Colombia, Sede Bucaramanga, año 2014.

Constitución política de Colombia 1991

Estrategia cibernética de Estados Unidos 2018, DoD.