Concepto estratégico en ciberseguridad y ciberdefensa del Estado colombiano para contrarrestar los nuevos riesgos y amenazas que emanan del ciberespacio

Juan Guillermo Cid Gámez
Guillermo Enrique Fernández De La Barrera
Pablo Cesar Pabón Forero

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

2016

Ministerio de Defensa Nacional

Comando General Fuerzas Militares

Escuela Superior de Guerra

Concepto Estratégico en Ciberseguridad y Ciberdefensa del Estado Colombiano para contrarrestar los nuevos riesgos y amenazas que emanan del ciberespacio

Mayor Juan Guillermo Cid Gámez

Mayor Guillermo Enrique Fernandez De La Barrera

Mayor Pablo Cesar Pabón Forero

Especializacion Seguridad y Defensa Nacional

Bogota – Colombia

2016

CONTENIDO

Introducción..... 5

El Ciberespacio..... 9

Las Ciberamenazas..... 12

La Ciberseguridad..... 18

La Ciberdefensa..... 24

Conclusiones 33

Referencias Bibliográficas..... 36

Concepto Estratégico en Ciberseguridad y Ciberdefensa del Estado Colombiano para contrarrestar los nuevos riesgos y amenazas que emanan del ciberespacio[1]

Guillermo Enrique Fernandez De la Barrera[2]
Juan Guillermo Cid Gamez[3]
Pablo Cesar Pabon Forero[4]

Resumen

Los riesgos, amenazas y ataques provenientes del ciberespacio, han desencadenado una alerta mundial de gran impacto ya que pueden tener consecuencias en temas económicos, políticos o sociales. El propósito es plantear un concepto estratégico que permita diseñar los lineamientos en la toma de decisiones en todos los aspectos relacionados con amenazas provenientes del ciberespacio a partir de revisión y análisis documental correspondiente a ciberdefensa y ciberseguridad, y mediante la caracterización del estado actual de una de las entidades públicas con injerencia en el tema como lo es la Fuerza Aérea Colombiana.

Analizada la información se establece que los escasos lineamientos y políticas por parte del Estado en materia de Ciberseguridad y Ciberdefensa son insuficientes para contrarrestar las amenazas, riesgos y peligros que surgen del empleo indiscriminado del ciberespacio afectando el uso seguro de la información pública o privada. Así mismo, la insuficiente capacidad para evitar el daño a la infraestructura critica que soporta el flujo de información sensible y de interés del Estado.

---

[1] Artículo de reflexión presentado como opción de grado para optar por el título de Especialista en Seguridad y Defensa Nacional. Artículo vinculado al proyecto de investigación "Políticas y Modelos en Seguridad y Defensa" del grupo de investigación "Masa Crítica" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Los autores agradecen el apoyo institucional.

[2] Administrador Aeronáutico, Escuela Militar de Aviación, Oficial de Defensa y Seguridad de Bases de la Fuerza Aérea Colombiana. Correo Electrónico guillermito1974@hotmail.com

[3] Administrador Aeronáutico, Escuela Militar de Aviación, Oficial de la especialidad de vuelo de la Fuerza Aérea Colombiana. Correo Electrónico juancid23@hotmail.com

[4] Administrador Aeronáutico, Escuela Militar de Aviación, Oficial de la especialidad de vuelo de la Fuerza Aérea Colombiana. Correo Electrónico canario176@gmail.com

La información del proyecto proviene de la recopilación bibliográfica acerca de la ciberespacio, ciberamenazas, ciberseguridad y ciberdefensa, documentos rectores de ciberseguridad y ciberdefensa dentro la Fuerza Aérea Colombiana, documentos CONPES y casos de uso de importantes ataques informáticos llevados a cabo contra diferentes naciones. El artículo permite desde la perspectiva de la revisión documental plantear la importancia del establecimiento del Concepto Estratégico en Ciberseguridad y Ciberdefensa del Estado Colombiano estableciendo las políticas y criterios para hacer uso de las capacidades del Estado para salvaguardar el Ciberespacio colombiano.

Palabras Clave. Concepto estratégico, riesgos, seguridad nacional, ciberseguridad, ciberdefensa, amenazas cibernéticas, ciberespacio.

Abstract

The risks, threats and attacks from cyberspace, have sparked a global alert about the great impact they can have in economic, political or social ways. The purpose of this article is to analyze the documentation of cyber defense and cyber security, regulations and characterize the current state of the Colombian Air Force addressing this issue; in order to define a strategic concept to design the guidelines in decision-making in all aspects of threats from cyberspace.

After analyzing the information it states that the limited State guidelines and lack of provision of adequate resources by the institution to strengthen the cybernetics unity of the Colombian Air Force born in 2012 in order to protect the face of the threats emanating from cyberspace critical infrastructure of the FAC and strengthen intelligence and counterintelligence in cyberspace; are the main causes for a Strategic Concept does not exist in cyber security and

defense of the Colombian State to counter the new risks and threats to the infrastructure in public and private networks.

Project information comes from the bibliographic compilation about cyberspace, cyber threats, cyber security and cyber defense, governing documents of cyber security and cyber defense within the Colombian Air Force, CONPES documents and use cases of major cyber attacks carried out against different nations. The article allows from the perspective of the document review raise the importance in establishing the Strategic Concept in cyber security and cyber defense of the Colombian state as the rector and guideline criteria in managing risks from cyberspace element, serving as the foundation for development of normativities and establishing itself as a logical systematic, and objective decision making.

Key Words. Strategic concept, risks, national security, cyber security, cyber defense, cyber threats, cyberspaces.

Introducción

La presente investigación se desarrolló en el contexto del programa de especialización en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra en el curso de estado mayor en un estadio de tiempo de los últimos 10 años, la cual permitió construir el planteamiento de un concepto estratégico entendido como el establecimiento de una línea estratégico-programática que debe seguirse con el fin de realizar una reforma y/o modernización ideológica y estructural, de tal forma que sea más fácil, eficaz y eficiente enfrentarse a las nuevas necesidades del entorno; estableciendo de esta forma una proyección de la visión, del Estado, con plena viabilidad, que apunte a establecer parámetros a desarrollar por los responsables del medio denominado el ciberespacio (OTAN, 2010).

Para tal efecto, en la primera parte se puso en contexto los conceptos de seguridad y defensa nacional, al igual que la importancia del elemento constitutivo como lo es el "ciberespacio", entendido según (Gibson, 1984) como un ambiente virtual que permite la interacción entre nodos o usuarios a través de redes de computo.

Frente a esta definición se establece que si bien los beneficios de compartir y acceder a información en tiempo real son muchos respecto al aumento en la productividad y globalización, también representan un espacio más en el cual pueden generarse problemas en relación a la pérdida o fuga de información, ya que estas interconexiones crean un ecosistema virtual, en el cual también es necesario que el estado ejerza soberanía.

De igual forma, se abordaron los conceptos básicos respecto a las amenazas, la seguridad y la defensa del ciberespacio, con el fin de fortalecer e impulsar programas, políticas, proyectos y desarrollos específicos estableciendo como resultado el planteamiento de un concepto estratégico, que pueda conducirse desde el nivel estratégico y aplicarse en los niveles operacional y táctico sobre la inherente asimetría existente en cuanto a ciberseguridad.

Así mismo, se determinó si la Fuerza Aérea Colombiana se encuentra alineada con las políticas de ciberseguridad y ciberdefensa, a partir del análisis del estado actual de la institución frente a temas relacionados con el control del ciberespacio.

Finalmente, se planteó el concepto estratégico, considerando que si bien el concepto de ciberespacio es ampliamente usado y se encuentra inmerso dentro de las leyes de seguridad de la información. En la actualidad el gobierno no cuenta con un concepto estratégico claramente definido que permita tomar cursos de acción frente a su normalización de cara a la ciberdefensa y ciberseguridad.

Considerando que el estado colombiano carece de la definición de un concepto estratégico en materia de Ciberseguridad y Ciberdefensa, es preciso construir una propuesta que aborde estos aspectos dentro de un planteamiento marco que permita establecer los criterios de actuación y gestión para contrarrestar los riesgos, peligros y amenazas que afectan el uso del ciberespacio del Estado Colombiano.

Considerando que el conflicto interno colombiano ha permitido que todos los fenómenos de delincuencia en particular bandas criminales, terrorismo y tráfico de personas en especial menores de edad (redes sociales), utilicen como herramienta delictiva el ciberespacio y ha dado paso a que estas actividades perdieran su categoría de ser riesgos de menor impacto social para pasar a ser una amenaza potencial, que también encuentra apalancamiento de recursos por medio del narcotráfico para mitigar el accionar de la Fuerza Pública convirtiéndose a la fecha en crímenes Trasnacionales que pueden afectar varios estados.

Motivo por el cual es necesario definir a lo largo del documento los conceptos de ciberseguridad, ciberamenaza y ciberdefensa, y su importancia respecto a la conservación y contención de los ataques que puede llegar a sufrir la nación desde ciberespacio.

Es así como el resultado de la revisión documental de la legislación, normas, documentos CONPES, las leyes, las normas de seguridad de la información, derechos de autor, propiedad industrial e intelectual, comercio electrónico y firmas digitales, verificando la ausencia del concepto estratégico de ciberseguridad y ciberdefensa del estado colombiano, se pudo establecer la ausencia de criterios de orden estratégico en materia de Ciberseguridad y Ciberdefensa. Considerando que los conceptos estratégicos permiten establecer un curso de acción como resultado de la apreciación de una situación de carácter trascendental, y que desarrollo puede entenderse como la ruta para adaptarse a los cambios en el entorno y así mismo establece la

forma de actuar frente a ellos, mediante un enfoque sistemático, lógico y objetivo para la toma de decisiones (Marenco, 2015).

De otra parte es necesario que se estructure una definición que enmarque la seguridad nacional del país haciendo eficaz y oportuna la gestión de contrarrestar las nuevas amenazas afianzándolas con una política estratégica que vaya de la mano con la evolución de los sistemas informáticos y control de redes en el ciberespacio.

Adicionalmente es de suma importancia que dicha iniciativa nazca por intermedio de la Fuerza Aérea Colombiana armonizando un concepto que permita dar una orientación objetiva y clara de protección de los intereses del estado desde todos los sectores político, social, económico y militar.

El presente artículo se encuentra encuadrado dentro de un tipo de investigación descriptiva mediante un estudio cualitativo, donde se caracteriza documentación referente a ciberamenazas, ciberseguridad y ciberdefensa.

Así mismo se analiza cualitativamente la información correspondiente al desarrollo de conceptos estratégicos en manuales y procedimientos y la situación nacional actual; factores que inciden en la toma de decisiones y el establecimiento de planes, programas y normatividades frente a la ciberseguridad y ciberdefensa del estado colombiano.

La metodología llevada a cabo en el presente artículo se desarrolla a través de las siguientes fases metodológicas:

Fase 1: Revisión de la normatividad actual en lo referente a ciberamenzas, ciberseguridad y ciberdefensa, con el fin de sentar bases del proceso de investigación.

Indagación, clasificación y análisis de la información pública y reservada relacionada con los conceptos de ciberamenzas, ciberseguridad y ciberdefensa; así mismo, revisión y análisis de

la información a nivel mundial sobre los diferentes peligros y riesgos que surgen del ciberespacio.

Fase 2: Determinación de la alineación de capacidades de la Fuerza Aérea Colombiana frente a las políticas de ciberseguridad y ciberdefensa.

Considerando que la Fuerza Aérea Colombiana (FAC) es la institución responsable del control y la operación aérea y espacial de la nación según la constitución colombiana artículos 216 y 217. Se realiza una caracterización del estado actual de la institución frente al control del ciberespacio, con el fin de identificar y establecer el curso de acción frente al establecimiento de dichos aspectos como concepto estratégico de la nación.

Fase 3: Establecimiento del concepto estratégico en ciberseguridad y ciberdefensa del estado colombiano.

Estructuración de un concepto aplicable a los sistemas de ciberseguridad, ciberdefensa y ciberamenazas que establezcan políticas claras que permitan efectuar un trabajo coordinado y dinámico frente a la seguridad y defensa del ciberespacio Colombiano.

El ciberespacio

Actualmente todo tipo de interacciones se realizan en el ciberespacio; constituyéndose no solo como un repositorio de información sino como un canal que permite la transaccionalidad de la información tanto pública como reservada. Con el fin de establecer un proceso sistemático para el desarrollo del concepto estratégico, se expone a continuación una breve descripción de los aspectos integrales ciberseguridad y ciberdefensa.

Considerando que el ciberespacio es la base constitutiva de las comunicaciones y alberga el crecimiento y diversificación de la tecnología, es apropiado realizar un acercamiento a su

concepto y contextualización frente a la seguridad y defensa nacional, con el fin de establecer su importancia e implicaciones.

De tal forma, que el ciberespacio es entendido como un entorno intangible, constituido por redes informáticas que permiten la interacción de diversos usuarios con el propósito de compartir información; el ciberespacio es un entorno virtual, no es una página web en sí, por el contrario las páginas web se encuentran alojadas y hacen parte del ciberespacio.

Así mismo, (Stepp, 1993) define el ciberespacio como "el espacio de posibilidades informáticas interactivas, en el que los usuarios de ordenador[5] tienen acceso a los ordenadores de todos los demás y a sus contenidos".

De otra parte, la (Unión Internacional de Telecomunicaciones, 2007), argumenta que la actuación humana ha cambiado por las interacciones con entornos intangibles respecto a que "las tecnologías informáticas transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al permitir modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos".

Es por esto que el ciberespacio cobra bastante relevancia ya que es el medio donde la información transita e interactúa siendo accesible a un sinnúmero de redes y medios de comunicación, impulsando la productividad de todos los actores involucrados; estos actores que se pueden clasificar en gobierno, sector privado y ciudadanos, los dos últimos pueden subcategorizarse en grupos específicos que casi siempre tienen intereses económicos, políticos, religiosos o étnicos en la transaccionalidad de la información.

Si bien la interacción en el ciberespacio genera toda clase de efectos sobre la sociedad, desde el punto de vista económico y de seguridad, su impacto es notable, porque se tiene un

[5] Refiriéndose ordenador a un computador.

contacto inmediato a un costo muy bajo incidiendo en factores virtuales que cambian el curso del mundo real.

Frente a las implicaciones del uso del ciberespacio se plantean dos conceptos denominados: ciberdefensa y ciberseguridad. La ciberdefensa tiende a agrupar todas las acciones para la protección de la soberanía nacional, es en su mayoría requiere el uso de las fuerzas militares y de la inteligencia para contrarrestar las amenazas, entre tanto la ciberseguridad comprende las acciones en conjunto que realiza el estado y el sector privado para disminuir las amenazas que puedan presentar entidades o inclusive el ciudadano común (Cortés, 2015).

En el ambiente militar se presenta un teatro propicio para emplear el ciberespacio, pero su uso también representa diversas amenazas y riesgos, los cuales pueden variar desde perdidas de información, hasta planeación de ataques terroristas con base a la información recabada de las bases de datos del gobierno. Como sucedió en diciembre de 2015 en uno de los servidores del centro de meteorología de Australia, el cual también servía de plataforma para facilitar información a varios organismos nacionales, contando además con un enlace con las oficinas del departamento de defensa, lo cual causo fugas de información de seguridad nacional que le costó millones de euros a este país.

Por tal razón (Llongueras, 2013), establece en cuanto a la seguridad nacional de un Estado que "el ciberespacio es un elemento de poder dentro la seguridad nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias forjándose y desarrollándose el concepto de las operaciones militares centradas en redes".

En ese orden de ideas el ciberespacio debe ser utilizado como un instrumento de desarrollo tecnológico cuyo uso debe ser regulado dadas las implicaciones e influencia en el desencadenamiento de sucesos que generan gran impacto sobre las organizaciones, la información y la infraestructura critica, entendida como "aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas". Definición establecida por la Directiva europea: 2008/114/CE del 8 de diciembre de 2008.

Las Ciberamenazas

La digitalización de la información personal y laboral ha desencadenado grandes avances en productividad de cara a la automatización de procesos y aumento de eficiencia en las tareas, pero de esta misma forma cada día se hace más atractivo el botín de información disponible para quienes han profesionalizado su actividad en vulnerar la seguridad del tráfico de datos por el ciberespacio con fines lucrativos o ideológicos.

Si bien la tecnología de internet ha evolucionado para suplir la demanda actual también lo han hecho las amenazas a las cuales se enfrenta, tanto gusanos[6], como virus y otros códigos dañinos, pasaron de ser una molestia a ser un problema de seguridad grave y a convertirse en instrumentos de ciberespionaje. (Bejarano, 2013).

Llongueras (2013), propone que:

Con el nacimiento del ciberespacio se ha difuminado el concepto de gran potencia en lo referente al "status quo" internacional tradicional, puesto que Internet es barato y tiene

[6] Los Gusanos son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones.

> acceso hasta el país más pobre o cualquier persona del mundo, solo se necesita un ordenador y un hacker para poner en peligro la seguridad nacional de un país o causar graves accidentes y millones de víctimas (p. 49).

Con base a esta argumentación se entiende que todo tipo de vulnerabilidad virtual o real que provenga del ciberespacio es considerada una ciberamenza; dentro de las amenazas del ciberespacio más comunes se encuentran el espionaje industrial, ataques mercenarios, delincuencia contra servicios financieros, venta de información, fraude, extorsión, virus, ataques activistas y sabotaje, todos ellos enmarcados en ataques puntuales sobre los sistemas de información por descuido, desatención o inobservancia de la seguridad de los datos que se alojan en el ciberespacio (Entelgy, 2013).

Por lo tanto el término ciberamenaza es una palabra utilizada para referirse a un riesgo o posible peligro proveniente del ciberespacio. Esta amenaza también debe tomarse como un peligro latente, el cual no se ha desencadenado, pero permite tener las alertas encendidas en cuanto a que es posible que se convierta en un peligro real.

En la actualidad las amenazas a la información que se encuentran en el Ciberespacio han venido creciendo de manera exponencial, teniendo en cuenta que los sistemas de información cada día son más complejos y de fácil acceso a todo público, han generado que la empresa privada haya efectuado grandes inversiones para protegerse internamente de ataques a sus sistemas de información, específicamente los económicos. Muy pronto esta problemática pasa a evolucionar y a colocar en alto riesgo la seguridad informática de los estados convirtiéndose en ciberamenazas potenciales.

Tomando como marco referencial el documento (CONPES-3856, 2016), mediante el cual el gobierno nacional enfoca la política en materia de ciberseguridad y ciberdefensa. Se puede

identificar que se concentra en el análisis de las ciberamenazas y los objetivos para contrarrestarlas mediante un plan de acción, el cual tiene proyectado ejecutarse durante los años 2016 a 2019 con una inversión total de 85.070 millones de pesos donde estos recursos serán ejecutados por los Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

En esta política de implementación para la protección de amenazas al ciberespacio de Colombia, se evidencia la inexistencia de responsabilidades sobre las entidades del estado colombiano, afrontando el problema de manera independiente sin que exista un ente rector que efectué el control estratégico que permita formular capacidades efectivas con resultados óptimos a la protección de la información del país.

Por tanto la política de seguridad nacional se construye hoy desde una perspectiva multidimensional: militar, política, económica, social y medioambiental. Es decir, como equivalente a exención de peligro, daño o riesgo en todos estos ámbitos, y por lo tanto entendida como seguridad colectiva, compartida y global (Instituto Español de Estudios Estratégicos, 2010).

Algunos gobiernos han tomado las ciberamenazas como base para desarrollar políticas de protección contra los recursos del estado y su población, sin embargo, en la mayoría de las situaciones han generado o motivado que estos mismos al no existir un protocolo basado en un concepto de direccionamiento sean empleados de forma arbitraria en búsqueda de información que pueda contrarrestar los conflictos de cuarta generación que se están presentado a nivel mundial; es fundamental enfatizar que garantizar la protección del ciberespacio se requieren recursos económicos altísimos siendo estos utilizados con efectividad por las grandes potencias

como Estado Unidos, china Y Rusia que en la actualidad poseen recursos económicos suficientes para crear Ciberejercitos que protejan sus estados.

No obstante, se ha podido evidenciar la ausencia de un marco legislativo sobre seguridad en las redes en la mayoría de países, que en general permite de una parte el libre juego de empresas y consumidores, y de otra, una creciente intervención de los Gobiernos, que se proyecta sobre la gestión de los contenidos, la identificación, el filtrado y los sistemas de criptográficos siendo este engranaje una vulnerabilidad creciente a todos las naciones que tengan una conexión a internet (Cussac, 2011).

En la actualidad el crimen organizado cibernético tiene mayor capacidad para suplantar al personal en las entidades privadas y estatales, con el fin de conseguir información, requiriendo entonces unos lineamientos que permitan asumir credenciales legitimas a los usuarios para desarrollar capacidades en la administración del riesgo y amenazas cibernéticas las cuales se han visto evidenciadas en numerosos incidentes ocurridos en los últimos ocho años los cuales han tenido como resultado la transferencia de información, riquezas y los secretos nacionales mejor guardados, básicamente a manos anónimas y, lo más probable, maliciosas (Bejarano, 2013).

Tabla 1

Contexto internacional ciberseguridad y ciberdefensa

Países	Incidentes Presentados
Alemania	Recibió miles de intentos de espionaje comercial por parte de hackers chinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas. Constantemente recibe ataques por parte de hackers rusos a su red

	eléctrica y ferroviaria
Australia	En múltiples ocasiones, hackers norcoreanos y chinos han ingresado y bloqueado páginas web del Gobierno. En noviembre de 2008, el sitio del Primer Ministro fue desconectado completamente por dos días.
China	China se ha embarcado en una serie de asaltos informáticos a naciones occidentales como Corea del Sur, Alemania, Australia, Reino Unido y Estados Unidos
Corea del Norte	A pesar de haber sido acusada de numerosos asaltos informáticos, Corea del Norte no ha aceptado oficialmente que dichos asaltos provengan de organismos oficiales.
Corea del sur	Sus redes informáticas civiles y militares están bajo continuo ataque; se reporta que mensualmente sufren alrededor de 10.500 intentos de ingresos piratas y de 81.700 contagios con virus informáticos. En 2004, hackers chinos y norcoreanos robaron información ultrasecreta de sistemas de diferentes agencias gubernamentales
Estados Unidos	En enero de 2009, hackers robaron información ultrasecreta del Joint Strike Fighter ó F-35 (el proyecto de un sistema de armas más costoso en la historia de Estados Unidos). El 4 de julio de 2009, deshabilitaron las páginas web del Departamento del Tesoro y de Estado, de la Comisión Federal de Comercio, del Pentágono y de la Casa Blanca
Estonia	En 2007, sufrió el peor ataque cibernético ocurrido en la historia.

	Luego de un incidente diplomático, hackers rusos bloquearon los sistemas informáticos de las agencias gubernamentales. El país quedó completamente desconectado y sin servicios bancarios, de internet y de fluido eléctrico por varios días.
Francia	En enero de 2009, aviones de combate franceses no pudieron despegar de su portaviones al ser desactivado, por medio de un virus informático, su sistema electrónico.

Nota: Ministerio de Defensa Nacional

La tabla anterior muestra ejemplos de incidentes presentados en diferentes países, generando una perspectiva de los múltiples escenarios que puede tomar la guerra de Cuarta Generación en forma de ciberterrorismo, ciberataque y ciberespionaje los que finalmente son todos conceptos derivados de las ciberamenazas que vulneran según su foco la seguridad de la información del ciberespacio. Tabla No 1.

Hoy en día existen diferentes factores que acrecientan las ciberamenazas partiendo de la expansión de la capacidad técnica en cuanto que cada vez más agentes pueden acceder al ámbito cibernético, donde antes solo personas con conocimientos técnicos y altamente especializados tenían acceso, todo tipo de información está en contacto directo y/o transita por el ciberespacio y existe una creciente conectividad a Internet mediante múltiples canales, donde hasta los ataques menos sofisticados pueden causar daños significativos sobre cualquier red.

Según el (MINDEFENSA, 2009) existen dos factores incidentes en las ciberamenazas "los riesgos de un ataque cibernético a las redes interconectadas del país son cada vez más altos y la ciberdefensa y ciberseguridad son un tema estratégico para el país " en primera instancia, si se extiende el uso y la dependencia de tecnologías e infraestructuras ciberneticas, el nivel de

vulnerabilidad aumenta, así mismo si existe cualquier tipo de amenaza que afecte la infraestructura critica de una nación la ciberdefensa y la ciberseguridad son capacidades estratégicas prioritarias para desarrollar y fortalecer en todas las naciones.

De tal manera, que los sectores gubernamentales, administrativos y políticos de un país se deben centrar en establecer lineamientos políticos y organizativos que resguarden los sistemas de información y redes militares de ciberataques e incluir capacidades de reacción y respuesta, las cuales también se extienden a sistemas de información de terceros que puedan también resultar críticos para la nación.

La Ciberseguridad

Internet y cualquier tipo de comunicaciones y transferencia de datos se encuentran arraigados como parte del establecimiento y desarrollo de la sociedad moderna que permea tanto a organizaciones públicas como privadas. El uso de este tipo de datos permite una automatización de procesos desencadenando optimización de tiempos y de recursos e impulsando aún más el uso del ciberespacio como medio transaccional. Este nuevo esquema hace que la información se convierta en un activo sensible a riesgos, donde las amenazas son de naturaleza cibernética y se convierten en intangibles críticos para el funcionamiento de las organizaciones y de la sociedad en general, cuyo impacto genera afectación social, económica, política soberana y coercitiva del país.

De acuerdo con el documento (CONPES-3854, 2016) el concepto de ciberseguridad es "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".

El término Ciberseguridad fue adoptado en el año 2000 con la "limpieza" del error de software por el cambio del milenio (Klimburg, 2012). Este error fue ocasionado por la práctica de los programadores de abreviar un año de cuatro dígitos a dos dígitos, en vez de escribir en el software de la computadora el año 2.000, programaron solo los dos últimos dígitos 00 con el objetivo de economizar memoria; como consecuencia después del 31 de diciembre de 1999 sería el 1 de enero de 1900 en vez de 1 de enero de 2000, lo cual genero cientos millones de dólares gastados en planes de contingencias por gobiernos y empresas privadas.

En la actualidad el termino o concepto de Ciberseguridad es definido por muchas naciones atreves de sus documentos de estrategia nacional. A partir del 2012 con la publicación Nacional Cyber Security Framework Manual por la OTAN, más de 50 naciones han publicado algún tipo de una estrategia cibernética para definir lo que significa la seguridad para sus futuras iniciativas de seguridad nacional y económica (Klimburg, 2012). Colombia es una de ellas a través de su documento CONPES 3854 2016 elaborado por Consejo Nacional de Política Económica y Social.

Así mismo y específicamente en materia de seguridad nacional, la ciberseguridad se considera el desarrollo de estrategias que contrarresten el aumento de las amenazas informáticas que afectan una red, materializado en la capacidad del estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética (MINTIC, 2014).

Una forma de explicar dicho concepto es a través de la familiarización de otras concepciones sobre ciberseguridad seleccionados por países pertenecientes a la Organización

para la Cooperación Económica y el Desarrollo - *Organisation for Economic Co-operation and Development* (OECD):

- CIBERSEGURIDAD OTAN (Organización del Tratado del Atlántico Norte)

Define ciberseguridad como la capacidad de proteger adecuadamente la confidencialidad con integridad y disponibilidad de la CIS (Sistema de comunicaciones e información) y la información procesada, almacenada o transmitida (Klimburg, 2012).

- CIBERSEGURIDAD ISO (Information Security Standard)

La norma de la seguridad estándar de la información - *Information Security Standard* (ISO), define la seguridad cibernética como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio" (Klimburg, 2012).

- CIBERSEGURIDAD IUT (International Telecomunications Union)

La unidad Internacional de telecomunicaciones Unidad Internacional de Telecomunicaciones (UIT) define ciberseguridad como la colección de instrumentos, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, las mejores prácticas, la garantía y las tecnologías que se pueden utilizar para proteger el medio ambiente y la organización cibernética y los bienes de los usuarios (Klimburg, 2012).

- CONCEPTO CIBERSEGURIDAD-CANADA

Detectar, identificar y recuperar de los ataques cibernéticos, que "incluye el acceso involuntario o no autorizado, uso, manipulación, interrupción o destrucción (por vía electrónica) de información electrónica y la infraestructura física utilizada para procesar, comunicar y/o almacenar esa información. La gravedad del ataque cibernético determina el nivel apropiado de respuesta o medidas de mitigación" (Klimburg, 2012).

- CIBERSEGURIDAD-HOLANDA

La seguridad cibernética en Holanda ha definido en términos más generales la ciberseguridad, en el sentido de "libertad frente al peligro o daño debido a la interrupción, avería o mal uso de las Tecnologías de la Información (TIC). El peligro o daño resultante de la interrupción, avería o mal uso pueden consistir en limitaciones a la disponibilidad o fiabilidad de las TIC, quebrantamientos de la confidencialidad con la información almacenada en los medios de comunicación TIC, o daños a la integridad de ese información" (Klimburg, 2012).

- CONCEPTO CIBERSEGURIDAD-REINO UNIDO

Son las acciones tomadas para reducir el riesgo y asegurar los beneficios de un entorno digital de confianza para las empresas y los individuos (Klimburg, 2012).

- CONCEPTO CIBERSEGURIDAD-ESTADOS UNIDOS

Incluye la estrategia, la política y las normas en cuanto a la seguridad de las operaciones y en el ciberespacio, y abarca la completa gama de reducción de la amenaza, la reducción de la vulnerabilidad, la disuasión, la participación internacional, la respuesta a incidentes, capacidad de recuperación y las políticas y actividades de recuperación (Klimburg, 2012).

El tema común para todas las definiciones anteriores varía, sin embargo el punto predominante redunda en que la seguridad informática es fundamental tanto para la protección personal como para el resguardo de la información confidencial del gobierno, permitiendo a través de diferentes estrategias la protección de infraestructuras críticas que impulsan la economía global. La ligera diferenciación en la definición entre los gobiernos y las organizaciones intergubernamentales de es irrelevante, ya que su enfoque compartido sobre las cuestiones ilustra el primer paso en el largo camino para proveer seguridad cibernética sin importar la definición.

Considerando que la ciberseguridad es un tema de interés nacional e internacional que debe apoyarse en soluciones tecnológicas que ayudan a conseguir los objetivos de protección, dichas soluciones deben respaldarse en sistemas de gestión y estandarización de procesos y procedimientos adecuados; el modelo de gestión que contribuye a este ordenamiento es el sistema de gestión de seguridad de la información, recogido de la norma ISO 27032, en el que confían más de 24.000 organizaciones en todo el mundo.

La norma ISO 27032 sirve de guía para ayudar a las organizaciones a implantar sus sistemas de gestión de seguridad de la información, donde se establece el plan para la definición de políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware; una vez establecidos estos controles deben revisarse y mejorarse en forma constante para asegurarse que son efectivos. La norma se estructura en 14 secciones de seguridad, 35 objetivos de control que reflejan lo que se quiere conseguir y 114 controles de implementación.

En las instituciones del Estado no rige la norma ISO 27032 y pocas empresas privadas se encuentran certificadas o siguen sus lineamientos. Esto es una radiografía de la situación país en Colombia donde se evidencia un marco normativo nacional disperso en torno a la seguridad digital que comprende leyes, decretos y otros actos expedidos bajo condiciones diferentes a las actuales.

Si bien en Colombia se han empezado a plantear lineamientos nacionales de política en ciberseguridad en busca de una estrategia que minimice el aumento de amenazas informáticas; el estado colombiano aún carece de una visión estratégica basada en la gestión de riesgos y no cuenta con una instancia de coordinación nacional en seguridad digital que optimice la gestión de los recursos destinados a esta materia. Dicha ausencia no permite que el estado articule las funciones y actividades de la institucionalidad existente en torno a los objetivos nacionales en

seguridad digital. Situación que conduce a la duplicación de esfuerzos y a una menor eficiencia (CONPES 3854, 2016).

De igual manera, el documento CONPES 3854 emite lineamientos, responsabilidades y asigna recursos al Ministerio de Defensa Nacional, de cómo trabajar en temas de Ciberseguridad y Ciberdefensa, también implica al Gobierno Nacional en el compromiso de garantizar la seguridad de la información y le asigna responsabilidad directa frente a la protección de la infraestructura critica de la nación, ya que esta puede ser objeto de ataques, producto del empleo del ciberespacio. Un ataque cibernético a la infraestructura critica o estratégica puede afectar directamente los servicios esenciales de las personas, un ejemplo de ello puede ser el ataque cibernético al sector energético, que afectaría directamente el bienestar de la población.

De otra parte, la constitución política Colombiana en su artículo No 217 establece que las Fuerzas Militares deben estar en la capacidad de contrarrestar cualquier tipo de amenazas que pongan en riesgo la seguridad nacional y/o de los ciudadanos; considerando que una amenaza que emana del ciberespacio también clasifica dentro de este deber constitucional, es necesario el desarrollo de un concepto estratégico en ciberseguridad como resultado de la política y de los lineamientos estratégicos del Estado y el sector Defensa, que permitan tener una visión estratégica basada en la gestión de riesgos y enfocada en contrarrestar cualquier tipo de ciberataque.

La Ciberdefensa

El proceso de evolución, incremento y sofisticación de los ataques cibernéticos, establecen la necesidad de acoger medidas que permitan identificar, administrar y controlar el riesgo de las amenazas cibernéticas que aquejan tanto al Estado como a la ciudadanía. Según el (MINTIC, 2014) "El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países en los ámbitos tanto público como privado e incluyendo a la sociedad civil".

La ciberdefensa se cataloga como las actividades o procedimientos encaminados a prevenir y preservar la seguridad de los sistemas de información institucionales, organizacionales o personales y tomar medidas reactivas frente a ataques reales a dicha infraestructura (Llongueras, 2013).

El 26 de abril de 2007, el pequeño estado báltico de Estonia experimentó la primera ola de ataques de denegación de servicio (DoS); estos ataques dieron inicio a disturbios en las calles y pusieron en marcha la expulsión del gobierno de Estonia del monumento soldado de bronce en Tallin, monumento de guerra soviético erigido en 1947. Los ataques fueron dirigidos a los sitios web gubernamentales prominentes a lo largo de las páginas web de bancos, universidades, y periódicos estonios. Después de tres semanas, los ataques cesaron tan repentinamente como habían comenzado, pero no antes de que el gobierno de Estonia emprendiera medidas para bloquear todo el tráfico web internacional, cerrando efectivamente el "país más conectado en Europa" del resto del mundo. Lo anterior activó las alertas y marcó un hito en términos de ciberdefesa, ya que Estonia solicitó apoyo por primera vez a la Organización del Tratado Atlántico Norte por sus siglas (OTAN). No obstante, la alianza no disponía en ese entonces de un plan para este tipo de ataques y es así como este organismo internacional recomienda a todos sus

miembros implementar un conjunto de medidas orientadas a mejorar la protección ante los ciberataques. Acordando también desarrollar una Política de Ciberdefensa. (Caro, 2011)

En el año 2009 el Ministerio de Defensa Colombiano realizó un primer diagnóstico en cuanto a la ciberseguridad y ciberdefensa a partir de un estudio de incidentes presentados en diferentes países como Alemania, China, Estados Unidos, entre otros; mediante el cual llego a determinar aspectos cruciales para afrontar las amenazas provenientes del ciberespacio, entre ellas la necesidad de una estrategia nacional que incluyera diferentes ámbitos como sistemas seguros y resistente, doctrina y normatividad, sensibilización y cambio cultural, roles y misiones, compromiso internacional, educación y capacidades de investigación y desarrollo y por ultimo infraestructura y equipamiento (MINDEFENSA, 2009).

Considerando que la ciberdefensa y la ciberseguridad se convierten en un asunto estratégico para el estado, ante la aparición de nuevas amenazas tanto regulares como irregulares que tienen la capacidad de afectar la seguridad nacional de cualquier estado, llevan a los gobiernos y a sus Fuerzas Militares a considerar estos dos ambientes como ambientes estratégicos a fortalecer en los próximos años. (Ministerio de Defensa Nacional de Colombia, 2009). A partir de allí el Estado colombiano ha implementado una serie de estrategias como incluir nuevos tipos penales como delitos informáticos hasta la consolidación de una política pública plasmada en el CONPES 3701 "Lineamientos de política para ciberseguridad y ciberdefensa". (Conpes, 2011)

La adopción de una Política Nacional de ciberseguridad y ciberdefensa que involucre a todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa Nacional y en coordinación con las demás entidades del Estado, es un imperativo al que debe darse la mayor de las prioridades. (DNP, 2011). Como conclusiones de las actividades realizadas, las instituciones

del Estado solicitaron al Ministerio de Defensa Nacional asumir un liderazgo nacional que permitiera impulsar políticas en seguridad cibernética, así como crear mecanismos que pudieran dar respuesta a los incidentes y delitos cibernéticos que afectaran a la nación. (DNP, 2011)

Desarrollar todos los tópicos relacionados con ciberseguridad y ciberdefensa conlleva una responsabilidad del Gobierno Nacional para garantizar la seguridad de la información. Así que, si bien este documento busca sentar las bases de política para los temas relacionados con estos conceptos, los organismos del estado responsable deberán desarrollar las bases y generar mecanismos para garantizar la seguridad de la información a nivel nacional. Para lo anterior, el concepto resultante deberá tener en cuenta las normas y los estándares establecidos a nivel nacional e internacional, así como las propuestas internacionales sobre protección de infraestructura crítica. (DNP, 2011) El principal logro alcanzado por la política de ciberseguridad y ciberdefensa, fue el fortalecimiento de la institucionalidad en el tema.

Lo anterior, fue posible por medio de la creación de nuevas instancias tales como el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana. (DNP, 2016). La implementación inicial del colCERT, el CCP y el

CCOC en el Ministerio de Defensa Nacional, implicó la asignación de los siguientes recursos por parte del Ministerio:

2011 $ 1.428.444.328

2012 $ 5.400.000.000

2013 $ 5.000.000.000

2014 $ 4.600.000.000 (DNP, 2011)

Sin embargo en el documento CONPES 3701 de 2011 estableció un primer concepto de Ciberdefensa el cual se enunciaba como la "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" (DNP, 2011). Más adelante en el documento CONPES 3854 de 2016 se realiza una actualización a la definición concibiéndola como: el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales (DNP, 2016).

Por esta misma línea la Information Systems Security Association (ISSA) en Chile, estableció una serie de parámetros que permiten darle viabilidad al concepto estratégico y pueden ser extrapolables en su implementación práctica en Colombia (Anabalón R. Juan, Ramírez S. Manuel, 2016).

Desarrollar y mantener listas fuerzas y capacidades para llevar a cabo operaciones de ciberespacio

Defender la red de información de defensa, asegurar los datos y mitigar los riesgos para la misión del ministerio de defensa y sus ramas operativas.

Estar preparado para defender el territorio y los intereses vitales de ciberataques perjudiciales o destructivos de consecuencia significativa.

Desarrollar y mantener opciones cibernéticas viables y planear el uso de esas opciones para controlar la escalada del conflicto y dar forma a la situación de conflicto en todas las capacidades.

Construir y mantener sólidas alianzas internacionales y asociaciones para disuadir las amenazas compartidas y aumentar la estabilidad y la seguridad internacionales.

Si bien existen según su intensidad diferentes clases de ciberataques, siendo el ataque de alta intensidad aquel con gran visibilidad que tiene como objetivo equipamientos militares o infraestructuras críticas que traería como respuesta una acción bélica por parte de la parte perpetrada y el ataque de baja intensidad que es el más común, puesto que establece delitos electrónicos con fines económicos (Llangueras, 2013). Frente a los anteriores conceptos y lineamientos está claro que si bien el estado tienen el deber de identificar y minimizar las amenazas que provienen del ciberespacio, la ciberdefensa no es solo responsabilidad del Estado, los ciudadanos usuarios de internet, son responsables de la información que extraen e insertan en los sistemas a través de las redes. La educación cibernética debe concientizar a todo el personal que hace parte de una compañía, ya sea pública o privada, desde el nivel ejecutivo hasta el nuevo empleado; Ya que cualquier interacción aparentemente inocua puede crear un puente de acceso a información sensible que puede incluso acarrear problemas públicos y de seguridad nacional.

El Estado colombiano se ha venido preparando los últimos años para enfrentar la amenaza cibernética y desarrollar y consolidar las capacidades necesarias que contrarestren y

mitiguen el riesgos de forma tal que el Ministerio de Relaciones Exteriores creó un grupo interagencial de trabajo para analizar, administrar, gestionar y controlar todos los temas concernientes al ciberespacio. Mediante esta iniciativa fue posible que el Ministerio de Tecnologias de la Informacion y Telecomunicaciones, identificara las brechas y los vacíos que tiene la Nación en materia de Seguridad Informática. A partir de todo este trabajo la Cancillería involucro al Ministerio de Defensa para que liderara los temas de Ciberseguridad y Ciberdefensa. Como resultado fue creado en el año 2009, el colCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia), cuya función principal según (MINDEFENSA, 2009) es "coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano, frente a emergencias de cibernéticas que atenten o comprometan la Seguridad y Defensa Nacional".

De cara a cumplir con estos objetivos se establecieron tres líneas principales de acción donde el Ministerio del Interior y de Justicia se encarga de la adecuación y adopción de las medidas legislativas y judiciales para la ciberseguridad; el Ministerio de Relaciones Exteriores se encarga del seguimiento a tendencias internacionales e implementación de acuerdos asumidos por el Estado y Ministerio de Defensa se encarga de implementar las medidas para la seguridad y defensa del Estado Colombiano (MINDEFENSA, 2009).

Estado actual de la fuerza aérea en el control del ciberespacio

El Estado Colombiano se ha venido preparando para enfrentar la amenaza cibernética a través de la creación de grupos interagenciales de trabajo para analizar y profundizar en los temas concernientes al ciberespacio, se establece que tanto actores públicos como privados cuentan con capacidad instalada para hacer frente a esta problemática, pero el liderazgo de la operaciones viene dado según el colCeRT por el cual el Ministerio de Defensa Nacional, el cual

delego a cada una de sus Fuerzas tareas para el establecimiento del control del ciberespacio desde su misión constitucional.

Por lo tanto, la caracterización del estado actual de Colombia en el control del ciberespacio se realizó de cara a la gestión que realiza la Fuerza Aérea Colombiana, considerando que es una fuente medible y aprovechando el acercamiento que se puede tener a este tipo de información de carácter reservado al ser todos los autores del documento pertenecientes a esta Fuerza.

Mediante el análisis de la información se logró establecer que la unidad cibernética de la Fuerza Aérea Colombiana nace en el año 2012 regida inicialmente bajo el documento CONPES 3701; con apoyo de personal de JAL, JIN y JOA se crean la subdirección de ciberdefensa, ciberinteligencia, cibercontrainteligencia y operaciones ofensivas (ciberguerra). Se encuentra bajo la dirección del Comando Conjunto Cibernético, donde cada una de las Fuerzas Militares de Colombia crea su propia unidad para administrar su propia estrategia de ciberseguridad y ciberdefensa, buscando mitigar las amenazas contra las infraestructuras críticas, inteligencia y contraintelegencia; cuenta con subdirecciones encargadas de ciberdefensa, ciberinteligencia, cibercontrainteligencia y operaciones defensivas.

Su misión principal es desarrollar capacidades enfocadas en 2 objetivos específicos, la protección de la infraestructura critica de la Fuerza Aérea y la inteligencia y contrainteligencia en el ciberespacio. Organizacionalmente la unidad se encuentra cuenta conformada por un grupo de oficiales y suboficiales altamente entrenados que dan cumplimiento a las directrices del comando general, capacitados y manejando una plataforma tecnológica adecuada.

Actualmente se enmarca bajo el documento CONPES 3854 y cuenta con un documento de Desarrollo de Operaciones Cibernéticas el cual funciona como un manual de doctrina para

realizar operaciones en el ciberespacio. Se basa en los siguientes documentos rectores, los cuales delinearon la ruta para crear la misión, la visión y todo el soporte documental y de gestión de la Unidad:

- Documento marco que asigna los roles de cada fuerza No. 101/ CGFM/DP/2014 sobre LINEAMIENTOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA LAS FUERZAS MILITARES DE COLOMBIA
- DIRECTIVA No.23 /MDN/2014 sobre LINEAMIENTOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA LAS FUERZAS MILITARES DE COLOMBIA
- DIRECTIVA No. 20 DEL 2014 sobre POLITICAS DE SEGURIDAD DE LA INFORMACION DEL SECTOR DEFENSA
- OFICIO ORFEO 2012-63361 sobre CREACION DE UNIDADES DE CIBERDEFENSA A NIVEL FUERZA

Desde la perspectiva del análisis cibernético se realiza una prospectiva y análisis de blanco mediante los lineamientos adquiridos en el año 2014 cuando se realizó un offset mediante Bell Helicopter para el desarrollo e implementación de la unidad, la cual trabaja según una hoja de Ruta entregada por Estonia y a través de un laboratorio para el entrenamiento en Ciberdefensa.

Actualmente se encuentran en el desarrollo de un centro operaciones de ciberseguridad y ciberdefensa a través de un datacenter existente, para identificar y gestionar la seguridad informática de la institución. El objetivo es contar con operadores y supervisores permitiendo desarrollar todo tipo de operaciones. Si bien actualmente la Fuerza Aérea Colombiana no busca liderazgo en este ámbito, dentro de sus lineamientos se encuentra la necesidad de estar preparada para la protección de infraestructuras críticas sin importar de qué flanco provenga la amenaza.

Adicionalmente parte del personal se encuentra recibiendo capacitación en Tallin capital de Estonia, con el fin de identificar los posibles accesos ilegales a la red. Donde también han realizado maestrías una serie de integrantes de la institución, permitiendo tener personal capacitado de los centros mejor calificados a nivel mundial en este tipo de actividades

Así mismo es preciso indicar que dentro de las capacidades del centro de operaciones se encuentran desde la identificación de computadores que estén accediendo desde cualquier lugar la red de la Fuerza Aérea hasta la capacidad la protección de la infraestructura critica aeronáutica mediante el desarrollo de un modelo de trabajo en profundidad tipo cebolla, donde cada capa establece una barrera para el posible ingreso a la red.

La unidad se encuentra trabajando en una propuesta encaminada en realizar un plan de carrera que le permita a una serie de integrantes de la institución recibir una capacitación y preparación que les permita asumir los cargos derivados de esta especialidad. Por lo tanto no solo es importante desarrollar este plan de carrera dentro de la Fuerza Aérea Colombiana, también es de vital importancia asignar los recursos necesarios para poder sostener estos sistemas, aunque con la base instalada actual se están realizando progresos importantes.

Si bien la unidad cibernética de la Fuerza Aérea Colombiana se encuentra trabajando en el establecimiento de una hoja de ruta en ciberdefensa para el futuro, el desarrollo de laboratorios de investigación y entrenamiento y se están realizando capacitaciones. En la actualidad es un soporte sostenible dentro de las requerimientos que se presentan, pero para lograr su sostenibilidad en necesario realizar una serie de convenios como prestación de servicios que pueden ayudar a monitorear diferentes redes y entidades como la Aeronáutica Civil, la banca y las empresas privadas, donde sea posible identificar todo tipo de vulnerabilidades provenientes del ciberespacio que afecten la estabilidad nacional.

Conclusiones

Mediante el análisis documental, se evidencio la ausencia de un marco legislativo sobre seguridad en las redes de la mayoría de países, lo cual ha desencadenado problemas en la gestión de contenidos, identificación y filtrado de información, requiriendo medidas de forma y fondo con el propósito de disminuir la vulnerabilidad creciente a todos las naciones que tengan una conexión a internet.

Se hace necesario que los sectores gubernamentales, administrativos y políticos de Colombia generen de manera sistemática lineamientos políticos y organizativos que resguarden los sistemas de información y redes militares de ciberataques, garantizando una capacidad de reacción y respuesta ante cualquier amenaza proveniente del ciberespacio.

Se evidencio que el Estado colombiano tiene la capacidad de responder a amenazas provenientes de ataques cibernéticos o ataques a infraestructura critica mediante el soporte de los grupos interagenciales, pero los elementos que componen la seguridad del ciberespacio se encuentran disgregados y no se integran, por lo tanto se desarrolló un concepto estratégico que permitió alinear todos los criterios, políticas y normatividades, que existen alrededor del ciberespacio.

Es de vital importancia que el presente postulado se establezca como una base de conocimiento para que a futuro pueda ser desarrollado como un proyecto de ley o una política del Estado frente al curso de acción del Estado frente a las amenazas que surgen del ciberespacio.

Por consiguiente y conscientes de la importancia que tiene para el Estado la seguridad nacional, se debe crear una ley de cicberseguridad que se construya con una perspectiva

multidimensional: militar, política, económica, social y medioambiental, donde se busca la exención de peligro, daño o riesgo en todos estos ámbitos; las ciberamenazas de cara a la seguridad nacional representan la base de desarrollo de políticas de protección contra los recursos del estado y su población, con el fin de garantizar la protección del ciberespacio.

Frente al control del ciberespacio es importante que plantear que el presente concepto estratégico incorpora los elementos claves sobre ciberseguridad y ciberdefensa que deben enmarcar el control del ciberespacio por parte del Estado Colombiano. Este concepto apunta a ser un lineamiento de orden superior que permanezca en el tiempo, pero a su vez puede ser actualizado periódicamente dependiendo del contexto político-estratégico de la Nación. Si bien este concepto estratégico no constituye una argumentación detallada sobre una estrategia militar, si es un marco de referencia general para todas las tareas de control público y privado sobre el ciberespacio.

Por tanto, el espectro de actividades de control del ciberespacio, se deben fundamentar en la integración de las capacidades de las fuerzas para minimizar las amenazas en torno a las condiciones de seguridad que se requieran, aplicando principios de identificación, mitigación y control, en conjunto y mediante comunicación clara y precisa entre cada una de las unidades cibernéticas; concepto por el Estado Colombiano deben enfrentar un escenario multidimensional de seguridad nacional y estrategias de guerra de cuarta generación.

Basados en el constante análisis de las redes de información y el fortalecimiento de la capacidad instalada de profesionales de seguridad informática, ejerciendo soberanía en el ciberespacio, anticipándose a la ocurrencia de situaciones que afectan la ciberseguridad del estado y/o reaccionando con tácticas de ciberdefensa según el tamaño de la amenaza. Todo esto apoyados en la estandarización de los procedimientos y en la voluntad de los comandantes para

compartir información con celeridad y precisión, y brindando los recursos puntuales que se requieran.

Este enfoque requiere de un liderazgo transformador que permee todas las instancias, con el fin de impulsar cambios, replicando el modelo en todos los niveles de la Fuerzas Militares; empleando con agilidad las capacidades distintivas de cada Fuerza, respetando sus roles y misiones particulares.

Referencias Bibliográficas

Alexander Klimburg. (2012), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012 PAG 12 Cyber Terms AND Definitios.

Acosta, O. Pérez, J. Arnáiz, D. & Taboso, P. (2009). Seguridad Nacional y Ciberdefensa. Madrid (Esp.). Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Anabalón R. Juan, Ramírez S. Manuel, T. E. A. (2016). Propuestas de ISSA Chile a la Política Nacional de Ciberseguridad (PNCS) 2016-2022.

AUSTRALIAN GOVERMENT-DEPARTMENT OF DEFENCE. (2009). Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper. CBS NEWS. (2009). Gates: Cyber Attacks A Constant Threat

Bus, J. (2011) Dependencia y confianza social. Para Unión Internacional de Telecomunicaciones (2011). La búsqueda de la paz en el ciberespacio. Ginebra. ITU.

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

Caro, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Caro, M. J. (2011). DOCUMENTO INFORMATIVO DEL IEEE 09/2011 NUEVO CONCEPTO DE CIBERDEFENSA DE LA OTAN.

Cussac, J. L. G. (2011). Estrategias legales frente a las ciberamenazas. Cuadernos de estrategia, (149), 83-127.

Canadian Department for Public Safety (2010), Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.

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

Constitución Política de Colombia. (1991). Artículo 126. Bogotá. República de Colombia. http://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-v/capitulo-2

Constitución Política de Colombia. (1991). Artículo 127. Bogotá. República de Colombia. http://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-v/capitulo-2

COUNCIL ON FOREIGN RELATIONS. (2008). The Evolution of Cyber Warfare.

CRS REPORT FOR CONGRESS (2001). Cyberwarfare

Del Río Durán, J. D. (2011). La ciberseguridad en el ámbito militar. Cuadernos de estrategia, (149), 215-256.

DNP. (2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa - Conpes 3701.

DNP. (2016). Política Nacional de Seguridad Digital - Conpes 3854.

DOCUMENT Cyber security Strategy (2009). Australian Prime Minister, The First National Security Statement to the Australian Parliament.

Entelgy. (2013). Las diez ciberamenazas mas comunes.

Gibson, W. (1984). Neuromante. Clasicos Minotauro.

GOETZ,J; ROSENBACH, M; SZANDAR, A. (2009). National Defense in Cyberspace. Spiegiel International

Gómez Azuero, J. P. (2015). Ciberdefensa y ciberseguridad: una nueva prioridad para las naciones.

IA NEWSLETTER (2009). Army, Navy, Air Force, and Cyber – Is it time for a Cyberwarfare

Branch of Military. Vol. 12 No. 1.

Instituto Español de Estudios Estratégicos (2010). Ciberseguridad. Retos y Amenzas a la Seguridad Nacional en el Ciberespacio.

ISO/IEC 27032 (2012), Tecnología en la información, técnicas de seguridad – Guidelines for cybersecurity. PAG 12 Cyber Terms AND Definitios.

Joyanes, L. (2011) Introducción. Estado del arte de la ciberseguridad. Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Llongueras, A. (2013). La guerra inexistente, la ciberguerra.

Mª José Caro Bejarano (2013) LA NUEVA DIMENSIÓN DE LA AMENAZA GLOBAL: LA AMENAZA CIBERNÉTICA

Marenco, K. (2015). Direccionamiento Estrategico.

Ministerio de Defensa Nacional de Colombia. (2009). Ciberseguridad y Ciberdefensa: Una primera aproximación.

Molas, J. (2007) Políticas de I+D de Defensa de varios países europeos y de EE.UU. En Relaciones entre las innovaciones tecnológicas y la Defensa. Madrid (Esp.) Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

Observatorio, Ciberseguridad. (2016). Ciberseguridad. Estamos preparados en América Latina y el Caribe.

Organización del Tratado del Atlántico Norte. (2010). Concepto estratégico de la OTAN

Pastor, O. Pérez, J. Arnaíz, D. & Taboso, P. (2009). Seguridad Nacional y ciberdefensa. Madrid (Esp.). Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

PILKINGTON, E. (2008). China winning cyber war, Congress warned. The Guardian: Londres. Disponible en: http://www.guardian.co.uk/technology/2008/nov/20/china-usmilitary-hacking

Shane, Harris. (2010). THE WATCHERS y @WAR: The Rise of the Military-Internet Complex.

Stepp, Ermel. (1993). The virtualisation of institutes of research. Electronic journal of virtual culture, v. 1, nº 6.

UNAD. (2006). Lección 6: Investigación Exploratoria, Descriptiva, Correlacional y Explicativa. Bogotá: Autor. http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin__exploratoria_descriptiva_correlacional_y_explicativa.html

Unión Internacional de Telecomunicaciones ITU (2007) Guía de Ciberseguridad para los países en Desarrollo. Tomado de www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007- MSW-S.doc

UK OFFICE OF CYBER SECURITY. (2009). Cyber Security Strategy of the United Kingdom.

Vargas Pulido, W. (2014). Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la seguridad nacional?.