UNIVERSIDAD MILITAR
NUEVA GRANADA

¿Cómo minimizar el riesgo de afectación de un ataque cibernético en los blancos estratégicos nacionales?

Trabajo final para obtener el título de Especialista en Alta Gerencia

Presentado por:

Benjamín Montoya Gaitán

Presentado a:

Dr. Ricardo Rubianogroot Román

Universidad Militar Nueva Granada

Especialización en Alta Gerencia

Noviembre de 2016.

Resumen

En el presente documento se relaciona como alternativa de solución, ante las continuas y cada vez más crecientes amenazas en el ciberespacio, la formulación estratégica nacional de Ciberseguridad y Ciberdefensa (en adelante Ce y Cd) para Colombia, cuyo objetivo es establecer unos principios generales, líneas de acción y la hoja de ruta de la Cs y Cd 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 SD del Estado.

Palabras clave: Amenaza, Blanco Estratégico, Ciberdefensa, Ciberespacio, Ciberguerra, Infraestructuras Críticas.

Abstract

This document is presented as an alternative solution to the ongoing and increasingly growing threats in cyberspace, the National Strategy formulation of cyber security and defense departs Colombia , which will establish general principles, lines of action and roadmap cybersecurity and national cyberdefense, which reflects the strong commitment, collaborative work, cooperation, coordination and harmonization of all those responsible and resources for the protection and defense of cyberspace, in order to ensure the prevention, detection, response, neutralization and containment intentions or potential, imminent and actual hostile actions originating in or through cyberspace and affecting the security and defense of the state.

Keywords: Strategic target, cyberspace, cyberwar, cyberdefense, critical Infrastructure, Threat**.**

TABLA DE CONTENIDO

Listado de Siglas o Acrónimos

CCOC	Comando Conjunto Cibernético
CCNA	Cisco Certified Network Associate
Ce	Ciberespacio
Cd	Ciberdefensa
Cg	Ciberguera
Cs	Ciberseguridad
CONPES	Consejo Nacional de Política Económica y Social
ENCC	Estrategia Nacional de Ciberseguridad y Ciberdefensa
ONU	Organización de las Naciones Unidas
OTAN	Organización Del Tratado Del Atlántico Norte
SD	Seguridad y defensa
SDN	Seguridad y defensa nacional
TIC	Tecnologías de la información y Comunicaciones

Definiciones

Los siguientes son los términos técnicos empleados a lo largo del ensayo con su respectiva definición, conforme al uso que se le dará en el marco del trabajo:

Ciberespacio: Se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir. La información se puede intercambiar en tiempo real o en tiempo diferido, y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar.

Ciberdefensa: Como esa nueva connotación sistémica y sistemática que deben desarrollar los gobiernos, para comprender ahora sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la comprensión de variables como, las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo online; la renovación de la administración de justicia en el entorno digital; y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

Ciberguerra: Ciberguerra se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, para producir alteraciones en datos y sistemas del enemigo, a la vez que se protege la información y sistemas del atacante. Para llevar a cabo estas actividades, se conocen distintos métodos para vulnerar la estructura informática del objetivo. Desde la inteligencia social hasta la aplicación de procedimientos requerientes de conocimiento técnico avanzado.

Ciberseguridad: Como realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital, en un conjunto de variables claves, acertadamente definidas por la ITU -International Telecommunication Union-, en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de una realidad digital y de información instantánea.

Ciberespionaje. Es muy normal que después de hacerse con la información la manipule, la borra o la destruye, etc. Así, dentro del ciberespionaje se puede incluir las siguientes acciones como, por ejemplo, reconocer los sistemas (obtener información previa sobre las organizaciones y sus sistemas informáticos, para poder escanear sus puertos con el objetivo de determinar qué servicios se encuentran activos, etc), detectar las vulnerabilidades de los sistemas (detectar las posibles vulnerabilidades de un sistema informático, para después desarrollar alguna herramienta que permita explotarlas fácilmente, como el "exploits"), robar información mediante la interceptación de mensajes, modificar el contenido y la secuencia de los mensajes transmitidos, analizar el tráfico (observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers" o "switches", ataques de suplantación de la identidad IP Soofing, capturar contraseñas y cuentas de usuarios, conectarse de forma no autorizada a equipos.

Fuentes de información: Son todos los recursos que poseen datos dispuestos en un medio, ya sea manuscrito, impreso o electrónico y elaborados con el propósito de comunicar esos mismos datos.

Seguridad digital: Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado

mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Introducción

La convergencia de las comunicaciones y la dinámica tecnológica están revolucionado al mundo trayendo consigo un sin número de beneficios, pero también de amenazas a las que están expuestos los ciudadanos, la industria y el gobierno. Por su impacto, tal fenómeno ha ocasionado que se consolide como uno de los mayores retos a solucionar para mantener en niveles controlados la seguridad nacional.

La dependencia del uso del Ce en todas y cada una de las actividades cotidianas, de la sociedad y del Estado, obliga a los diferentes países, y sin duda alguna a Colombia, a poner especial atención para conocer sus ciberamenazas y gestionar sus riesgos a fin de buscar las medidas y capacidades que ayuden a su protección y defensa adecuada.

El desarrollo de los sistemas de las tecnologías de la información y las comunicaciones (en adelante TIC), el fomento de su uso, su fácil acceso y la proliferación de nuevos servicios en el ciberespacio, han contribuido significativamente al crecimiento exponencial del Internet en nuestro país. Además, es importante reconocer que estos factores vienen forjando el crecimiento de las actividades económicas y sociales de Colombia, tanto de forma directa como indirecta. Es un hecho que las TIC soportan un proceso creciente de integración en los mercados globales, que aceleran la innovación y la gestión en las empresas, crean riqueza y, en definitiva, generan desarrollo y bienestar.

En nuestro país, es cada vez mayor la dependencia que se tiene del complejo sistema de infraestructuras tecnológicas que dan soporte y posibilitan el normal

desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras tecnológicas suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población para amenazar la seguridad nacional, causar muertes masivas, debilitar la economía, y dañar la confianza y la moral de los ciudadanos en o a través del ciberespacio.

Para que Colombia haga un uso adecuado de las TIC, se hace necesario garantizar un liderazgo nacional y la coordinación de esfuerzos: la presencia del Estado y de la sociedad en los nuevos escenarios de comunicación, la protección de los derechos en el ciberespacio, así como definir responsabilidades y garantizar la cooperación en el Ciberespacio tanto a nivel nacional como internacional.

1. Contexto y Antecedentes

Desde el año 2007, El Ministerio de Defensa Nacional con el Comando General de las Fuerzas Militares con su unidad el Comando Conjunto Cibernético (CCOC), la Policía Nacional con el Centro Cibernético Policial, en Colombia vienen trabajando en temas relacionados con Cs y Cd, como el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones; así como socializando la importancia de contar con una estrategia de Cs y Cd Nacional que permita articular y armonizar los esfuerzos aislados que han adelantado tanto el gobierno como los sectores públicos y privados.

En el año 2011, mediante el documento CONPES 3701, "Lineamientos de Política para Ciberseguridad y Ciberdefensa", Colombia emitió unas directrices y lineamientos generales que permitieron fortalecer tres ejes estratégicos que fueron abordados de manera transversal durante un periodo de tiempo establecido, así:

- Se estableció la importancia de crear instituciones responsables de la Cs y Cd.

- En segundo lugar, se emitieron algunas metas relacionadas con la capacitación, con el fin de fortalecer la oferta y cobertura de capacitación especializada en Cs y Cd, enfocándola desde diferentes contextos como los niños, jóvenes, trabajadores oficiales, privados, sector defensa y sector justicia, entre otros.

- La tercera línea fue el marco normativo y legal, es decir fortalecer las leyes en Colombia, con nueva legislación y regulación en el ámbito de los ataques cibernéticos y delitos informáticos.

El documento CONPES 3701 permitió a Colombia dar inicio a importantes actividades y coordinaciones entre el gobierno y los sectores público y privado, así como avanzar en la cultura de la seguridad de la información; sin embargo, las actividades previstas en dicho documento finalizaron el 31 de diciembre de 2014. Es por lo que se hace necesario dar continuidad a esta política a través de varios mecanismos, entre ellos la Estrategia Nacional de Ciberseguridad y Ciberdefensa (en adelante ENCC).

Con este documento, Colombia dio inicio al desarrollo de capacidades en materia de seguridad y defensa (en adelante SD) de sectores y blancos estratégicos nacionales susceptibles de un ataque cibernético en Colombia.

Es un sector estratégico, toda vez que tiene la capacidad de influir positiva o negativamente en la seguridad de un país, entendido éste como el conjunto de instituciones que comprenden al Estado y la nación, por lo tanto, con el propósito de delimitar el alcance de este análisis, en términos conceptuales y con base en la estructura teórica del Neorrealismo, se adoptará una definición restrictiva de seguridad, que tiene relación con la supervivencia del Estado. Es prudente advertir que un ataque cibernético a un sector o blanco estratégico de un país, podría ser devastador para su componente económico, social, político e incluso para la Seguridad y Defensa Nacional (en adelante SDN), teniendo en cuenta la influencia y el impacto que estos pueden llegar a ejercer en la plena gobernabilidad de la nación.

Sin embargo, a pesar de las capacidades y grandes logros obtenidos con el desarrollo del documento CONPES 3701, los esfuerzos de Colombia para abordar la Cs y Cd están

limitados por falta de una política nacional que dé una visión general estratégica para el país, y establezca responsabilidades, autoridad y recursos para actuar en el ciberespacio.

En consecuencia, la pregunta de investigación que orientara este trabajo es: ¿Cómo lograr que Colombia implemente las medidas necesarias para lograr prevenir, neutralizar y responder a los ataques a la infraestructura critica cibernética, a fin de preservar la SDN frente a las amenazas y riesgos de seguridad que se producen en el ciberespacio?

2. Apreciación estratégica

Se considera fundamental realizar una comprensión y análisis general de la amenaza cibernética y de la evolución de sus tendencias, como punto de partida para trazar las líneas de acción de la ENCC que requiere el país para afrontar los nuevos desafíos que impone ésta, entendiendo que siempre está implícita en los sistemas de tecnologías de la información y de las comunicaciones, avanzando al mismo ritmo de su evolución y su desarrollo.

En el nuevo contexto mundial, los países, especialmente los más desarrollados, han contemplado la amenaza cibernética como una de las de más alta prioridad, gracias a las características propias del ciberespacio que propician clandestinidad, anonimato, fácil acceso, poco o ningún control gubernamental, rápido flujo de información, bajos costos, bajos riesgos y alto impacto de destrucción, disrupción, mal funcionamiento o toma de control de sistemas tecnológicos, también por la rentabilidad en términos económicos y políticos por parte de personas, industrias y Estados, constituyendo la amenaza cibernética en una preocupación presente y futura para los estados, más aún, cuando la dependencia tecnológica es una realidad inevitable, con la cual necesariamente tendrán que convivir la sociedad, y sobre la que se soporta cada vez más la actividad económica y social de los países.

La amenaza cibernética puede ser definida como una potencial violación de las propiedades de la información en lo que respecta a su confidencialidad, integridad y disponibilidad. Para entender la amenaza es fundamental conocer quiénes están detrás de ésta y cuáles son los motivadores que los impulsa a realizar acciones ilegales en o a través

del ciberespacio. En relación a los actores, son los que ejecutan las acciones y las fuentes de información son los que están detrás de estas acciones que se describen más adelante.

Las amenazas pueden ser diferenciadas de acuerdo a sus características, impacto, origen y actores, así estas pueden ser, accidentales o intencionales. Las amenazas accidentales son las que ocurren sin una intención premeditada y las amenazas intencionales son las que resultan de actos deliberados en contra de la seguridad de un activo. Estas últimas pueden ir desde un simple escaneo de redes usando herramientas disponibles de fácil uso, hasta el hecho de cometer ataques sofisticados usando el conocimiento de sistemas especializados. Las amenazas también pueden ser activas o pasivas, activas cuando dan como resultado el cambio en la operación de un sistema, ya sea por la modificación de datos y la destrucción de equipos físicos; en tanto que, la amenaza pasiva no involucra cambios en los sistemas y cuyo propósito es obtener información de los sistemas sin afectar los recursos.

La amenaza vista desde un enfoque general de las causas potenciales de daño y sus riesgos asociados, considera el ciberespacio como una fuente inagotable de amenazas emergentes, cada vez más variadas, con consecuencias que pueden escalar al orden más alto y se evidencia con el creciente número y efectividad de los usuarios públicos y privados que lo usan para realizar todo tipo de actividad ilegal en beneficio propio, de terceros e inclusive de Estados-Nación; por lo tanto, los sistemas (TIC) y las Infraestructuras Críticas se ven amenazadas por un nuevo tipo de guerra, la de la información y en ese sentido el ciberespacio debe ser considerado un nuevo dominio de

guerra, que ha alertado a los Estados del mundo para prepararse a afrontar este nuevo tipo de amenaza.

Adicionalmente, no existe una normatividad adecuada para la operación segura de los sistemas TIC en el ciberespacio, lo que propone un riesgo adicional, ya que existen Estados que no están interesados por el momento en la regulación; por lo tanto, es aprovechado por los diferentes actores para lanzar sus ataques desde o a través de esos países que al momento de obtener cooperación y colaboración es simplemente imposible; porque no hay obligaciones, responsabilidades y peor aún, ni voluntades para contribuir a contrarrestar este tipo de amenaza transnacional.

Por lo anterior, es importante analizar como una alternativa viable para Colombia, el desarrollar e implementar una ENCC con una visión integradora, y con un enfoque global, que soporte los objetivos de más alto nivel del Gobierno y que integre un conjunto de acciones planificadas sistemáticamente a corto, mediano y largo plazo; evaluadas desde diferentes ámbitos de actuación como la conveniencia, oportunidad, efectividad, viabilidad, legalidad y costos, con el fin de poder ser tomada como un punto de partida y marco de referencia de un modelo integrador y articulador de todos los componentes y recursos del Estado con responsabilidades de Cs y Cd en la República de Colombia, en donde se incluyen los sectores público y privado y la ciudadanía en general tomando como base la legalidad y constitucionalidad de Colombia.

La ENCC para la República de Colombia, deberá ser un documento de carácter estratégico que involucre diferentes líneas de acción, el cual pueda ser utilizado por el Gobierno de Colombia para planear, prever y armonizar acciones en materia de protección

y defensa del Ciberespacio que trasciendan en el tiempo y contribuyan tanto a la prosperidad económica como social del país.

Así mismo, donde se propongan lineamientos para prevención, defensa, detección y respuesta frente a las ciberamenazas sobre los blancos o sectores estratégicos, a fin de afrontar los nuevos retos que suceden y se imponen en o a través del ciberespacio, y propendan por garantizar la libertad y seguridad cibernética de los ciudadanos y la soberanía nacional, la independencia, la integridad territorial y el orden constitucional en el ámbito cibernético.

Desde esta perspectiva, el disponer de una ENCC, garantiza a Colombia, contar con un instrumento en el que con una mirada de más largo plazo, se expliciten los desafíos a la Cs y la Cd, con una clara visualización de los intereses nacionales y de los riesgos y amenazas de que se puede ser objeto en ese cometido.

De igual forma, contribuirá a informar a las respectivas sociedades y a la construcción de la "culturas de Cs y Cd", indispensables al interior de cualquier Estado para abordar estos desafíos con sentido de unidad, además de constituir un valioso instrumento, para en el contexto de la comunidad internacional, aportar a una mayor transparencia, a la generación de confianza entre los Estados y al fortalecimiento de la cooperación internacional.

2.1. El Ce como escenario de conflicto

En menos de una generación, la informática ha pasado de ser de una mera herramienta administrativa que facilitaba los trabajos burocráticos de las oficinas, a constituir por sí misma un recurso estratégico nacional para muchas naciones.

La evidencia de la importancia que las nuevas tecnologías están adquiriendo en el peso específico de las naciones viene demostrada por el hecho de que Estados Unidos haya desplazado su centro de gravedad hacia el ciberespacio. Considerar al ciberespacio como el centro de gravedad de una nación significa reconocer que constituye el centro neurálgico de todos los poderes del país, el ente del que todo depende.

"Nuestra estimación es que los ciberataques serán un componente importante de cualquier conflicto futuro, independientemente de que involucre a grandes naciones, estados hostiles o grupos terroristas"[*].

Por dinámica del conflicto se entiende el proceso de su evolución desde sus orígenes hasta su finalización. Un conflicto no surge de la nada, ni de la noche a la mañana. Todos tienen sus causas y evolucionan de una manera progresiva desde un estado inicial de paz hasta el de guerra declarada. Un conflicto no resuelto con los instrumentos de poder pacíficos puede escalar a uno armado y éste a una guerra declarada.

Por norma general, este proceso de escalada de violencia comprende las seis siguientes fases:

a) Paz: los países no están enfrentados y luchan por intereses legítimos que no son convergentes.

[*] William J. Lynn, III, vicesecretario de Defensa de Estados Unidos.

b) Paz inestable: los intereses nacionales de distintos países empiezan a coincidir. Es un periodo en el que la tensión y las sospechas son elevadas pero no hay violencia o ésta es muy esporádica.*

c) Tensión: situaciones de inestabilidad creciente que alteran la vida normal del Estado y la acción de gobierno y que, por su peligrosidad potencial para la seguridad nacional o colectiva, inducen a los gobiernos a tomar medidas preventivas que pueden provocar la activación de sus sistemas de alerta o el empleo de los recursos de la Defensa Nacional.**

d) Crisis: momentos decisivos dentro de una situación de tensión en los que se produce o prevé un cambio inminente de consecuencias importantes. Suele aparejar la movilización de las Fuerzas Armadas y es posible la aparición de escaramuzas esporádicas también de escasa intensidad.

e) Conflicto armado: es la confrontación física entre colectividades organizadas, aunque no necesariamente reconocidas a la luz del Derecho Internacional, caracterizada por el empleo de medios militares de combate con la finalidad de imponer cada una su voluntad.***

f) Guerra: Es la forma más violenta y más desarrollada de enfrentamiento. Consiste en la confrontación entre colectividades políticamente estructuradas con la finalidad de imponer la voluntad de una sobre otra o de defender los propios intereses. Se caracteriza por el empleo masivo y organizado de medios de combate. La guerra tiene connotaciones de

---

* Lund, Michael S.: Curso de Certificación de Análisis de Conflictos, U.S. Institute of Peace.
** Doctrina Aeroespacial.
*** Ibídem.

> carácter legal y normalmente se desencadena cuando un estado la declara a otro. El reconocimiento formal de la situación de guerra tiene implicaciones jurídicas y políticas.[*]

"La ciberguerra, no se encuentra en la punta de la pirámide de la escalada de un conflicto. La ciberguerra, en su forma de ciberespionaje, tendrá lugar desde las primeras fases del proceso. En su forma de ciberataque dependerá de las tácticas que se adopten en el planeamiento conjunto de las operaciones, si bien normalmente será anterior y/o simultánea a la fase de conflicto. Un ciberconflicto se puede originar de una forma aislada, sin necesidad de que haya una mayor escalada de violencia". (López de Turiso & Sánchez, 2012, p. 119).

"Comparando los conflictos de los últimos años en los que ha existido ciberguerra con los totales del último siglo, se observa que tanto las causas, como los actores implicados o las fases por las que han pasado, se ciñen igualmente a los moldes generales de los conflictos aquí descritos. Se llega, por tanto a la conclusión de que los conflictos han sido y siguen siendo los mismos a lo largo de la Historia, y lo único que han variado han sido los escenarios en los que se llevaron a cabo" (p. 125).

"Durante el tiempo que persista un conflicto, las naciones utilizarán todos los instrumentos a su alcance para luchar por la consecución de sus legítimos intereses nacionales. Estos instrumentos son los denominados «instrumentos de poder" (p. 126)

El ciberespacio está marcado a lo largo de su historia por diferentes tipos de guerras y conflictos, por naciones preocupadas por demostrar su poderío a cada momento, por

---

[*] Ibídem.

potencias claramente marcadas en todos los continentes, por Estados que buscan autoprotección y si es posible, expansión y territorio. Y aunque la misma historia nos ha obligado a establecer organizaciones que han puesto pausas a dichos conflictos y mejor aún, han diseñado mecanismos para acabarlos sin necesidad de convertirlos en nuevas guerras, no podemos negar que la ventana de un posible conflicto se encuentra permanentemente abierta para cualquier nación con intereses estratégicos.

Es por esto que debemos detenernos a pensar que un país como Colombia, con intereses estratégicos definidos, con un posicionamiento geoestratégico privilegiado en la región y con un crecimiento económico en proceso, no está exento de llegar al establecimiento de un conflicto con cualquier otra nación. Pero, ¿qué pasará si dicho conflicto se presenta en un escenario cibernético? ¿Estamos preparados para esto? Debemos tener en cuenta que en los últimos años el internet y las telecomunicaciones han sido los grandes protagonistas en el desarrollo de las naciones a nivel mundial y Colombia no es la excepción.

Pensar en el Ce como un escenario de conflicto en Colombia, nos debe llevar a reflexionar que tan en serio debemos tomar este tema, sabemos que potencias mundiales como los Estados Unidos han desplazado su centro de gravedad al ciberespacio, esto no dice otra cosa que se debe tomar este escenario tan en serio como un conflicto armado tradicional, ya que un posible ataque cibernético en Colombia no solo afectaría las telecomunicaciones sino la economía, la industria y la capacidad de defensa, entre otros.

Sabemos muy bien que un ciberataque se puede generar de forma aislada, sin necesidad de que el conflicto presente una mayor escalada de violencia, convirtiéndolo en

un enemigo silencioso y extremadamente peligroso. Es por esto que en Colombia debe mirar la ciberdefensa como algo primordial, como un objetivo a cumplir, como una mirada prospectiva a la defensa estratégica de los intereses nacionales y como un plus más para seguir creciendo como potencia a nivel regional.

2.2. Los ataques cibernéticos a los sectores y blancos estratégicos, y su afectación a la SDN

Hoy en día, para vencer a una nación no hace falta acribillar a su ejército, basta con destruir la estructura informática de sus infraestructuras críticas cibernéticas nacionales o atacar los blancos estratégicos de una nación. Imaginado. ¿Qué sucedería en Colombia o en cualquier otro país, si por un día se interrumpen todas sus telecomunicaciones? ¿Y si se suspende la red de energía eléctrica?, ¿O si dejan de funcionar los semáforos de todo el país por horas? Todo esto se puede logar con computadores robustos y varias personas capacitadas y bien entrenadas para vulnerar sistemas de información y comunicaciones. Esta nueva guerra sucede a diario y a escala global. Su objetivo es el caos y el acceso de información sensible, lo que puede traducirse en pérdidas millonarias. Podemos notar que es un tema tan sensible que a mediados del año 2014, el presidente Barack Obama solicitó la creación de un /kill switch/ para desactivar eventualmente la internet en todo los Estados Unidos y destina anualmente 191 millones de dólares en preparar escuadrones para una contra ofensiva en caso de un Pearl Harbor digital (Huertas, 2014).

Para el Departamento de Defensa de Estados Unidos, “el ciberespacio se ha convertido en un campo de operaciones de igual proporción que la tierra, el mar, el aire o el espacio y por tanto susceptible de ser escenario tanto de maniobras defensivas como ofensivas, lo que podría incluir ataques preventivos y represalias” (2011, p. 5). Así mismo, según

LT.Col. April Cunningham, portavoz del Pentágono en declaraciones a la BBC, señaló: “Estados Unidos se reserva el derecho a responder a través de medidas diplomáticas, informáticas, económicas y militares, a cualquier amenaza contra la seguridad nacional en el ciberespacio y más allá” (BBC, 2011). Por otra parte, Clarke y Knake (2010) afirman que en Rusia, China, Estados Unidos y una veintena más de países se crearon “cibercomandos”, cuya misión es usar el internet y las tecnologías de la información como armas. Estados como Francia, Reino Unido, Alemania, España, Noruega, Unión Europea, China, India, Irán, Pakistán y Rusia entre otros (Acosta, Pérez Rodríguez, Arnáiz de la Torre, & Taboso Ballesteros, 2010, pp. 27-34), han desarrollado iniciativas que les permitan actualizar los mecanismos de ataque y defensa ante la diversificación y aumento de amenazas cibernéticas transnacionales. Lo anteriormente descrito, refleja el interés por parte de Estados Unidos y algunos otros países por implementar medidas y contramedidas que le permitan brindar un manejo adecuado en materia de ciberguerra dentro las políticas de SDN de cada Estado.

En lo que respecta al continente europeo, la OTAN ha definido la ciberdefensa como "la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques" (OTAN, 2012). Entre los principales esfuerzos realizados por la OTAN en ciberdefensa se encuentran:

- La creación del centro de respuesta ante incidentes de seguridad informática (NATO Computer Incident Response Capability - NCIRC) en el año 2004.

- La aprobación de la Política de Seguridad en Ciberdefensa de la OTAN (“Nato Policy on Cyber Defense”) el 7 de enero del 2008,

-El Acuerdo sobre el "Concepto de Ciberdefensa de la OTAN" ("NATO Cyber Defence Concept") a comienzos del año 2008.

- La asignación de las Responsabilidades en Ciberdefensa, la creación de la Autoridad de Gestión de la Ciberdefensa de la OTAN (NATO Cyber Defence Management Authority, NCDMA) y del Centro de Excelencia Cooperativa de Ciberdefensa (Cooperative Cyber Defence Centre of Excellence, CCD COE) en el 2008.

Cabe destacar, que los esfuerzos realizados por la OTAN tuvieron un importante impulso debido a los Ciberataques que sufrió Estonia en Abril del 2007 (Acosta, Pérez Rodríguez, Arnáiz de la Torre, & Taboso Ballesteros, 2010, p. 35).

En febrero de 2014, la Alianza de Ministros de Defensa de la OTAN, desarrolló una adición a la política de defensa, en cuanto a ciberdefensa colectiva, asistencia a los Aliados, gobernanza, consideraciones legales y relaciones con la industria. Posteriormente en abril de 2014, el North Atlantic Council (NAC) accedió a cambiar el nombre del Comité de Política y Planes de Defensa (Defensa Cibernética) como el Comité de Defensa Cibernética, en junio de 2014, los Ministros de Defensa de la OTAN aprobaron la nueva política de defensa cibernética, que se está aplicando en la actualidad (CCDCOD, 2014). Cada uno de los esfuerzos realizados por la OTAN, confirma que la amenaza cibernética está siendo considerada de alta prioridad y la importancia que cobran cada vez más, reflejan la necesidad por parte de los Estados de protegerse ante los ataques cibernéticos, el ciberterrorismo y la ciberguerra. Es innegable, que los ataques cibernéticos simultáneos a la Infraestructura Crítica (IC) Cibernética Nacional ocasionaría niveles de impacto inimaginables, tanto a nivel de pérdida de vidas humanas, sufrimiento de la población,

pérdidas económicas, afectaciones al medio ambiente e incluso deterioro de la imagen del país que desencadenaría en la pérdida de confianza de la población en su Gobierno, ocasionando consecuencias fatales para la sociedad y la gobernabilidad del país.

De acuerdo a lo descrito en la monografía de Casar:

> "En la seguridad de las IC, la estrategia de la Defensa debe comprender siempre la prevención de posibles ataques, la protección para disminuir la vulnerabilidad y en caso de crisis minimizar los daños y acelerar el periodo de recuperación. Las amenazas enemigas a las IC siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora también ataques en tiempos de paz por medio ciberataques. Los sucesos actuales, incluyendo los ejemplos de Israel y Estonia, demuestran que se puede alcanzar cierto nivel de disturbio real sólo con paquetes de datos hostiles: los bancos se quedaron sin conexión, los medios de comunicación se silenciaron, se bloqueó el comercio digital y se amenazó la conectividad gubernamental con sus ciudadanos." (et. al. 2012).

Considerando que en los países con altos niveles de desarrollo tecnológico, la mayoría de los servicios esenciales a la población se encuentran soportados en la infraestructura tecnológica, no es absurdo pensar que el desarrollo de un conflicto cibernético o ciberguerra conlleva a razonar en múltiples factores, entre ellos, quizás el más importante, es que en la actualidad no existen leyes o normas que regulen las reglas de enfrentamiento en el ciberespacio, por lo que los servicios esenciales a la población como electricidad, agua, gas, comunicaciones se verían afectados y doblegarían la voluntad del Gobierno de cualquier país.

Lo que cada vez hace más peligrosa a la guerra cibernética es que para atacar a un Estado no es necesario la incursión de grandes ejércitos con armas avanzadas, o con

aviones supersónicos o bombas de destrucción masiva, solo basta con un grupo de personas capacitadas acompañadas de computadoras robustas para realizar una afectación masiva a todos los sistemas de telecomunicaciones, energía, el sector bancario, medios de comunicación, entre otros, generando así un gran caos, no solo económico sino social logrando colapsar todo un sistema por muy bien estructurado que se encuentre.

En otra época los blancos estratégicos de afectación a la DSN eran totalmente tangibles, se hablaba de zonas de concentración de armas, antenas de telecomunicaciones, áreas de concentración militar, etc., todo esto obligaba a diseñar sistemas de defensa enmarcado en sectores específicos los cuales a través de sistemas de seguridad robusta con hombres armados, alarmas o sistemas de defensa antiaéreos.

Pero hoy, cuando se habla de guerra cibernética debemos referirnos a blancos intangibles, a la protección de sistemas de información y comunicaciones, a la incertidumbre de no saber dónde nos pueden atacar, a pensar que no tenemos amenazas por el hecho de no estar inmiscuidos en un conflicto mientras estas nos están atacando. Es por esto que la ciberseguridad no debe tomarse como como una mera prevención en caso de conflicto o guerra con otra nación, se debe gestionar de manera permanente, como política de Estado, estrategia permanente en la defensa y seguridad de nuestra nación, solo de esta manera podremos prevenir cualquier ataque cibernético que pueda generar un caos peor al que generaría un conflicto armado.

2.3. Alcances y limitaciones de las iniciativas Colombianas en el Ce

En el año 2016, el 11 de abril, mediante el documento CONPES 3854 “Política Nacional de Seguridad Digital”, el gobierno de Colombia cambió el enfoque tradicional

al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hizo bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política.

Entre ellos, destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

En primer lugar, se establecerá un marco institucional claro en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional.

En segundo lugar, se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital.

Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.

Por último, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico. Para poner en marcha esta política, se ha construido un plan de acción que se ejecutará durante los años 2016 a 2019 con una inversión total de 85 070 millones de pesos. Las principales entidades ejecutoras de esta política son el 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.

Colombia necesita reforzar sus capacidades para proteger sus infraestructuras críticas nacionales y asegurar la defensa nacional en el entorno digital, con un enfoque de gestión de riesgos de seguridad digital.

La política nacional de seguridad digital entenderá los conceptos de seguridad digital, múltiples partes interesadas, infraestructura crítica cibernética nacional y economía digital, como se definen a continuación.

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital Ce, derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de Cs; y (iii) el uso efectivo de las capacidades de Cd, que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Múltiples partes interesadas: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del

entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Infraestructura crítica cibernética nacional: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o el eficaz funcionamiento de las organizaciones e instituciones, incluso de la administración pública.

Economía digital: economía basada en el uso de tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

A continuación se describen las estrategias que se implementarán para alcanzar los objetivos enunciados.

- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos. Este objetivo específico busca desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado. Al mismo tiempo que busca mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional. Para esto, el Gobierno nacional adelantará las estrategias que se describen a continuación.

- Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital. El Ministerio de Defensa Nacional elaborará, entre junio y octubre de 2016, un plan de fortalecimiento que permita al sector Defensa generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra del Estado y su infraestructura crítica. Dicho plan se concentrará en la definición de mejores prácticas y estándares internacionales en los componentes operativos, administrativos, humanos, científicos, de infraestructura física y tecnológica para el CCOC y las Unidades Cibernéticas de las Fuerzas Militares. Se estima que el horizonte del proyecto será hasta 2019. Los mecanismos mediante los cuales se fortalecerán las entidades responsables de la defensa nacional en el entorno digital, se definirán en el marco de la construcción del plan de fortalecimiento. Este proceso estará liderado por el CCOC con el aval del Ministerio de Defensa Nacional e incluirá dos estudios de viabilidad técnica para la conformación de un Centro de operaciones cibernéticas de las Fuerzas Militares, y de un Centro nacional de protección y defensa de infraestructura crítica cibernética nacional, por medio de los cuales se robustecerá la seguridad digital, toda vez que otorga una autonomía cibernética para el Estado colombiano.

- Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional. El Ministerio de Defensa Nacional, a partir de la Guía para la Identificación de Infraestructura Crítica Cibernética (2015), llevará a cabo la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales. A partir de esto, establecerá los contenidos de los planes de protección de la infraestructura crítica cibernética nacional, y los socializará en el marco de la agenda nacional de seguridad digital.

El catálogo de infraestructura crítica se construye de forma conjunta entre el Ministerio de Defensa Nacional y las múltiples partes interesadas. Para esto, en una primera instancia, cada sector levantará su información con base en los siguientes criterios transversales: identificación de la infraestructura crítica digital, interdependencia con otras infraestructuras, y evaluación de la continuidad de negocio dependiendo de las amenazas latentes de sus servicios esenciales. Los avances en el levantamiento de la información se verificarán mensualmente por medio de reuniones convocadas por el CCOC. En una segunda instancia, las múltiples partes interesadas entregarán la información mencionada al Ministerio de Defensa Nacional para identificar, priorizar y definir el grado de criticidad de cada sector y entidad (catálogo de infraestructuras críticas cibernéticas nacionales).

El grado de criticidad de las infraestructuras cibernéticas definido por el catálogo, será el insumo principal para diseñar la estrategia de protección y defensa de la infraestructura crítica cibernética nacional. Esta estrategia será construida por el Ministerio de Defensa Nacional en coordinación con los sectores, los subsectores y las entidades que participaron en el levantamiento de la información.

La estrategia tendrá que realizarse periódicamente con el fin de contar con un catálogo y una estrategia actualizados en todo momento. Característica esencial en lo relacionado con seguridad digital, teniendo en cuenta la evolución permanente de las amenazas en el ciberespacio. En cada actualización se buscará vincular a los sectores y entidades que aún no hayan decidido participar en el catálogo, reiterando la invitación a hacer parte del grupo de trabajo de la primera instancia. Esto permitirá robustecer el catálogo, y en consecuencia, la estrategia de protección y defensa.

Finalmente, en materia de cooperación nacional, el CCOC viene adelantando el proceso de elaboración del catálogo de infraestructuras críticas cibernéticas nacionales en el país. El catálogo en mención permitirá, a futuro, coordinar y gestionar los planes y programas de protección y defensa a infraestructuras críticas cibernéticas nacionales. A 2015, el Ministerio de Defensa Nacional había elaborado la Guía para la Identificación de Infraestructura Crítica Cibernética, la cual se constituye como el insumo principal de dicho catálogo, construido en coordinación con las múltiples partes interesadas." (CONPES, 3854, 2016).

Con el documento CONPES 3854 "Política Nacional de Seguridad Digital", referenciado en alguno de sus apartes, Colombia da un salto al futuro para presentar las posibles soluciones que le puedan permitir al país mantenerse a la vanguardia de las nuevas amenazas que se presentan en el ciberespacio y tomando las medidas necesarias para que en un corto plazo pueda estar a la vanguardia de los países que cuentan con estrategias de Cs y Cd, como nos podemos dar cuenta el CCOC está elaborando un catálogo de infraestructuras críticas cibernéticas las cuales deben ser actualizadas a partir del mes de enero de 2017 por los sectores que la integran y con ellos pueden determinar su nivel de criticidad.

3. Conclusiones

Conclusión 1.

Para proponer la Estrategia, es necesario contar con una visión general de como las Tecnologías de la Información y Comunicaciones (TIC) impactan a la República de Colombia desde diferentes contextos como económico, político, social, medioambiental y geográfico a fin de identificar sus nodos estratégicos y determinar su dependencia tecnológica para garantizar la operación de sus procesos misionales.

Conclusión 2.

Para formular una ENCC, se considera fundamental realizar una comprensión y análisis general de la amenaza cibernética y de la evolución de sus tendencias, como punto de partida para trazar las líneas de acción de la ENCC que requiere la nación para afrontar los nuevos desafíos que impone ésta, entendiendo que siempre está implícita en los sistemas de tecnologías de la información y de las comunicaciones, avanzando al mismo ritmo de su evolución y su desarrollo.

Conclusión 3.

La estrategia de Cs y Cd para la República de Colombia, deberá garantizar unos principios rectores que estén alineados con los principios de la Constitución Política de Colombia de 1991, y los tratados suscritos o ratificados por Colombia, basados en la adecuada protección y cumplimiento de los derechos de los ciudadanos, bajo la responsabilidad del Gobierno. Así como analizar el contexto legal a nivel de Cs y Cd y tener una visión clara de las leyes a nivel nacional que permitirá establecer el grado de

madurez del país en este contexto a fin de realizar las recomendaciones más apropiadas para optimizar los niveles de seguridad cibernética de Colombia.

Conclusión 4.

Un componente fundamental a garantizar en la ENCC es promover la optimización y resiliencia de las infraestructuras críticas del Estado y de los blancos estratégicos e intereses nacionales, la igualdad en el uso del ciberespacio, y coordinación de esfuerzos nacional e internacional, encaminados al logro de una Cs y Cd reales.

Conclusión 5.

Colombia debe implementar y fortalecer las Unidades de Cs y Cd como son: El CCOC, el COLCERT, y el Comando Cibernético Policial, las cuales son las Unidades encargadas de proteger su infraestructura crítica, este fortalecimiento se hace con medios tecnológicos adquiriendo nuevas herramientas tanto en hardware como en software, que le permitan hacerle frente a las nuevas amenazas cibernéticas, los cuales se implementaran capacitando al personal en el manejo de nuevas tecnologías, y con capacitación en todas las áreas de la seguridad informática, iniciando con cursos básicos en redes de datos como son el CCNA, especialización en seguridad informática y maestría en seguridad de la información que les da nuevas herramientas al personal de informática para proteger el ciberespacio.

Referencias Bibliográficas

Acosta, Pérez Rodríguez, Arnáiz de la Torre, & Taboso Ballesteros. (2010) "Seguridad Nacional y Ciberdefensa". Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones Ciudad Universitaria, Madrid.

BBC. (2011) "Ciberespacio: el nuevo ámbito de la guerra para el Pentágono". Recuperado de: http://www.bbc.com/mundo/movil/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml.

BuRghaRdt, Tom: Cyberspace, the Battlefield of the Future: Pentagon Ramps- Up Cyberwar Plans, (2011). Recuperado de: http://www.globalresearch.ca/index.php.

Casar, C. J., Ortega, L. F., Enriquez Gonzalez, C., López de Turiso, J., Gomez de Agreda, Á., Acosta, O. P., & Pérez Cortéz, M. (2012). El Ciberespacio. Nuevo escenario de confrontación. Recuperado el 20 de 05 de 2015, de Ministerio de Defensa de España. Recuperado de: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf.

Department of Homeland Security. (2013). Critical Infrastructure. Recuperado el 17 de 05 de 2015, de Department of Homeland Security: http://www.dhs.gov/critical-infrastructure.

Departamento Nacional de Planeación. (2016). Documento CONPES 3854 "Política Nacional de Seguridad Digital" Bogotá D.C.: Ministerio de Interior y de Justicia Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.

Definición de ciberespacio. Recuperado de: http://repositoriodigital.academica.mx/jspui/bitstream/987654321/480529/1/ARTICULO%20CIBERESPACIO.pdf.

Definición de ciberguerra. Recuperado de: https://dspace.palermo.edu:8443/dspace/bitstream/handle/10226/1448/Ciberguerra-Pantano%2068586.pdf?sequence=1&isAllowed=y

Definición de ciberespionaje. Recuperado de: http://iugm.es/uploads/tx_iugm/ACTAS_IV_JORNADAS_DE_EST_DE_SEGURIDAD.pdf.

Definición de ciberseguridad y ciberdefensa. Recuperado de: http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf.

Definición de seguridad digital. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Departamento Nacional de Planeación. (2011). Documento CONPES 3701: "Lineamientos de Política para Ciberseguridad y Ciberdefensa". Bogotá D.C.: Ministerio de Interior y de Justicia.

Departamento Nacional de Planeación. (2016). Documento CONPES 3854 "Política Nacional de Seguridad Digital" Recuperado de:https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.

Ganuza aRtiles, N. (2010) "Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio: la situación de la ciberseguridad en el ámbito internacional

y en la OTAN", Instituto Español de Estudios Estratégicos-Instituto Universitario «General Gutiérrez Mellado», Dirección General de Relaciones Institucionales, Ministerio de Defensa, Madrid.

Informe de Ciberseguridad e Infraestructuras Criticas de las Americas. Trend Micro-OEA-2015.

Lund, Michael S.: Curso de Certificación de Análisis de Conflictos, U.S. Institute of Peace, en: http://http://es.scribd.com/doc/61965893/5/Paz-inestable.

Ministerio de Defensa Nacional, Colombia. (2015) Guía para la Identificación de Infraestructura Crítica Cibernética.

Nolasco Gonzalez, A. (s.f.). Recuperado de:https://f-informacion.wikispaces.com/file/view/Act1_AlejandroNolascoGonzalez.pdf.

Shaw, D. (2010). Cyberspace: What Senior Military Leaders Need to Know. PENNSYLVANIA USA: U.S. Army War College CARLISLE BARRACKS.

(BBC, 2011). Por otra parte, Clarke y Knake (2010)