Análisis y prospectiva de la ciberdefensa en la Fuerzas Militares de Colombia

Julio César Villanueva Méndez
Carlos Arturo Martínez Forero

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

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

2020

ANÁLISIS Y PROSPECTIVA DE LA CIBERDEFENSA EN LAS FUERZAS MILITARES EN COLOMBIA

AUTOR: MY. JULIO CÉSAR VILLANUEVA MÉNDEZ
ASESOR: MY. CARLOS ARTURO MARTÍNEZ FORERO

ESCUELA SUPERIOR DE GUERRA
"GENERAL RAFAEL REYES PRIETO"
MAESTRIA EN SEGURIDAD Y DEFENSA NACIONALES
BOGOTÁ D. C.
2020

ANÁLISIS Y PROSPECTIVA DE LA CIBERDEFENSA EN LAS FUERZAS MILITARES EN COLOMBIA[1]

ANALYSIS AND PROSPECTIVE OF THE CYBER-DEFENSE IN MILITARY FORCES IN COLOMBIA

CYBER DEFENSE

Julio Cesar Villanueva[2]

Escuela Superior de Guerra "Rafael Reyes Prieto"

Resumen:

En el siguiente artículo científico se encontrará un análisis frente a la Ciberdefensa y la Seguridad de la Información que ha evolucionado en Colombia, de tal manera que se observe de qué forma el Ministerio de Defensa desarrolla nuevas tecnologías para que el sector de la defensa apoye a las Fuerzas Militares, esto a través del Comando Cibernético Conjunto (CCOCI), que está a cargo de la defensa del país en el Ciberespacio; de ahí que, este trabajo pretenda llevar a cabo la prospectiva del mismo para proteger la soberanía en el Ciberespacio en Colombia teniendo en cuenta la actual estrategia de Ciberdefensa y Seguridad Digital de las FFMM en la nación, el estudio de los principales sectores que han sufrido ataques Cibernéticos que afectan la Seguridad Nacional y comparando las metodologías sobre Ciberdefensa utilizados en el Centro de Excelencia de Estonia.

---

[1] Artículo Científico para optar el título de Magister en Seguridad y Defensa Nacional de la Escuela Superior de Guerra bajo la dirección de Carlos Arturo Martínez Forero.

[2] Oficial del Ejército Nacional de grado Mayor. Magister en Sistemas de Información y Proyectos Tecnológicos, Universidad EAN. Estudiante de la Maestría en Seguridad y Defensa Nacional de la escuela Superior de Guerra.

Palabras claves: Ciberdefensa, Ciberespacio, Ciberataque, Infraestructura Crítica, Colombia, Fuerzas Militares.

Abstract:

In the following scientific article, you will find an analysis of Cyber Defense and Information Security that has evolved in Colombia, in such a way as to observe how the Ministry of Defense develops new technologies for the defense sector to support the Military Forces, this through the Joint Cybernetic Command (CCOCI), which is in charge of defending the country in Cyberspace; Hence, this work aims to carry out its prospective to protect sovereignty in Cyberspace in Colombia, taking into account the current Cyber Defense and Digital Security strategy of the Armed Forces in the nation, the study of the main sectors that have suffered Cyber attacks that affect National Security and comparing the Cyber Defense methodologies used in the Estonian Center of Excellence.

Keywords: cyber defense, cyberspace, cyber attack, critical infrastructure, Colombia, Colombian Military Forces.

Introducción

El siguiente trabajo analiza los retos que tienen las Fuerzas Militares de Colombia actualmente, en relación a la Seguridad y Defensa Nacional para evitar los ataques anónimos en el ciberespacio; el cual nos permite reflexionar acerca de una política efectiva para mitigar los riesgos de seguridad digital en el país.

Rodrigo Cortés, experto en delitos informáticos asegura que, con la materialización de la era digital, Internet y la sociedad de la información, se han emergido nuevos desafíos para los Estados y los distintos sectores de la sociedad, haciendo necesario implementar políticas públicas que permitan hacerles frente. (Cortés, p.25, 2015)

Es así como se pretende evaluar una prospectiva en la seguridad de la Ciberdefensa de la nación, ya que se debe desarrollar este concepto en las operaciones militares centradas en redes con el fin de promover capacidades de prevención, detección, contención, respuesta, recuperación y defensa, así como mejorar la protección, preservar la integridad y la resiliencia de la infraestructura Crítica-Cibernética Nacional.

Como es visiblemente apreciado, el uso del concepto de resiliencia será asumido desde la concepción del CERT de Seguridad e Industria, en su trabajo "Resiliencia: Aproximación a una marca de medición" INTECO (2018, p. 11) citado por Gómez, M. (2019, p. 23) en donde plantea que cuando un sistema es capaz de soportar todas las presiones sin cambiar su comportamiento, es robusto. Cuando un sistema no puede soportar más presiones, pero puede integrar cambios para disminuirlos y puede seguir adelante, es resiliente al ciberespacio.

Y aunque, Colombia en la última década, sea líder en la región de Latinoamérica, respecto a la forma como el Estado ha venido enfrentando los desafíos que plantean la Ciberseguridad y la Ciberdefensa al propio Estado y a la sociedad en general, este trabajo servirá para hacer un llamado en articular un pie de fuerza en seguridad digital que potencialice los comandos y grupos de investigación de defensa y seguridad digital.

Teniendo en cuenta lo anterior, se plantea la siguiente pregunta de investigación ¿Cómo las estrategias que plantea las FFMM fortalecen la Ciberdefensa en Colombia?

La cual, para una adecuada organización, se desarrollará en tres ejes temáticos constituidos de la siguiente manera: primero, estudiar la actual estrategia de Ciberdefensa y seguridad digital de las FFMM en Colombia; segundo, evaluar los principales sectores que han sufrido ataques Cibernéticos que afectan la Seguridad Nacional y comparar las metodologías sobre Ciberdefensa utilizados en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Estonia, con el fin de encontrar unas breves conclusiones y recomendaciones.

Con respecto al primer eje, se hará un recorrido histórico de la actual estrategia en seguridad digital de las FFMM basado en el análisis del CONPES 3701, documento soporte que generó temas en Ciberdefensa en el país y empleó los primeros recursos económicos para su primera fase y que a lo largo de este artículo se desglosará sus etapas hasta el 2019.

Así mismo, en relación al segundo eje temático, fundamentado en el catálogo de Infraestructura Crítica Cibernética de Colombia (2016), se analizarán algunos sectores que han sufrido ataques cibernéticos en su infraestructura crítica digital, ya que estas

situaciones pueden afectar la seguridad y defensa del país, a partir del estudio de sectores con mayor porcentaje de ataque como el sistema financiero y el sector defensa.

Por último, como ejemplo se analizarán las estrategias de Ciberdefensa del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Estonia, debido a que dicho país que fue el primero en sufrir un ataque Cibernético y tras su creación, han diseñado guías y modelos de estrategia que sirven a Colombia como ejemplo para el diseño y en la Estrategia de Ciberdefensa y Ciberseguridad en el país.

Para ello, este trabajo se desarrollará a partir de las teorías metodológicas de (Sampieri, 2006. p, 179), (Anguera, 1989) y (Sarriá y Brioso, 1999) que se centran en la observación o investigación descriptiva con el propósito de analizar la prospectiva de la Ciberdefensa en las F.F.M.M desde distintas unidades de análisis como: Ciberdefensa, Ciberespacio y proyección.

1. **Estudiar la actual estrategia de Ciberdefensa y seguridad digital de las FFMM en Colombia.**

La defensa de una nación ya no se centra únicamente en el territorio físico, aéreo o marítimo, sino que las Fuerzas Militares deben defender el Ciberespacio y allí, contrarrestar las amenazas del Cibercrimen desarrollando estrategias que le permitan aumentar los planes y maniobras que fundamenten su Ciberdefensa, a partir de elementos de defensa activa y pasiva de los medios de información que posee cualquier institución para así protegerse de los ataques cibernéticos y amenazas informáticas.

En ese sentido, Colombia no ajena a esta problemática, desde el año 2011 formuló el CONPES 3701 de 2011 "Lineamientos de política para la Ciberseguridad y Ciberdefensa", en el que se inició a desarrollar una estrategia nacional para contrarrestar el incremento de las amenazas informáticas que afectan significativamente al país y crear las entidades apropiadas como El Comando Conjunto Cibernético (CCOCI) donde se coordina la proyección de todos los aspectos de seguridad y protección en temas relacionados con la Ciberdefensa de las Fuerzas Militares, con capacidades para la gestión de eventos de seguridad de la información, respuesta en línea a incidentes de Ciberseguridad y un centro de operaciones de seguridad (SOC).

De ahí que, como uno de los proyectos más importantes que se generaron gracias al CONPES 3701 fue darle importancia a la seguridad de la infraestructura crítica digital del país, donde en cabeza del Comando Conjunto Cibernético y con la colaboración de más de 10 Ministerios y varias empresas de diferentes sectores, se dio la tarea de identificar la infraestructura crítica y desarrollar medidas para enfocar recursos y articular esfuerzos para su protección y fortalecimiento (CONPES, 2011).

Con relación a lo anterior, durante el CONPES 3701 (2011) se proyectaron lineamientos y políticas de Ciberseguridad y Ciberdefensa en el gobierno, el cual destinó $ 16.428.444.000 millones de pesos para vigencias futuras de la siguiente manera: en el 2011 $ 1.428.444.000, 2012 $ 5.400.000.000, 2013 $ 5.000.000.000 y en el 2014 $4.600.000.000, de esta manera, con dicho presupuesto se creó el COLCERT del Ministerio de Defensa, el CCOC de las FFMM y el CCP de la Policía Nacional.

Posteriormente, realizando un seguimiento al plan de acción se logró evidenciar en el año 2015, que el 79% de las actividades propuestas se ejecutaron: por ejemplo, "el

CCOCI y el COLCERT pasaron de gestionar un total de 769 incidentes digitales de Defensa Nacional durante el año 2014, a 957 en el 2015" (CONPES 3854.p. 44), por tal razón, analizando el CONPES 3701 se reconoció de qué manera, la estrategia de Ciberseguridad y Ciberdefensa fue acertada mitigando incidentes digitales.

Por tal motivo, el gobierno mediante un informe enviado por el BID y la OEA en el 2016 según el (CONPES 3854. p.41) concluyeron que, de acuerdo a su modelo de madurez de capacidad de seguridad cibernética, el marco jurídico y reglamentario de seguridad cibernética en aspectos como privacidad, protección de datos y otros derechos humanos se reconoce que en Colombia se han aplicado procedimientos reglamentarios y de legislación integral sobre protección de datos, evidenciado con la generación de la Ley 1581 de 2012, y su Decreto reglamentario 1377 de 2013. En esta ley se reconoce el derecho a la privacidad entregando la libertad al titular para elegir cómo serán tratados sus datos personales, así como estableciendo los responsables de dicho tratamiento.

Por todo lo anterior, el gobierno tomó la decisión de darle continuidad a esta importante estrategia mediante el CONPES 3854 políticas y seguridad digital en el que se destinaron $37.375.000.000 Billones de pesos sólo para el sector Defensa, para ser ejecutados durante los años 2016 al 2019 en el que se desarrolla la segunda fase de la Ciberdefensa y Ciberseguridad en el país con unas Fuerzas Militares un nivel de madurez e infraestructura más robusta y con un país con una normatividad para su judicialización.

La estrategia de Ciberseguridad y Ciberdefensa permitirá establecer unos principios generales, unas líneas de acción y la hoja de ruta de la Ciberseguridad y Ciberdefensa Nacional, que refleje el compromiso decidido, el trabajo colaborativo, la cooperación, articulación y armonización de todos los responsables y recursos en materia de protección y

defensa del ciberespacio, con el fin de garantizar la prevención, detección, respuesta, neutralización y contención a intenciones o acciones hostiles potenciales, inminentes y reales que se originen en o a través del ciberespacio y que afecten la seguridad y defensa del estado (Realpe, M. et al., 2014, p. 8).

Es por esto, una vez mencionada la actual estrategia en seguridad digital que se está desarrollando en el país por parte de las FFMM se creó la directiva permanente 0118000011705 sobre lineamientos de ciberdefensa y ciberseguridad para las Fuerzas Militares. Y el Manual de Ciberdefensa Conjunta 3-38 con el propósito de generar la doctrina y las políticas a seguir dentro del Comando de las Fuerzas Militares.

> "Este manual es el documento de mayor jerarquía en las Fuerzas Militares con respecto a la Doctrina en Ciberdefensa y Ciberseguridad, su aplicación abarca tanto en tiempos de conflicto armado como en tiempos de paz; plantea los procedimientos, criterios, directrices y órdenes del complejo planeamiento y conducción de las operaciones conjuntas y propias de cada Fuerza en el ciberespacio. Se explican los fundamentos de la organización, relaciones de mando, capacidades y limitaciones de las Unidades y Dependencias de Ciberdefensa de las Fuerzas Militares" . (Comando de las Fuerzas Militares (2016) Manual de Ciberdefensa Conjunta 3-38. p. 9).

Por lo tanto, las FFMM deben estudiar sus posibles amenazas en el ciberespacio para determinar quién o qué estados se pudieron haber tomado la autoría para generar estos Ciberataques (interna o externa o simplemente es una guerra hibrida de quinta generación) con el fin de hacer terrorismo y desestabilizar una nación a través de sus activos críticos. Según José Tomás Tarrero "la defensa de los intereses estratégicos marca una línea a seguir

en la política de defensa de un Estado impulsado por su legítimo interés de defensa de su soberanía" Hidalgo, J. (2013).

Según el Observatorio de la Ciberseguridad en América Latina y el Caribe después de haber realizado análisis a la región, planteó cómo los países son vulnerables a sufrir ataques a su Ciberdefensa potencialmente devastadores. Cuatro de cada cinco países no tienen estrategias de Ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética y la gran mayoría de las Fiscalías carece de capacidad para perseguir los delitos cibernéticos.

> "A pesar de los avances prometedores que hemos logrado hasta el momento, la necesidad de continuar con cooperación multilateral y la creación de capacidad sigue siendo igual de urgente. Las tecnologías de la información y las innumerables formas en que las utilizamos siguen evolucionando a un ritmo acelerado, al igual que las vulnerabilidades que traen consigo y los actores y las amenazas que buscan aprovecharse de estas. Solo trabajando juntos podemos seguir el ritmo y asegurar que los beneficios de este dominio digital" (Observatorio de la Ciberseguridad en América Latina y el Caribe, 2016.p. 12)

En Colombia, específicamente la Ciberdefensa y Seguridad de la Información ha evolucionado de tal forma que el Ministerio de Defensa está apoyando con semilleros, profesionalización y económicamente para adquisición de nuevas tecnologías al sector defensa para apoyar a las Fuerzas Militares, esto por medio del Comando Conjunto Cibernético (CCOCI), quien es el encargado de la defensa del país en el Ciberespacio (Camacho, J. 2016, p.8).

De ahí que, el CCOCI reúne a cada una de las Unidades Cibernéticas de las Fuerzas Militares con el fin de controlar los ataques Cibernéticos de las Infraestructuras Críticas Propias y las que le sean asignadas bajo su responsabilidad de acuerdo con su rol misional (Villanueva, J. 2015, p.5).

De igual forma, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT es un organismo coordinador que apoya al (CCOCI) a nivel nacional en aspectos de Ciberseguridad y Ciberdefensa, además de ello tiene como misión la protección de la infraestructura crítica del Estado Colombiano frente a emergencias que atenten o comprometan la Seguridad y Defensa Nacional (COLCERT, 2020).

Es así como Las Fuerzas Armadas del mundo para (Peralta Rodríguez, O. H. 2015), a corto y mediano plazo, se han visto obligadas a cambiar sus escenarios pasando de la guerra en campo físico al campo virtual, generando un cambio en las políticas y estrategias relacionadas con actualización de su doctrina, optimización de recursos y personal especializado, con el fin de orientar sus esfuerzos hacia las nuevas amenazas; en el caso de las Fuerzas Militares de Colombia, estas actividades han cobrado gran importancia y prioridad sin descuidar la problemática del conflicto interno.

Por esta razón, las Fuerzas Militares se deben preparar con equipos de tecnología, talento humano y herramientas para afrontar la lucha antiterrorista, con el fin de neutralizar los ataques de las plataformas informáticas de los terroristas; fomentando una educación digital y priorizando una nueva forma de ver el mundo, para combatir las intenciones de los delincuentes cibernautas, las intenciones de las organizaciones terroristas, y adelantarse a los planes de ciberataque de las organizaciones extremistas opositoras (Peralta Rodríguez, 2015. p.23).

De ahí que, la Infraestructura Militar deba ser adaptada a las realidades de seguridad de la presente época siendo lo suficientemente flexibles como para adaptarlos a los peligrosos avances militares de este nuevo siglo. La misma esencia del internet libre y generoso con la información y conocimiento se está cambiando debido al Ciberterrorismo y al fraude cibernético.

Por lo tanto, Las Fuerzas Militares deben estar preparadas para actuar y regular el efecto que un delito informático pueda ocasionar a la institución, con la experiencia y habilidad técnica suficiente para contrarrestar o minimizar las acciones Cibercriminales o Ciberterroristas y la pericia suficiente para establecer los rastros, registros y efectos de dichas acciones ocasionados por intrusos o dentro de las redes y sistemas en medio de la ausencia física del autor sin fronteras su anonimato e impunidad (Peralta Rodríguez, O. H. 2015, p.24).

En ese sentido, la Ciberdefensa un aspecto esencial y estratégico para la defensa nacional el uso de las comunicaciones y tecnologías de la información; se han incorporado en el diario vivir de la nación forzando el crecimiento y el desarrollo de las actividades económicas y sociales revolucionando por aportar beneficios al mundo pero también provocando riesgos a los que están expuestos los ciudadanos la industria y los gobiernos amenazas que son uno de los mayores retos a solucionar para mantener la seguridad y defensa nacional (Sanabria, D. 2018, p. 14).

Por consiguiente, para garantizar la seguridad y la infraestructura nacional del Gobierno Colombiano es necesario fortalecer las capacidades técnicas y tecnológicas articulando los esfuerzos civiles militares dentro del ciberespacio.

Así mismo, con el apoyo del Comando Conjunto Cibernético conformado por las Fuerzas Militares y las Unidades Cibernéticas del Ejército Nacional, La Armada Nacional y La Fuerza Aérea Colombiana se proporcionará la defensa del país a través de estrategias que permitan prevenir y contrarrestar toda amenaza de ataque de naturaleza cibernética que afecte los valores e intereses de la nación (Sanabria, D. 2018, p. 36).

Por tal razón, la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra a través de su grupo de investigación "Masa Crítica", categorizado en nivel (C) por Colciencias, planteó que es fundamental desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado, así como mejorar la protección, preservar la integridad y la resiliencia de la infraestructura Crítica-Cibernética Nacional; para lo cual es necesario adecuar un marco jurídico para abordar la protección y defensa del mismo (Becerra, J. et al., 2019).

Sin embargo, para lograr esto se necesita capacitación y sensibilización, pero lo más importante es la cooperación para fortalecer el intercambio de información entre todas las entidades nacionales e internacionales que nos permiten construir mancomunadamente un ecosistema más seguro, así como prevenir reaccionar y mitigar las amenazas digitales.

Finalmente la investigación del Coronel Diego Luis Sanabria frente a la propuesta de creación de una brigada cibernética para el Ejército Nacional de Colombia, el autor propone crear una infraestructura crítica de la institución en la que esta unidad realiza operaciones de defensa pasiva y defensa activa en todo el territorio nacional y además de ello, su principal objetivo de la unidad de Ciberdefensa es que forme parte del control y protección de los datos informáticos del Estado colombiano debido a que el mundo

digital al ser "tan libre" podría originar que organizaciones criminales y terroristas atentaran contra la nación (Sanabria, D. 2018, p. 36).

Ya que el enemigo puede atacar las redes de comando y el menciona que el ciberespacio es un nuevo campo de batalla hay que partir de una diferencia básica entre el armamento regular o tradicional y las tecnologías informáticas al interponerlo como modelo de defensa y seguridad (Sampaio, F. 2001).

Para Rodrigo Cortés (2015), en ese sentido, manifiesta que, con la materialización de la era digital, Internet y la sociedad de la información han emergido nuevos desafíos para los Estados y los distintos sectores de la sociedad, que han hecho necesario implementar políticas públicas que permitan hacerles frente.

En ese sentido (Gaitán, A. 2012. p. 25) propone lo siguiente: "Los estados deben prepararse para librar la Ciberguerra y ganarla", esto quiere decir que, el poder militar al exigir la concepción estratégica operacional y táctica debería reconocer la importancia de las tecnologías informáticas en relación con la Seguridad Nacional y aunque el número de países que se han percatado de la realidad del Ciberespacio hayan aumentado, su modelo de Ciberdefensa[3] como nuevo campo de batalla se debe incrementar.

[3] Término el cual Adriana Llongueras Vicente (2013, p. 19) citado por Vargas, E. (2014) manifiesta que es un elemento de poder dentro la seguridad nacional, y que a través de este nuevo y artificial dominio que ejerce una innovadora influencia estratégica en el siglo XXI.

Por tanto, los actores principales para desarrollar las operaciones militares de las FFMM en Colombia deben no solo centrarse en la soberanía nacional sino a la vez en el dominio digital.

2. **Evaluar los principales sectores que han sufrido ataques cibernéticos que afectan la Seguridad y Defensa Nacional.**

La creciente participación de ciudadanos en el entorno digital trae consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para contrarrestar las amenazas, los ataques e incidentes en la seguridad digital.

Por ejemplo, según estimaciones de Accenture, el costo para los negocios derivado del impacto de los ciberdelitos ha incrementado en un 72 % entre 2014 y 2019 (Accenture, 2019); esto exponiendo tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. En consecuencia, a ello, el desarrollo de una economía digital, para cualquier país, requiere la construcción de un entorno digital seguro, como elemento clave para que sea confiable y además esté acorde con el aumento y dinamismo de las actividades digitales.

En ese orden de ideas, debido a la existente dinámica en el Ciberespacio y la evolución de las amenazas Cibernéticas, las organizaciones ya sean públicas o privadas deben mantener operaciones conjuntas con el fin de fortalecer precisamente, sus apoyos a la Infraestructura Crítica Cibernética.

El Ciberespacio según lo anterior, es considerado como un nuevo teatro de batalla para los conflictos armados del Siglo XXI; de ahí que se plantee como a finales del siglo XX los Ejércitos de las potencias ya empezaban a hablar sobre information War, es decir la guerra de la información. Considerado este, "como un sistema integrado de comunicación capaz de desarrollar una defensa y una ofensiva de carácter estratégico" (Gaitán, A. p.17, 2012) para robustecer capacidades humanas, operativas y estratégicas que se integren y apoyen las acciones de protección.

En comparación a lo anterior, (Becerra, J. et al. p. 197, 2018) la seguridad digital en América Latina presenta un gran interés por investigar las posibles debilidades y los ataques sufridos a su Ciberdefensa, tratando de evitar vulnerabilidades reportadas.

> Para el caso de Colombia, este índice muestra que, en relación a la evolución del entorno de confianza digital, el país ocupa el puesto 32 entre un total de 42 países, con un puntaje de 2,33, ubicándose por debajo del promedio global (2,78 puntos). (Foro Económico Mundial - FEM, 2018)

Ya que a partir del Informe Global de Riesgos 2019 se presentó que, el fraude de datos, los ciberataques y las vulnerabilidades tecnológicas, aparecen como grandes preocupaciones junto a eventos climáticos o desastres naturales, ubicándose dentro de los diez principales riesgos globales con mayor grado de probabilidad de ocurrencia (Foro Económico Mundial - FEM, 2019).

En ese sentido, entre noviembre de 2017 y septiembre de 2019, se originaron alrededor de 536 millones de ataques en el país" (contados entre inicio de sesión malicioso

y ataques a aplicaciones web). (Holmes et al., p.16, 2020). Haciendo evidente que el entorno digital es un dominio que nos conecta con el resto del mundo, entonces hay un gran número de ataques a los cuales se encuentran expuestos los ciudadanos en Colombia, no sólo por los ataques que pueden suceder en el país, sino por la sumatoria de ataques que se ocasionan globalmente.

Con lo anterior, Global Cibersecurity Index, que tiene como propósito medir el compromiso de 175 países evaluados en torno a la Ciberseguridad, y el cual genera un ranking mundial dio a conocer por medio de 5 pilares: (legal, técnico, organizacional, construcción de nuevas capacidades y cooperación), que Colombia debe mejorar la confianza y la seguridad digital. Debido a que pasó del puesto 46 en la versión 2017 al puesto 73 en la versión 2018, perdiendo así varias posiciones en corto tiempo, lo cual evidencia que Colombia no ha mejorado sus capacidades para dar respuesta oportuna a incidentes y amenazas en seguridad digital. (Unión Internacional de Telecomunicaciones, 2018)

Por esta razón, es importante plantear que dentro de los retos que tienen los países actualmente, en relación a la Seguridad y Defensa Nacional es evitar los ataques anónimos en el ciberespacio[4] el cual nos permite que Colombia realice una política efectiva para mitigar los riesgos de seguridad digital.

Según el CONPES 3995 de 2020, se evidenció que en Colombia hay deficiencias en todo el

[4] Feliú Ortega, L. (2013, p.8) Citado por Borrero, R. C. (2015): El Ciberespacio es el espacio artificial creado por el conjunto de Sistemas de Información y Telecomunicaciones que utilizan las Tecnologías de la Información (informática) y las Comunicaciones (telecomunicaciones)] interconectados a nivel mundial. El ciberespacio es pues mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio.

conjunto de las capacidades relacionadas con la seguridad digital tanto por parte de los ciudadanos del sector público y del sector privado (Holmes et al., p. 23, 2020); causando que el país presente bajos niveles de preparación y de avance en la materia, lo que a su vez incrementa la vulnerabilidad de la defensa ante ataques y amenazas cibernéticas, deteriorando la confianza y el normal desarrollo de nuestro entorno digital.

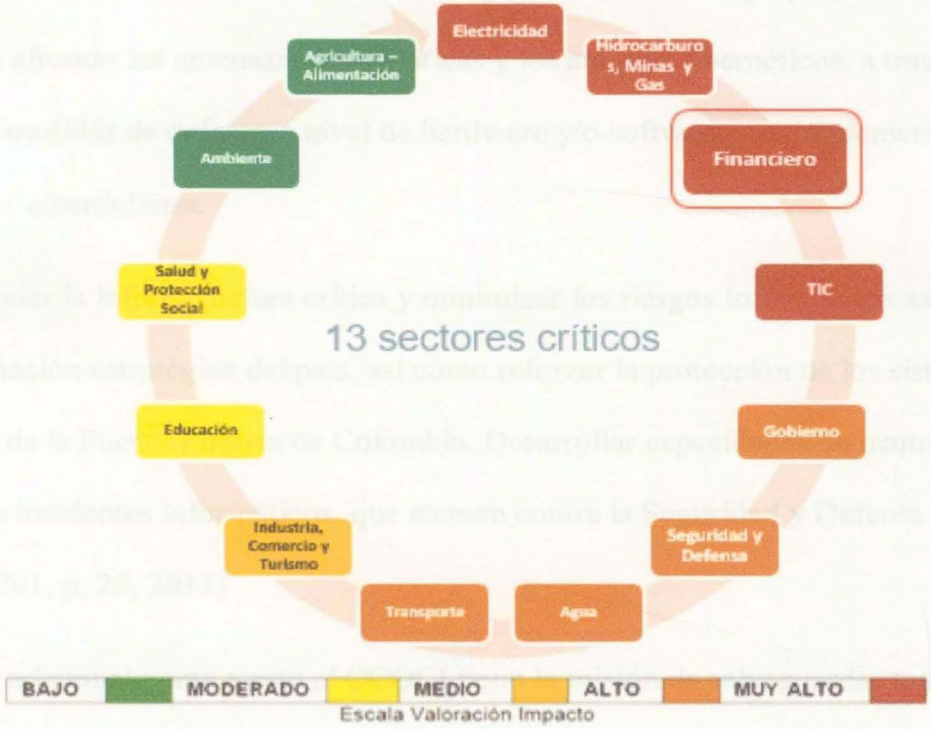
De esta manera cabe evaluar, cómo podemos saber si una amenaza cibernética puede afectar la Seguridad Nacional de un país ¿Qué sectores de una nación, se pueden considerar críticos y cuáles no? Es por eso que el Ministerio de Defensa de Colombia admite que la protección de la soberanía y los ciudadanos depende en gran medida de la lucha contra la delincuencia cibernética y de la defensa de la Infraestructura Crítica Cibernética de Colombia.

Sin embargo, en controversia a lo anterior, el Gobierno Nacional, el Ministerio de Defensa y demás sectores del país ya venían desarrollando desde el año 2017 el Plan de Protección de Infraestructuras Críticas Cibernéticas PNPICC, cuyo objetivo principal fue el siguiente:

> Optimizar los niveles de protección de las infraestructuras críticas cibernéticas a través de la coordinación y articulación de los organismos e instituciones responsables; con el fin de reducir el riesgo, minimizar las vulnerabilidades, mejorar la prevención, preparación, respuesta y fortalecer la resiliencia e investigación cibernética nacional; contribuyendo al fortalecimiento del desarrollo económico y social de la nación, así como la Seguridad y Defensa Nacional en materia Cibernética. (Comando Conjunto Cibernético, p.1, 2017)

Por intermedio de sus comités se clasificaron los sectores según su prioridad, criticidad y nivel de emergencia de acuerdo a la infraestructura crítica Cibernética del país de la siguiente manera:

Trece Sectores Críticos del País



Catálogo de infraestructura crítica cibernética del país (2017).

Teniendo ya definidos estos sectores críticos se va a dar a conocer algunos datos estadísticos del sector defensa y el sector financiero que sufrieron ataques Cibernéticos o tuvieron alguna amenaza Cibernética y posteriormente concluir cómo estos dos sectores pueden afectar la seguridad nacional.

Estadísticas de los principales ataques cibernéticos sufridos al sector Defensa, específicamente las FFMM.

Desde la creación del CONPES 3701 de 2011 el Ministerio de Defensa asumió la primera responsabilidad en el diseño y creación de la estrategia de Ciberdefensa y Ciberseguridad del país y por este motivo, se creó El Comando Conjunto de las Fuerzas Militares (CCOCI) con el fin de fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.

Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia. Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional. (CONPES 3701, p. 25, 2011)

Pero, adicionalmente a esto el CCOCI tiene la misión de salvaguardar todos los activos informáticos de las Fuerzas Militares que puedan generar algún riesgo para la defensa estratégica del país.

Para nadie es un secreto que uno de los principales objetivos de los grupos hacktivistas y grupos delincuenciales es tratar de vulnerar y robar información secreta de las Fuerzas Militares y del país. De ahí que, la tabla que se presentará a continuación refleja cómo el CCOCI desde el año 2012 hasta la fecha ha tenido que mitigar varios ataques

cibernéticos demostrando así la capacidad de sus plataformas tecnológicas y estrategia de defensa pasiva.

Estadísticas CCOCI

INCIDENTES POR TIPO DE CATEGORIA / AÑO	INTRUSIONES	MALWARE	POLÍTICAS DE SEGURIDAD	COMPROMISO DE INFORMACIÓN	DISPONIBILIDAD	OBTENCIÓN DE INFORMACIÓN	
2012	13	10	20	0	15	12	70
2013	56	50	55	0	14	29	204
2014	177	54	32	0	28	3	294
2015	281	145	55	5	19	5	510
2016	121	492	34	4	34	32	717
2017	84	339	60	0	32	96	611
2018	53	248	11	3	15	32	362
2019	26	161	49	6	37	103	382
2020	13	73	19	11	11	13	140
Total							3290

Comando Conjunto de Ciberdefensa de las Fuerzas Militares (2020).

Una vez verificado el cuadro de estadística del CCOCI se puede analizar que los ataques cibernéticos incrementaron cada año demostrando así, que este es uno de los sectores que más atención se le debe prestar debido a que el sector defensa es el principal bastión para mantener la seguridad nacional y controlar cualquier nivel de amenaza que pueda alterar la independencia nacional, la integridad territorial y la convivencia pacífica de sus ciudadanos.

De este modo, se puede analizar que existe una variación de ataques buscando vulnerar la seguridad informática de las redes de las FFMM; iniciando con Malware básico como Phishing, y Denegaciones de servicio hasta ataques más complejos como Amenazas Persistentes Avanzadas (APT) y así poder limitar los controles que tienen las plataformas tecnológicas.

Los analistas del CCOCI también han hallado que las plataformas informáticas de las Fuerzas Militares no son atacadas por simples grupos hacktivistas sino por organizaciones que en el mundo de las Ciberdefensa pueden realizar Ciberterrorismo desde otras naciones.

Todos estos factores mencionados anteriormente, demuestran que el Sector Defensa en cabeza de sus Fuerzas Militares deben hacerse un autodiagnóstico para medir la Capacidad de Defensa para superar cualquier tipo de ataque cibernético y a su vez, tener una resiliencia en contra de grupos ciberterroristas, y así conocer más a fondo las vulnerabilidades de la Institución, su infraestructura y tener en cuenta que este es un trabajo mancomunado que debe realizarse con otras entidades tanto públicas como privadas, y con miembros de las FFMM de otras naciones.

Estadísticas de los principales ataques cibernéticos sufridos al sector Bancario

La Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, es el gremio representativo del sector financiero colombiano, y es un miembro activo del comité de Protección de Infraestructuras Críticas Cibernéticas debido a que su sector está dentro de los 4 más críticos para el país y es la entidad encargada de publicar y gestionar cualquier incidente Cibernético trabajando siempre de la mano del Centro Cibernético Policial.

Según un análisis del panorama de las amenazas financieras publicado por los expertos de Kaspersky Lab, casi la mitad de los ataques de phishing tenían como objetivo robar el dinero de una entidad financiera y esta información se complementa con el dato aportado por la OEA en su reporte "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe" (Asobancaria Memoria Anual, 2019).

En el que revela que 9 de cada 10 bancos de América Latina y el Caribe sufrieron incidentes cibernéticos el último año. el 37% de los bancos de la Región fueron víctimas de ataques que resultaron efectivos, el 39% de los incidentes no son reportados, dato que en el caso de las entidades bancarias de mayor tamaño baja hasta el 19% y 6 de cada 10 usuarios que no utilizan servicios de banca digitales lo hace por desconfianza sobre la seguridad de las transacciones.

En ese sentido, se utilizó los datos estadísticos suministrados por del informe "tendencias Cibercrimen Colombia 2019 – 2020" realizado por el Centro de Ciberdefensa Policial (CCP) y la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, donde se reportó lo siguiente:

- El delito informático más denunciado en Colombia es el hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.

- Durante los meses de enero hasta la tercera semana de marzo de 2020, las denuncias por Ciberdelitos en Colombia reportaban un incremento de 6.082 casos, es decir, un 8% más respecto al mismo periodo del 2019.

- El delito de Suplantación de sitios web para capturar datos personales se convierte entonces en la infracción penal con mayor auge en 2020.
- Los esquemas de phishing bancarios son los líderes absolutos entre todos los tipos de phishing financiero. Uno de cada cuatro ataques (25,76 por ciento) utilizó información falsa de la banca en línea, u otro contenido relacionado con los bancos.

Análisis al Sector Financiero

SECTOR FINANCIERO	
TIPO DE ATAQUES	**PORCENTAJE 2019**
Troyano bancario	29%
APT	21%
RAT	16%
Ransomware	9%
Botnet	8%
Spyware	5%
ATM	4%
Exploits	3%
POS	2%
Skimmer	2%
Keylogger	1%
Backdoor	0.5%

CSIRT Financiero Asobancaria (2019).

Por lo anterior, se puede establecer como a favor del sector financiero se pudo establecer que más del 50% de las entidades cuenta con soluciones SIEM (Security Información Event Management) que permiten recopilar registros e información relacionada con la seguridad informática, analizarla, detectar posibles comportamientos anómalos para tomar medidas defensivas oportunas, con el que también que están

realizando dos o más veces al año pruebas de hacking ético para encontrar vulnerabilidades que pudieran facilitar la intrusión de ciberdelincuentes a los sistemas de información.

De igual forma, en el transcurso del 2019 Colombia sufrió 42 billones de intentos de ataques Cibernéticos, así mismo, es uno de los países que recibe más intentos de Ciberataques en la región, las empresas e instituciones gubernamentales. Por ejemplo, en este año, el "DoublePulsar" es otro de los Ciberataques más utilizados y estuvo entre los cuatro con más recurrencia en el país; este troyano se empleó sobre todo para afectar sistemas de instituciones financieras, y fue el vehículo que se utilizó para distribuir malwares como lo hizo "Ransomware" en 2017, uno de los Ciberataques que afectó a gran parte del mundo (Dinero, 2019).

> No obstante, "Las acciones y grupos de trabajo de las unidades de seguridad e investigación informática y forense de la Policía y las Fuerzas Armadas, aunque están en un alto nivel", Según mediciones del Centro de Cibercrimen de Microsoft, en los Estados Unidos, así como de empresas como Symantec, McAfee y Eset, Colombia es un país que ya muestra altos índices de criminalidad digital. Robos de identidad digital con fines extorsivos; de recursos de entidades, empresas y personas; ataques dirigidos contra oficinas del Estado y compañías financieras" Borrero, R. C. (2015, p.15). Por esta razón, el entorno digital de las empresas tanto gubernamentales como las que no lo son, deben evitar a toda costa las amenazas crecientes que utilizan los Cibercriminales

De igual manera, "el secuestro" de equipos e información pública y privada, son algunas de las modalidades que más crecen en Colombia. Según, El Tiempo (2019) en un artículo titulado El "Plan Colombia" para la Ciberseguridad, Colombia tendría un sistema

de seguridad externa (Ciberdefensa) y otro de políticas internas (Ciberseguridad). Ambos con coordinación unificada y con enlace directo a Presidencia, refuerzo de personal, el pie de fuerza en seguridad digital crecerá. Se destinarán más recursos a los comandos y grupos de investigación de defensa y seguridad digitales. En este aspecto, se aumentará el presupuesto y el trabajo con expertos privados.

3. Comparar la metodología sobre Ciberdefensa utilizada en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN.

En este apartado se comparará la metodología empleada en el Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN debido a que este fue el primer modelo de integración de varios países para luchar en contra de las Ciberamenazas logrando de esta manera unir el sector defensa, el sector privado industrial y el sector educativo de las naciones entendiendo que la Ciberdefensa y la Ciberseguridad es un trabajo colectivo.

Igualmente, se dará a conocer cómo han sido las estrategias de buenas prácticas propuestas por este centro de excelencia y como los países de la OTAN los ha venido incluyendo dentro de sus estrategias de seguridad nacional debido a que cada país maneja una posición frente a la estrategia de Ciberdefensa en relación a la seguridad nacional.

En materia de Ciberdefensa, la estrategia de unión y trabajo colaborativo entre los países para identificar y mitigar las amenazas cibernéticas se materializó a través del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN el cual es un centro de ciberdefensa multinacional e interdisciplinario donde se realizan investigaciones,

capacitaciones y ejercicios en cuatro áreas fundamentales: tecnología, estrategia, operaciones y derecho (CCDCOE, 2020).

En ese sentido, este centro de excelencia se estableció desde el 2008 por iniciativa de Estonia junto con otras seis naciones (Alemania, Italia, Letonia, Lituania, República Eslovaca y España).

> "El caso de Estonia fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica" (Fonseca, C. 2013, p. 129).

A partir del año 2010, la CCDCOE organiza anualmente el ejercicio internacional de defensa cibernética de fuego real más grande y complejo del mundo, denominado Locked Shields, y uno de los logros de investigación más conocidos y reconocidos internacionalmente para esta institución ha sido el proceso del Manual de Tallin.

A partir de enero de 2018, (CCDCOE, 2020) es responsable de identificar y coordinar soluciones de educación y capacitación en ciberdefensa para todos los organismos de la OTAN; y para ello, se basa en sus cuatro áreas fundamentales: tecnología, estrategia, operaciones y derecho.

El primero, plantea la necesidad de la tecnología puesto que es el vínculo entre el hombre y el ciberespacio. Todo se mueve en "Bits", y aún más con los nuevos fenómenos como la internet de las cosas (IoT), la inteligencia artificial (I.A.), las redes sociales, los sistemas S.C.A.D.A. (Supervisory Control And Data Acquisition), el big data, los UAV (Unmanned Air Vehicle), el cloud computing y el 5G entre otras. (Martínez, C. 2020).

Para ello el centro de excelencia a través de sus laboratorios de investigación ha definido que la principal estrategia para poder identificar estas nuevas amenazas tecnológicas es a través de la capacitación y el constante entrenamiento para que el personal identifique y coordine soluciones en ciberdefensa para todos los organismos de la OTAN en toda la Alianza.

Para ello, la OTAN ofrece un portafolio de Capacitación con el que se centra en entrenar a nivel estratégico a través de seminarios cibernéticos ejecutivos que capacitan a nivel operativo y técnico la importancia de la planificación operacional la inteligencia operativa sobre amenazas cibernéticas y la protección de infraestructura de información crítica. Así como el entrenamiento técnico con el que se pretende contrarrestar los malware y los exploits, la supervisión de ciberdefensa, la detección de amenazas , la defensa y ataques de sistemas de TI, la mitigación de botnets, la seguridad de sistemas de control industrial y por último la importancia de los sistemas de control industrial, el análisis forense de teléfonos inteligentes entre otros; todo esto, para comprender los conceptos básicos de seguridad web y la obligación de incluir un entrenamiento legal por medio de un curso derecho internacional sobre las operaciones cibernéticas.

El segundo, concibe el estudio de las estrategias ya que las amenazas que un ciberataque realizado a cualquier país puede modificar las variables de la dinámica de un conflicto, pasando desde generar una crisis en una infraestructura hasta poder llegar a definirse como una agresión y desarrollar una guerra

Pero el interrogante en el ciberespacio es ¿Quién generó este ciberataque?, ¿quién o qué estado se tomará la autoría?, fue interno o externo o simplemente es una guerra hibrida de quinta generación que busca es hacer terrorismo y desestabilizar una nación a través de sus activos críticos. Esto es lo complejo que tienen que definir los diferentes países en la creación de una estrategia en Ciberdefensa y a su vez que sea una estrategia que proteja la defensa y seguridad nacional.

Para ello, el CCDCOE ha diseñado una guía de referencia destinada a apoyar los esfuerzos nacionales de desarrollo de estrategias de seguridad cibernética. El proceso fue liderado por la Unión Internacional de Telecomunicaciones (UIT). La guía representa un recurso integral completo para que los países obtengan una comprensión clara del propósito y el contenido de una estrategia nacional de ciberseguridad, Así mismo describe prácticas existentes con sus modelos. Entre los materiales de referencia se encuentran dos publicaciones de la CCDCOE de la OTAN, las Directrices de la Estrategia Nacional de Seguridad Cibernética y el Manual Marco Nacional de Seguridad Cibernética y los clasifica en 5 temáticas: Estrategias de seguridad cibernética, Estrategias de seguridad y defensa nacional, Legislación nacional, Declaraciones sobre derecho internacional e Informes de países.

En tercer lugar, se encuentra el alistamiento de las plataformas de Ciberdefensa por medio de operaciones, debido a que siempre los países deben estar preparados para recibir ataques de cualquier enemigo y en cualquier momento; por eso para el centro de excelencia la mejor forma de estar preparados para una operación es a través de la realización de ejercicios de Ciberdefensa tan reales que exijan a los países miembros de evaluar sus fortalezas y debilidades y para ello organiza estos ejercicios dirigidos a expertos técnicos, personal militar y tomadores de decisiones en los países miembros y dentro de la OTAN.

Los ejercicios más destacados por el centro de excelencia son: Ejercicio de interoperabilidad de Coalition Warrior (CWIX). La mayor prueba de interoperabilidad de la OTAN, un ejercicio en vivo en el que los aliados y socios de la OTAN practican el intercambio de tácticas, técnicas y procedimientos para mejorar la detección de incidentes cibernéticos y el tiempo de respuesta necesario para identificar y resolver nuevas amenazas de seguridad emergentes.

La Coyuntura tridente, el ejercicio más grande de la OTAN en décadas, donde los aliados de la OTAN y los países socios están probando su capacidad para operar juntos para defender nuestras poblaciones y territorios y disuadir a los adversarios potenciales.

El Jaguar tridente, un ejercicio de la OTAN que entrena y evalúa operaciones de respuesta a crisis que involucran capacidades de combate de guerra de alta intensidad en las primeras fases de tales operaciones y Operaciones Conjuntas Pequeñas Pesadas en Tierra.

La Coalición cibernética, el ejercicio pone a prueba y entrena a los ciberdefensores de toda la Alianza en su capacidad para defender las redes nacionales y de la OTAN.

Locked Shields, un ejercicio de ciberdefensa internacional único que ofrece el desafío técnico de fuego real más complejo del mundo y por último, Crossed Swords un ciber ejercicio técnico de teaming rojo organizado por la CCDCOE desde 2016.

Finalmente, la última área fundamental es el Derecho, porque como lo manifiesta Jesús Reguera Sánchez "El Derecho debe irrumpir en el ciberespacio como, por ejemplo, lo hizo con el espacio aéreo y las aguas territoriales" (2015, p. 7), y este ha sido uno de los factores más importantes para el centro de excelencia y de prioridad fue el tratar de analizar y estandarizar cómo aplicar el derecho internacional en los conflictos cibernéticos y la guerra cibernética. Las leyes en el ciberespacio, como en cualquier otra dimensión, debe entenderse con algunas limitaciones innatas y más en el tema de la seguridad y defensa de una nación.

Para ello, en el Centro de Excelencia diseñó en Londres de 2013 el Manual de Tallin como consecuencia de la falta de legislación aplicable a las nuevas guerras en el ciberespacio, una de las primeras iniciativas de este Centro, fue la convocatoria de un Grupo Internacional de Expertos (GIE) en defensa, ciberseguridad y Derecho internacional, para que trabajaran en lo que pudiera ser el equivalente de la Convención de Ginebra sobre el DIH, aplicado a los conflictos en el ciberespacio.

Algunos aspectos claves del Manual se centran en: Los Ciberataques y conflictos del DIH, la soberanía y responsabilidad, uso de la fuerza, el ataque armado, legítima defensa. Inminencia e inmediatez, principio de necesidad y proporcionalidad, así como participación directa en las hostilidades.

Posteriormente se diseñó el Manual 2.0 de Tallin, el cual sustituyó al primer Manual de Tallin. El grupo internacional de expertos para Tallin 2.0 fue más amplio tanto en origen (incluyendo miembros de Tailandia, Japón, China y Bielorrusia) y conocimientos especializados sustantivos (incluidos los expertos en derechos humanos, derecho espacial y derecho internacional derecho de las telecomunicaciones). El Comité Internacional de la Cruz Roja (CICR) fue invitado a enviar observadores, así como otros estados y organizaciones.

En última instancia, el Manual de Tallin 2.0 debe ser entendido sólo como una expresión de las opiniones de los Grupos Internacionales de Expertos en cuanto al estado de la ley. La intención del proyecto nunca ha sido ser una ley o producir un manual que tendría la fuerza de la ley.

El Manual de Tallin 2.0 está dividido en cuatro partes. La primera parte trata del derecho internacional general y el ciberespacio. La parte II abarca los regímenes especializados de derecho internacional y el ciberespacio. La parte III se refiere a la paz y la seguridad internacionales y a las actividades cibernéticas, que se extrae en su mayor parte de Tallin 1.0. Y la Parte IV es el resto de Tallin 1.0 y se aplica al derecho de los conflictos armados cibernéticos.

Y sus 20 capítulos mencionan la importancia de la: soberanía, debida diligencia, jurisdicción, responsabilidad de las leyes internacionales, operaciones cibernéticas no reguladas por las leyes internacionales, leyes de los derechos humanos internacionales, leyes consulares y diplomáticas, leyes del mar, aéreas, del ciberespacio, leyes internacionales en telecomunicaciones, acuerdos de paz, prohibiciones de intervención,

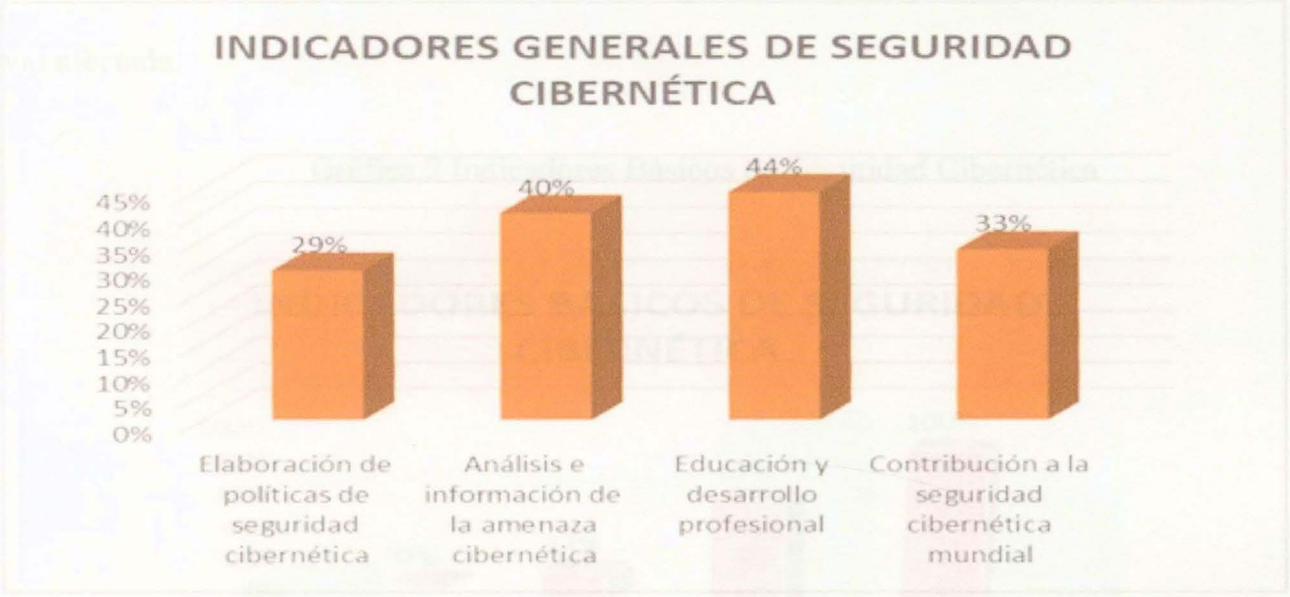
uso de la fuerza, seguridad colectiva, leyes generales del conflicto armado, conducta en hostilidades, actividades para ciertas personas y objetos, ocupaciones y neutralidad.

Colombia a pesar de ser unos de los primeros países de la región en buscar una estrategia en Ciberdefensa debe ser consciente que es importante mejorar en muchos de estos temas y llegar a un mejor nivel de madurez; por esta razón, debe realizar un benchmarking midiéndose con las mejores naciones y aprendiendo de los países que tienen una experiencia mayor en temas de Ciberdefensa y en este caso aprender del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN aprovechando que desde el año 2018 Colombia es "socio global" de la Organización del Tratado del Atlántico Norte (OTAN) y esto nos da el privilegio de participar en este selecto grupo de potencias.

A continuación, se realizará un comparativo de la estrategia de ciberdefensa realizado en Colombia basado en el Índice Nacional de Seguridad Cibernética (NCSI), el cual es un índice global que mide la preparación de los países para prevenir las amenazas cibernéticas y gestionar los incidentes cibernéticos. El NCSI también es una base de datos con materiales de evidencia disponibles públicamente y una herramienta para el desarrollo de capacidades de seguridad cibernética nacional.

Para gestionar estas ciberamenazas, un país debe tener las capacidades adecuadas para la ciberseguridad básica, la gestión de incidentes y el desarrollo general de la ciberseguridad. En este caso, Colombia en la última evaluación del año 2019, ocupó el puesto 60 entre 160 países que son evaluados por este índice (National Cyber Security Index, 2019); donde a continuación se mostrará cómo fueron evaluadas estas 3 capacidades y qué requiere Colombia para mejorar esta calificación.

Gráfica 1 Indicadores Generales de Seguridad Cibernética de Seguridad en Colombia.



Elaboración Propia (Villanueva, 2020), tomado de: National Cyber Security Index (2019) de: https://ncsi.ega.ee/country/co/

La gráfica 1, muestra unos indicadores basados en la elaboración de políticas, análisis de amenazas y un nivel de educación profesional en el país, en donde Colombia aún no alcanza un porcentaje aceptable.

A pesar que, la nación ya inició a implementar una estrategia de seguridad cibernética no existen todavía políticas definidas y los países más adelantados ya tienen hasta 3 políticas para la defensa de la ciberseguridad.

Por otro lado, a pesar que el indicador de educación alcanzó un 44% a diferencia de otros años, el indicador demuestra que en Colombia existen 41 programas relacionados con temas de ciberseguridad, pero aún no se plantea en el país una licenciatura ni un doctorado en ciberseguridad.

De igual forma, al no tener ningún foro o convenio internacional en el país en relación con el indicador de contribución a la seguridad mundial, su calificación también se vio afectada.

Gráfica 2 Indicadores Básicos de Seguridad Cibernética

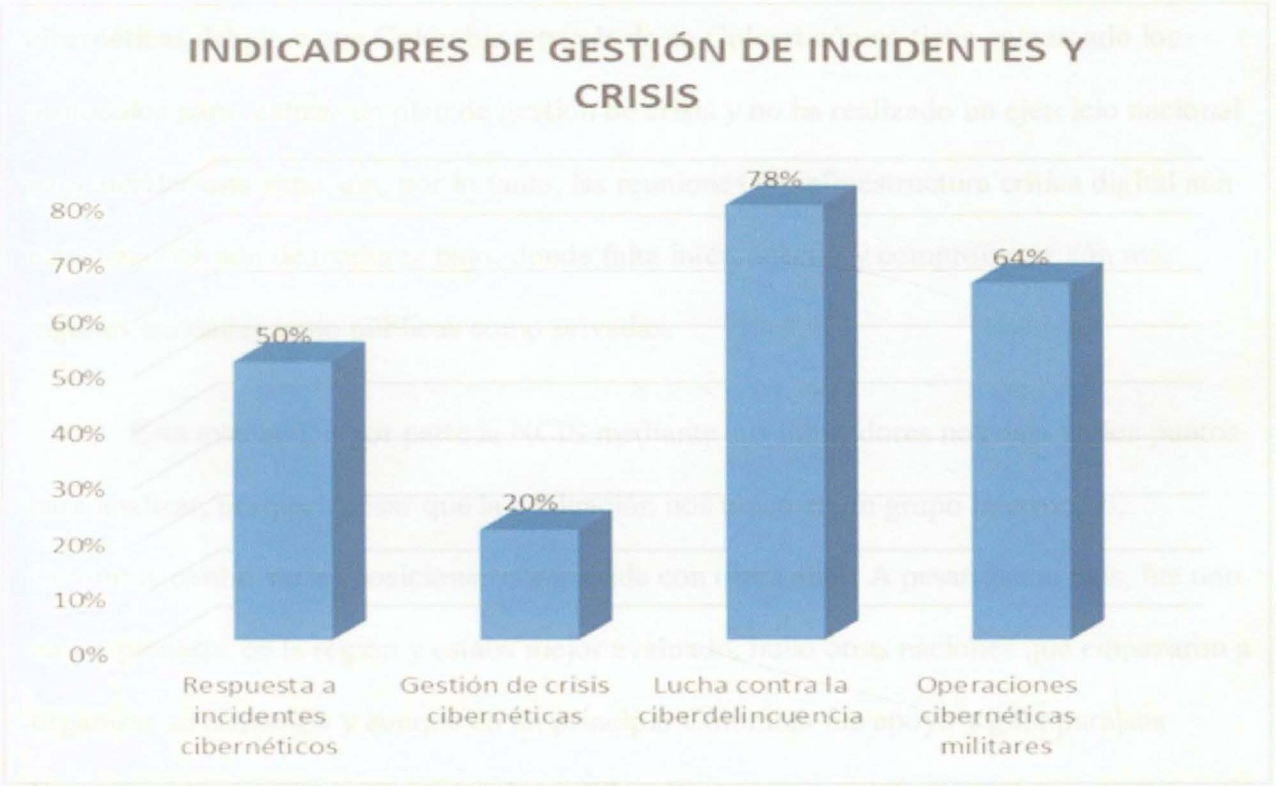
Elaboración Propia (Villanueva, 2020), tomado de: National Cyber Security Index (2019) de: https://ncsi.ega.ee/country/co/

La gráfica 2, muestra indicadores sobre protección en factores como servicios digitales, identificación electrónica y datos personales. De esta forma se puede visualizar una brecha donde Colombia tiene una calificación muy alta en la protección de los datos y la identificación electrónica gracias a la normatividad establecida como la ley 1273 de 2009 "protección de datos" y la ley estatutaria 1581 de 2012.

Pero a su vez, obtuvo una calificación muy baja en la protección de servicios digitales y esenciales donde muestran que tanto el sector público y privado aún no es consciente del tema de ciberseguridad y sus controles son muy básicos y en algunos casos

inexistentes; no mirándolos como una prioridad dentro de la entidad, ya que aún hay sectores que no emplean personal capacitado o no asignan responsabilidades ni recursos para asumir estos cargos.

Gráfica 3 Indicadores de Gestión de incidentes y crisis



Elaboración Propia (Villanueva, 2020), tomado de: National Cyber Security Index (2019) de: https://ncsi.ega.ee/country/co/

La 3 gráfica, es una de las más estables en la calificación donde involucra al sector defensa, en el que las instituciones de la Policía y las Fuerzas Militares han mejorado sus capacidades gracias a las estrategias impulsadas por los 2 Conpes del 2011 y el 2016.

Donde se demuestra ante el sector internacional que Colombia está luchando contra la ciberdelincuencia con el Centro Cibernético Policial (CCP), y se está preparando sus Fuerzas Militares en caso de emplear operaciones cibernéticas a través del CCOCI.

Como se puede observar, el indicador más bajo pertenece a la gestión de crisis cibernéticas debido a que Colombia a través de su Colcert aún no tiene enmarcado los protocolos para realizar un plan de gestión de crisis y no ha realizado un ejercicio nacional para atender esta situación, por lo tanto, las reuniones de infraestructura crítica digital aún están en un grado de madurez bajo, donde falta interconectar y comprometer aún más algunas entidades tanto públicas como privadas.

Esta evaluación por parte la NCIS mediante sus indicadores nos deja varios puntos para analizar, porque a pesar que la evaluación nos ubicó en un grupo intermedio, Colombia perdió varias posiciones comparada con otros años. A pesar que el país, fue uno de los pioneros en la región y estaba mejor evaluado, hubo otras naciones que empezaron a organizar su estrategia y aunque en un principio Colombia fue apoyo y guía para sus investigaciones, obtuvieron una mejor calificación.

Para terminar, una de las posibles causas de la baja calificación frente a los índices de Ciberseguridad, se debe a la ausencia de un marco de coordinación de políticas de Ciberseguridad en el cual el país no obtiene ningún puntaje, pese a que en el país existen diversas instituciones que trabajan en torno a la seguridad digital, la articulación entre dichas entidades no es clara y eficiente.

De igual forma, se evidenció que en Colombia hay deficiencias en todo el conjunto de las capacidades relacionadas con la seguridad digital, tanto por parte de los ciudadanos,

del sector público y del sector privado, causando que el país presente bajos niveles de preparación y se incremente el riesgo ante ataques y amenazas cibernéticas, deteriorando la confianza y el normal desarrollo de nuestro entorno digital.

Conclusiones

Como se pudo evidenciar en este artículo, el ciberespacio es un campo o dominio de batalla que tiene ciertas variables que generan ventajas para el enemigo como lo son el anonimato y la no existencia de fronteras reales, debido a que no es necesario tener un Ejército o una fuerza relativa superior basados en el número de hombres sino un equipo de expertos en temas informáticos. Esto sin contar que el ciberespacio sigue siendo un dominio sin regulación normativa.

Todo estas variables, hace que el ciberespacio tenga una complejidad VICA (volátil, incierta, compleja y ambigua); y a pesar que Colombia fue uno de los primeros países en Latinoamérica en alistarse para esta nueva amenaza y de acuerdo al Conpes 3701 le dio la acertada responsabilidad al Ministerio de Defensa de ser el garante de la ciberseguridad y la ciberdefensa en el país, lamentablemente se ha visto un estancamiento en este sector. Ya que según el Conpes 3995 que verificó el cumplimiento del plan de acción anterior, la nación no mejoró en el ranking mundial cayendo en el puesto 60.

Por tal razón, este artículo no solo estudió algunos sectores que sufrieron ataques cibernéticos sino cómo se están preparando las Fuerzas Militares para enfrentar las nuevas amenazas que genera este nuevo dominio de forma crítica, y para ello se analizó tanto las

fortalezas como las debilidades que se tienen, siempre siendo reflexivos que las Fuerzas Militares es una institución que depende de las políticas del señor presidente quién es el máximo comandante general y que todo, debe ir alineado a sus políticas.

Y estos indicadores reflejados por medio de la evaluación de ciberseguridad de la NCSI, donde las operaciones cibernéticas militares a cargo de la policía y las FFMM son un factor más de los muchos que regulan el país, ya que todos los indicadores deben estar interconectados apuntando hacia el mismo objetivo general el cual se preocupa por establecer una política de ciberseguridad a través de las estrategias de ciberdefensa y la ciberseguridad.

Las Fuerzas Armadas y la Fuerza Pública, en ese sentido han venido desarrollando unas estrategias militares en temas de ciberdefensa y ciberseguridad a través de sus manuales y directivas; pero paralelo a esta estrategia, uno de los pilares que dio inicio al proyecto de la estrategia de ciberdefensa en el país fue implementar una infraestructura robusta, alcanzando un nivel de madurez óptimo en tecnología y capacitación, no obstante, lo anterior se vuelve contradictorio porque el Conpes 3995 no destinó presupuesto para el sector defensa y se considere que con el mismo rubro de funcionamiento del Ministerio de Defensa se pueda mantener todas estas plataformas tecnológicas, su actualización y mantenimiento.

Así mismo la conjuntez con que trabajan las Fuerzas Militares debe ser un modelo para el sector privado que integran las entidades catalogadas con infraestructura crítica del país, porque este es un tema estratégico para la nación.

Y a pesar de diversas reuniones organizadas en cabeza del CCOCI y el COLCERT en donde se estudia dicha infraestructura, se observa cierta desconfianza para suministrar información que pueda afectar su reputación o goodwill ante el país, ya que no es fácil aceptar e informar que alguna entidad sufrió un ataque cibernético y posiblemente hubo robo de información, robo de dinero o daño informático que paralizó la entidad.

Por tal razón, sí las empresas públicas o privadas ocultan esta información no habrá manera de confrontar estos enemigos invisibles y estos ataques los seguirán realizando sin ningún control porque faltó colaboración por alguna entidad para alertar a las otras entidades.

Por otro lado, seguimos viendo la defensa y seguridad del Estado en el ciberespacio como algo netamente delincuencial, de robo de dinero o de grupos de hacktivistas que solo quieren bloquear páginas del Estado porque están en contra de este, pero hay que tener cuidado con esta forma de pensamiento.

Así como el Ejército cuida las fronteras terrestres, la Armada Nacional las fronteras marítimas y la Fuerza Aérea las fronteras aéreas, se debe cuidar la nación de los ciberataques o el Ciberterrorismo teniendo en cuenta un pensamiento y prospectiva estratégica de seguridad y defensa, en donde Colombia puede entrar en conflicto bélico con cualquier país de la región o del mundo, y la idea ni es ilógica o poco creíble porque en el ciberespacio no existe fronteras ni distancias; y un país aliado actualmente, en el siguiente gobierno puede ser un país desafecto, y este puede tener relaciones con potencias mundiales o países en otros continentes con su misma corriente y pensamiento político.

Lastimosamente Suramérica y Latinoamérica no es la Unión Europea para decir que todos se unen para luchar contra otra nación o grupo terrorista y hay que ser claros que en el ciberespacio no sabemos quién es nuestro enemigo o quién nos atacó.

Por eso las Fuerzas Militares deben seguir preparándose y capacitando a su personal, especializándose y manteniéndolo en sus cargos relacionados en temas de ciberdefensa y ciberseguridad, puesto que ha sido siempre una política los traslados cada dos años y sobre todo en el Ejército.

Pues, de nada sirve haber capacitado y entrenado a un oficial o suboficial dos años en temas de ciberdefensa y ciberseguridad si al término de este tiempo sale trasladado a unidades militares donde no va a continuar con su especialidad; y peor aún, que en muchos casos prefieren retirarse para irse a trabajar en una empresa privada. Mientras tanto esas entidades adquieren personal con experiencia y habilidades, y no tuvieron que invertir ni un solo recurso para capacitarlos.

Entretanto, las Fuerzas Militares tienen que volver a empezar desde cero capacitando a nuevo personal y retrocediendo en su transformación y nivel de madurez como lo solicitan las organizaciones mundiales que evalúan estos indicadores.

Otro factor primordial es la normativa mundial que regula las operaciones cibernéticas, para así saber qué pueden y no pueden hacer las Fuerzas Militares en el ciberespacio.

En el tema de la ciberdefensa y la ciberseguridad el país ha decretado muchas leyes y decretos, y ha firmado convenios como el de Budapest para tratar de frenar los

ciberdelitos, y con esto podemos sancionar y juzgar a una persona en Colombia por haber realizado un acceso indebido a un equipo informático.

¿Pero qué se debe hacer o a quién dirigirse en caso que un país o un grupo terrorista realice un ataque cibernético donde apague una terminal aérea y por motivo de esto, suceda un siniestro o también este ataque vulnere las medidas de control de un sistema SCADA de una hidroeléctrica y suceda una inundación en una región?

Colombia, a través de su COLCERT aún no tiene el respaldo normativo para contrarrestar y repeler estos ataques; por eso el país debe aprovechar, que siendo socio global en la OTAN debe aplicar el manual de Tallin para normativizar las operaciones en el ciberespacio. Ya que esta organización, a pesar de tener muchos detractores, es una guía para la ciberguerra, y algunas estrategias y políticas de defensa en el ciberespacio, permitiendo que este, sea un modelo para el país y así buscar que en la región también se estandarice estas normas y se adopte a los países de la región.

Por último, cabe preguntarnos ¿qué tan preparados estamos para afrontar un ciberataque? ¿somos lo suficientemente resilientes para superarlo? y sí las FFMM a través del CCOCI ¿puede apoyar un ciberataque a una empresa de infraestructura crítica del país? Por eso hay que ser claros y entender que la ciberdefensa se constituye en una capacidad que permite la supremacía militar, ser un apoyo estratégico a los otros dominios y convertirse en un factor de ventaja en situación de desigualdad armamentista.

Recomendaciones

Las Fuerzas Militares deben ser críticas y auto reflexivas en relación con la ciberdefensa al comprender que, aunque se tienen estrategias para su manejo, no somos los pioneros o líderes de la región en ciber como quisiéramos serlos.

Por esta razón, las siguientes recomendaciones no son basadas únicamente del estudio de este artículo sino también de otras investigaciones donde llegan a conclusiones muy similares para mejorar los índices calificativos de ciberdefensa y otros indicadores que se deben empezar a gestionar porque no existen; de este modo, se ayudará a fortalecer tanto la política del país como la estrategia de las FFMM en los temas de ciberdefensa y ciberseguridad.

La primera recomendación es la priorización de recursos para la capacidad de ciberdefensa, tanto en infraestructura como en capacitación, pero a su vez incluyendo un nuevo enfoque de trabajo integral que incluya la investigación, el desarrollo e innovación en el área de la ciberdefensa.

Segundo, entender que la capacidad de ciberdefensa no es un tema explícitamente de seguridad ciudadana sino un tema estratégico para la defensa del país, que puede afectar el correcto funcionamiento del Estado y para ello debe existir una política que respalde el desarrollo de la capacidad cibernética tanto en el campo político, normativo y técnico.

Tercero, el país debe contar con un marco normativo y doctrinal que permita el desarrollo de operaciones militares en el ciberespacio y de esta manera aplicar leyes de

referencia que protejan a las FFMM, para poder emplear las capacidades de ciber tanto en el campo defensivo como en lo ofensivo ante una posible agresión.

Cuarto, iniciar un modelo innovador de incorporación de talento humano que involucre a voluntarios en la defensa nacional del ciberespacio, sujeto al comando de las Fuerzas Militares con el fin de maximizar las capacidades, donde este modelo se articule a través de un sistema de acuerdos de colaboración, cooperación y comunicación con la academia, el sector público y privado en el ámbito nacional y con entidades internacionales.

La quinta recomendación es tener una nueva visión y diseño al plan de estudios del programa en ciencias militares, aeronáuticas y navales, donde se incluya la especialización en ciberdefensa y desde la educación básica de las escuelas de formación hasta los cursos de capacitación se impartan conocimientos en programación, desarrollo de código y temas de TI en general; que a futuro aporten con un personal apto para el diseño de proyectos en el área de la ciberdefensa.

Sexto, incluir la capacidad de operaciones cibernéticas como una nueva función de conducción de la guerra, para apoyo en el planeamiento estratégico y operativo. Esta nueva función ayudará a generar y mantener el poder de combate, alcanzar los objetivos y conseguir el estado final deseado de cualquier operación.

Séptimo, se debe actualizar y emplear las plataformas de entrenamiento en ciberdefensa que tiene el Comando General a través del CCOCI y empezar a adquirir nuevas plataformas por parte de los centros cibernéticos de las diferentes fuerzas.

En ese sentido, se ha dicho que el entrenamiento debe ser tan fuerte que la guerra parezca un descanso, y en el campo de la ciberdefensa debe ser igual; se debe entrenar tanto en estas plataformas que, en el momento de un ataque cibernético, la reacción sea inmediata y con capacidad de contraataque para proteger los sistemas de información e infraestructura crítica del país.

Por última recomendación, el proyecto más visionario y prospectivo corresponde a proponer un Centro de Excelencia Cibernética tipo OTAN en Colombia, que ayude a fortalecer y gestionar las políticas y estrategias de Ciberdefensa del país y de otras naciones, apoyado no solo en otros Ejércitos del mundo, sino también en especialistas de instituciones educativas y profesionales en áreas jurídicas y de investigación.

Referencias bibliográficas

Anguera, M. T. (1989). Metodología de la Observación en las Ciencias Humanas. En http://www.laislalibros.com/libros/metodologia-de-observacionciencias-humanas-L0280000964/

Accenture. (2019). Securing the Digital Economy. Reinventing the Internet for Trust. Obtenido de https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture- securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

Asobancaria, Memoria Anual (2019) Csirt Financiero 2019. En: https://mail.google.com/mail/u/1/?tab=wm&ogbl#inbox/FMfcgxwJXCJQPDNpSqSffJlrCKbfBqKl?projector=1&messagePartId=0.1

Becerra, J. Bohórquez, Castañeda, Sánchez, Páez, Baldomero & León (2019) La Seguridad en el Ciberespacio. Un desafío para Colombia. Bogotá. Maestría en Ciberseguridad y Ciberdefensa. Escuela Superior De Guerra "General Rafael Reyes Prieto". En: https://esdeguelibros.edu.co/index.php/editorial/catalog/download/42/48/741-1?inline=1

Borrero, R. C. (2015). Estado actual de la política pública de Ciberseguridad y Ciberdefensa en Colombia. Revista de Derecho, comunicaciones y nuevas tecnologías- No. 14, Julio diciembre de 2015. ISSN 1909-7786. Recuperado de: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

Camacho, J. (2016) Evolución de la Ciberdefensa y la Seguridad de la información en Colombia. Especialización de la Administración de la seguridad. Universidad Militar Nueva Granada. Bogotá. En: https://repository.unimilitar.edu.co/bitstream/handle/10654/14382/CamachoGarciaJuanDiego2016.pdf?sequence=1&isAllowed=y

Cámara Colombiana de Informática y Telecomunicaciones CCIT (2019) Tendencias del Cibercrimen en Colombia 2019-2020. En: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) (2020) Investigación. En: https://ccdcoe.org/about-us/

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN CCDOCOE (2017) Guía para la elaboración de una estrategia Nacional de Ciberseguridad. Participación Estratégica en la Ciberseguridad. Índice mundial de ciberseguridad. En: https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018/es

Consejo Nacional de Política Económica y Social(2011) Documento CONPES 3701. Lineamientos de política para Ciberseguridad y Ciberdefensa. En: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

CCOCI (2016) Catálogo infraestructura crítica cibernética de Colombia. Comando conjunto cibernético. Fuerzas Militares. Clasificado.

Comando Conjunto de Ciberdefensa de las Fuerzas Militares (2020). Estadísticas de los principales ataques cibernéticos sufridos al sector Defensa, específicamente FFMM.

Comando de las Fuerzas Militares (2016) Manual de Ciberdefensa Conjunta para las Fuerzas Militares 3-38. Primera Edición. En: Aplicación. Imprenta y publicaciones de las Fuerzas Militares. p. 9.

Comando Conjunto Cibernético (2019) Lineamientos de Ciberdefensa y Ciberseguridad para las Fuerzas Militares. Comando General de las Fuerzas Militares.

Dinero (2019) En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. En: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

Dirección de Asuntos Políticos Multilaterales (2017) Documento CONPES 3854. Política Nacional de Seguridad Digital. En:

https://www.cancilleria.gov.co/sites/default/files/planeacion_estrategica/conpes_3854_-_seguridad_digital.pdf

Fonseca, C. Perdomo, I. Arozarena, M. Ortíz, J. (2013) El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra. Revista de la escuela Superior de Guerra de la Argentina. En: http://www.cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf

Foro Económico Mundial - FEM. (2018). Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Obtenido de http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

Gaitán, A. (2012) el ciberespacio un nuevo teatro de batalla para los conflictos armados del Siglo XXI. En: capítulo primero albores de Las batallas ciberespacial es la transformación de la naturaleza de la guerra como producto de las tecnologías informáticas. División de investigación ESDEGUE. En: https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/212/330

Gómez, M. (2019) En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN y su posible transferencia a América del Sur. Editorial Autores de Argentina. ISBN 978-987-87-0208-7. En: https://www.educal.com.mx/0700-artes/9789878702087-en-busca-de-un-modelo-de-resiliencia-cibernetica-basado-en-las-experiencias-de-la-otan-su-posible-transferencia-a-america-del-sur.html

Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT (2020). El Gobierno de Colombia liderado por la Presidencia de la República comienza una

campaña de prevención cibernética. ¿Qué es y Cómo prevenir un ataque cibernético? En: http://www.colcert.gov.co/

Comando Conjunto Cibernético. (2017). Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. 51. En: https://www.ccoc.mil.co/recursos_user///PLAN_PUBLICO.pdf

Congreso de la República. Ley Estatutaria 1581 De 2012. Título IV. Derechos y Condiciones de Legalidad para el Tratamiento de Datos. Diario Oficial No. 48.587. De 18 de octubre de 2012. En: Http://Www.Secretariasenado.Gov.Co/Senado/Basedoc/Ley_1581_2012.Html

Hidalgo, J. (2013) Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. Monografías 137. Capítulo Primero: Principios de una Conciencia Nacional de Ciberseguridad. Escuela de Altos Estudios para la Defensa. Ministerio de Defensa de España. ISBN: 978-84-9781-862-9. En: https://publicaciones.defensa.gob.es/necesidad-de-una-conciencia-nacional-de-ciberseguridad-la-ciberdefensa-un-reto-prioritario-n-137-libros-papel.html

Holmes, C., García, T., & Hayes, C. R. (2020). Documento CONPES 3995. Política de Confianza y Seguridad Digital. 1–51. En: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx

Instituto Nacional de Tecnologías de las Comunicaciones. INTECO. (2018) Resiliencia: Aproximación a un marco de mediación. Madrid: CERT de Seguridad e industria- INTECO.

Martínez, C. (2020). Análisis prospectivo de la ciberdefensa del estado colombiano al año 2042.

National Cyber Security Index (2019) Índice Nacional de Seguridad Cibernética (NCSI) En: https://ncsi.ega.ee/country/co/

Observatorio de la Ciberseguridad en América Latina y el Caribe (2016) Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. En: http://www.observatoriociberseguridad.com/

PNPICCN (2017) Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PNPICCN V 1.0 Año 2017. En: https://mail.google.com/mail/u/1/?tab=wm&ogbl#inbox/FMfcgxwJXCJQPDNMrXnpxzPsdqGMzdNq?projector=1&messagePartId=0.1

Peralta Rodríguez, O. H. (2015). Ciberseguridad: nuevo enfoque de las Fuerzas Militares en Colombia. Bogotá. Universidad Militar Nueva Granada. Recuperado de: https://repository.unimilitar.edu.co/bitstream/handle/10654/7884/ensayo%20final%20EAS-2015%20UMNG%20OSCAR%20PERALTA.pdf?sequence=1

Realpe, M. Rodríguez, T & Hernández. J. (2014) Estrategia Nacional de Ciberseguridad y Ciberdefensa para la República de Colombia. Universidad de los Andes. Facultad de Ingeniería de Sistemas. Maestría en Seguridad de la información.

Reguera, J. (2015) Aspectos legales en el Ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. Grupo de Estudios en Seguridad Internacional. Universidad de

Granada. N. 7. p. 7. En: http://www.diariomilitar.es/jesus-reguera-aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario/

Rodrigo C. (2015) Retos de la Administración de Justicia frente a los Delitos Informáticos. Universidad Santo Tomas Sede Villavicencio. En: http://fiadi.org/wp-content/uploads/2015/08/Rodrigo-Cortes-Borrero.pdf

Sampaio, F. (2001, p. 2) ciberguerra: guerra electrónica e informacional un nuevo desafío estratégico. organizado para estudios científicos escuela superior de geopolítica de estrategia de Puerto alegre. Revista Científica ESDEGUE. En: https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/212/330

Sanabria, D. (2018) Propuesta de creación de una brigada cibernética para el Ejército Nacional de Colombia. Maestría en Seguridad y Ciberdefensa. Escuela Superior de Guerra.

Sampieri, R. (20016) Metodología de la investigación. Cuarta edición. McGraw-Hill Interamericana. México. En: https://s3.amazonaws.com/academia.edu.documents/38758233/sampieri-et-al-metodologia-de-la-investigacion-4ta-edicion-sampieri-2006_ocr.pdf?response-content-disposition=inline%3B%20filename%3DSampieri-et-al-metodologia-de-la-investi.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20200227%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200227T180705Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=447100c120c5bf6d8ab480d2ccf65e88b52491fd80c7b243b2d00879cbae1f85

Sarriá, E. y Brioso, A. (1999). Categorización y Observación de las funciones, morfología y características espacio-temporales de la comunicación intencional preverbal. En Arguilaga, M. Observación de conducta interactiva en contextos naturales: Aplicaciones. Recuperado de https://goo.gl/xWPCnQ

Tallinn Manual 2.0 (2017) On the international law applicable to Cyber Operations. Cambridge University Press. ISBN 978-1--316-63037-2.

Unión Internacional de Telecomunicaciones (UIT). (2018). Guía para la elaboración de una estrategia nacional de ciberseguridad. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Vargas E. (2014) Ciberseguridad y Ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional? Bogotá. Universidad Militar Nueva Granada. Especialización En Alta Gerencia De La Defensa Nacional. En: https://repository.unimilitar.edu.co/bitstream/handle/10654/12259/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf?sequence=1

Villanueva, J. (2015) La Ciberdefensa en Colombia. Universidad Piloto de Colombia. En: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2812/00002646.pdf?sequence=1