Concepto estratégico conjunto en ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia

Nelson Armando Cárdenas Vélez

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

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

2019

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA
MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

CONCEPTO ESTRATÉGICO CONJUNTO EN CIBERSEGURIDAD Y CIBERDEFENSA PARA LAS FUERZAS MILITARES DE COLOMBIA

Mayor NELSON ARMANDO CÁRDENAS VÉLEZ

Tutor

Teniente de Navío JULIÁN DAVID APONTE DÍAZ

BOGOTÁ - COLOMBIA
2019

Abstract

The networking, services and applications exponential evolution, and the each time bigger technological dependence of the society for its survival, put in the Estate´s spotlight the necessity of defend, control and govern the cyberspace, activities that different investigators affirm, is more important the politics application than the action executed from the network technical perspective.

Resumen

La evolución exponencial de las redes de datos, los servicios y aplicaciones que son prestados a través de estas y la cada vez mayor dependencia tecnológica de las sociedades para su supervivencia, pone en la mira de los Estados la necesidad de defender, gobernar y controlar el ciberespacio, actividades que varios investigadores coinciden afirmando, que incide más la aplicación de políticas que la acción ejecutada desde la perspectiva técnica de la red.

Keywords: Ciberdefensa – capacidad – ciberataque – seguridad nacional – estrategia – ciberespacio – acto – agresión – ciberdiplomacia – Estado – infraestructura – plan - seguridad.

TABLA DE CONTENIDO

Resumen 2
Tabla de abreviaturas 4
Introducción 5
CAPITULO 1 10
El ciberespacio y la política internacional 10
Seguridad Nacional y su relación con el ciberespacio, la ciberguerra y el ciberataque. 12
El dilema de los Estados 15
CAPÍTULO II 18
Caracterización de la amenaza 18
Ciberataque a Estonia 19
Ciberataque a Georgia 22
Ciberataque a Estados Unidos 24
Ciberataque a Irán 26
Experiencias que construyen 28
Tendencias mundiales 31
Tendencias regionales 47
Visión nacional 50
CAPÍTULO III 54
Operaciones militares en el ciberespacio; capacidades de ciberseguridad y ciberdefensa para las fuerzas militares 54
Política de seguridad y defensa del Estado Colombiano "Todos por un nuevo país" 55
Objetivos Estratégicos 2030 e Iniciativas Estratégicas 2015-2018 de las Fuerzas Militares de Colombia 56
Sistema por capacidades 59
Homologación con la estrategia OTAN 62
Conclusiones 67
Referencias bibliográficas 69
Tablas y figuras 71

Tabla de abreviaturas

CDCiber	Centro de ciberdefensa
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIP	Critical Infraestructure protection
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
GGE	Grupo de expertos gubernamentales
IAB	Junta de arquitectura Internet
IETF	Internet Engineering Task Force
ISP	Internet services provide
ICANN	Internet Corporation for Assigned Names and Numbers
NCW	Network centric warfare
NRA	National Risk Assessment
OTAN	Organización del tratado atlántico norte
TIC	Tecnologías de la información y las comunicaciones

Introducción

En la actualidad se han dado cambios en materia de las comunicaciones incitados principalmente por la necesidad de tener contacto permanente con las demás personas, además de la evolución tecnológica que ha llevado al hombre a hacerse más dependiente de ella. De esta manera, la búsqueda permanente por lograr una comunicación eficiente y que abarque largas distancias, ha sido el génesis de grandes inventos que de una u otra forma han facilitado y cambiado el modo como hoy se comunican los seres humanos.

Es así, como se pasó del desarrollo de ruidos, expresiones y señales, a la transmisión de voz, video y datos a través de una red mundial de computadores llamada "internet"[1], entendida como una red de ordenadores interconectados que permite un conjunto de servicios y aplicaciones de los cuales se puede hacer un uso provechoso. Este gran invento, considerado por muchos autores como uno de los más importantes de la humanidad, cambió la forma en que gran parte del mundo trabaja, se comunica e interactúa.

Existe una complejidad con respecto al poder de la computación que se deriva de la participación del ser humano en el sistema. El cambio tecnológico exponencial ha tornado el medio ambiente más complejo que nunca, as cifras que acompañan esta afirmación son asombrosas: "más de 2,1 millones de personas conectadas vía *internet*, 1,8 *zettabytes* de datos electrónicos creados en el 2011 y un total de 555 billones de sitios web" (Chang, Granger, 2012, p. 2012).

---

[1] En un primer momento, Internet se empleó con objetivos militares. Se diseñó como una red capaz de funcionar incluso en caso de que algunos de sus nodos fueran destruidos (ya que la información circularía por otros cauces de la red). Posteriormente, las universidades y las industrias se interesaron por esta red y fueron poco a poco cobrando protagonismo dentro de la misma. Actualmente Internet es un fenómeno social y económico por su extensión y por la falta de restricciones que la regulen (NTAE).

Actualmente se percibe que la cifra de dispositivos móviles conectados a la internet supero la cantidad total de personas en el planeta.

Aunque no era su objetivo inicial, la masificación de internet mutó hacia un área de tamaño inimaginable con un alcance cada vez más extenso y más difícil de controlar. Esta área es "el ciberespacio", definido por el NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) como:

> *El ambiente formado por componentes tangibles e intangibles, caracterizado por el uso de computadoras y del espectro electromagnético, para almacenar, modificar e intercambiar datos usando redes de computadores* (CCDCOE).

De tal manera que se trae a colación el concepto de Ciber, el cual será utilizado con frecuencia en este documento ya que es un prefijo utilizado ampliamente en la comunidad internacional para denominar conceptos relacionados con las redes (Cibercultura, Ciberespacio, Cibernauta, etc.). Su origen es la palabra griega κιβερναο, que significa pilotar una nave.

> *"Tras el avance de la tecnología informática (procesadores e internet), se puede inferir que la Tercera Revolución Industrial ha influido en nuevas manifestaciones de la guerra, estableciendo un nuevo poder militar: el Ciberespacio"* (Gaitán, 2011, p. 23).

Los estados no han sido ajenos al uso del ciberespacio y por ello hoy en día muchas infraestructuras críticas nacionales dependen del mismo para desarrollar sus actividades, lo que ha generado que aumenten las superficies de ataque en el ciberespacio. Bajo este escenario, ha surgido una nueva tipología de enfrentamiento interestatal denominado como Ciberguerra, la cual busca paralizar o destruir las conexiones y las infraestructuras críticas de un país anulando sus sistemas informáticos (Instituto Español de Estudios Estratégicos, 2010, p. 16).

Siguiendo la senda del Ciberespacio, es menester enfocar el presente documento al Ciberataque, entendido como una forma de Ciberguerra donde combinado con un ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a la misma (Instituto Español de Estudios Estratégicos, 2010, p. 333). En el escenario del ciberespacio como nuevo campo de batalla, los ciberataques (amenaza que afecta o desarticula los centros de gravedad de un enemigo), pueden ser tipificados como un acto de agresión ya que se violan las redes y los sistemas del adversario y por ende su seguridad. Además, tras no existir una legislación armonizada que le haga frente a esta amenaza, es necesario el desarrollo de iniciativas lideradas por los Estados que permitan el control de los ataques que afectan transversalmente al sector privado, público y de los ciudadanos.

En el escenario local donde la misión de las Fuerzas Militares contempla la protección de los intereses del Estado, se hace necesario el diseño de un proyecto que busque desarrollar las capacidades necesarias con el fin de preservar el ciberespacio de la nación, a través del diseño de un plan estratégico para alcanzar los lineamientos establecidos dentro de una estrategia cibernética nacional que le permitan a las Fuerzas Militares y demás entidades públicas y privadas, estar preparadas para prevenir, identificar y neutralizar cualquier tipo de amenaza que se encuentre en el ciberespacio. Esta investigación busca descubrir los factores clave en la y gestión de incidentes cibernéticos que permitan diseñar las líneas de acción que puedan ser recomendadas al alto mando militar y estatal, para concepto estratégico que permita contrarrestar las amenazas nacionales que utilizan las tecnologías de la información y las comunicaciones en su accionar, al tiempo que permitan desarrollar planes estratégicos, operacionales y tácticos orientados a patrocinar la ciberseguridad y la ciberdefensa del Estado.

La rápida evolución de las tecnologías de comunicación en los Estados durante el último cuarto del siglo XX y de principios del XXI, ha generado abundantes reflexiones sobre la dimensión política, estratégica, operativa y táctica del ciberespacio y de las actividades que pueden realizarse en ese entorno. Es así como la conveniencia de desarrollar capacidades militares de "Ciberseguridad y Ciberdefensa" por parte de los Estados ha pasado a ocupar los primeros espacios de debate en el diseño de una estrategia de defensa nacional.

Esa tendencia ha llevado a la adopción de una estructura funcional que identifica las capacidades para enfrentar las amenazas cibernéticas en las áreas de responsabilidad asignada a las Fuerzas Militares, las mismas se dividen básicamente en tres grupos cuyo objetivo general se describe en la tabla No.1.

Tabla 1 - Definición de capacidades cibernéticas (Aguilar, 2010)

CAPACIDAD	OBJETIVO
Defensa	Prevenir, detectar, reaccionar y recuperarse frente a ataques, intrusiones, interrupciones o cualquier tipo de acción hostil que pueda comprometer la información que transita dentro de la red cibernética naval, las redes utilizadas por las infraestructuras críticas y las redes que se encuentren dentro del área de responsabilidad de la Armada Nacional de la República de Colombia.
Inteligencia	Recopilar, analizar y procesar toda información relacionada con las tecnologías y sistemas utilizados por los adversarios.
Respuesta	Desplegar medidas y acciones que se deban tomar frente a amenazas y ataques que se presenten dentro de las redes de interés

	institucional o cualquier sector del ciberespacio donde se requiera la acción de la Armada Nacional.

Fuente: Aguilar, L. (2010). *biblioteca virtual de defensa.* (I. E. Estratégicos., Productor)

De este modo, la tesis planteada para desarrollar es, ¿Cuál debería ser el concepto estratégico conjunto en ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia? Para esto se empleara un método deductivo de investigación, mediante el cual se estudiaran los casos más representativos de ciberataques en el mundo y su incidencia en la seguridad nacional de tal forma que se pueda realizar una caracterización de la amenaza, para finalmente proponer el concepto estratégico conjunto en ciberseguridad y ciberdefensa para Fuerzas Militares de Colombia.

Con el fin de desarrollar esta tesis, la investigación se propone cumplir con el objetivo principal de, proponer el concepto estratégico conjunto en ciberseguridad y ciberdefensa para Fuerzas Militares de Colombia.

Este objetivo se alcanzara mediante los siguientes objetivos específicos: Primero, describir la relación de la Seguridad Nacional con el Ciberespacio, Ciberguerra y Ciberataque. Segundo, caracterizar la amenaza mediante la incidencia de la ciberguerra y los ciberataques en la Nación. Por último, Identificar las capacidades requeridas para enfrentar efectivamente las amenazas cibernéticas dentro del concepto estratégico de ciberseguridad y ciberdefensa de las Fuerzas Militares de Colombia.

CAPITULO 1

El ciberespacio y la política internacional

Es importante precisar la definición de un acto de agresión para poder analizar más a fondo la relación directa que tiene con los ciberataques y su influencia en las decisiones tomadas por los Estados.

> *Un acto de agresión está definido como el uso de las fuerzas armadas por parte de un Estado contra otro sin justificación de defensa propia o autorización por parte del Consejo de Seguridad. La definición de acto de agresión, así como de las acciones que califican como actos de agresión, establecida en las enmiendas (como la invasión a través de las fuerzas armadas, bombardeos o bloqueos) fue influenciada por la Resolución 3314 (XXIX) de la Asamblea General de la ONU del 14 de diciembre de 1974* (Corte Penal Internacional, 2013).

Con lo anterior, es relevante resaltar la importancia de este análisis ya que esta amenaza podría vulnerar la capacidad de respuesta de un Estado, hasta el punto de volver obsoleta su defensa estratégica mediante la afectación directa de los ámbitos social, político y económico, llevándolo a un estado de indefensión total. Esto ya ha ocurrido. Los Ciberataques han afectado no sólo a los Estados, sino a diferentes entidades gubernamentales y a la sociedad civil, haciendo que se cree la necesidad de aunar esfuerzos para hacerle frente a esta amenaza que es cada vez más latente, las fronteras y vulnera la seguridad y defensa nacional. En el marco de los Conflictos Armados Internacionales, resulta aún más importante un estudio exhaustivo de los Ciberataques con el fin, en primer lugar, de encontrar su sitio en la normatividad jurídica, a fin de

que pueda, si es el caso, ser tipificado como acto de agresión y en segundo lugar, para que el Estado logre anticiparse a cualquier intención de ciberataque contra sus infraestructuras críticas.

Hoy cuando nos encontramos en la era de las tecnologías de la información y las comunicaciones y se observa como es cada vez más factible que una persona con algunos conocimientos informáticos, promovida por un Estado o no, logre a través de un computador llevar a cabo una serie de acciones en contra de la infraestructura crítica de una nación, dirigidas a dañar gravemente las capacidades de esta con el fin de imponer la aceptación de un objetivo propio, o simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, definida por Clausewitz como un "acto de fuerza que se lleva a cabo para obligar al adversario para atacar nuestra voluntad", con la diferencia de que el método empleado no sería la violencia física, sino un ataque informático que permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso, para derrocarle en caso de guerra a través del ciberespacio (ONU, 2013).

Ante el presente panorama donde las amenazas cibernéticas son cada vez más evidentes para la comunidad, los Estados han tomado una serie de iniciativas orientadas a fortalecer su infraestructura física e informática, de tal forma que les permita desarrollar capacidades para prevenir, evitar, contener y responder ataques cibernéticos. Para lograr este objetivo, países como Estados Unidos, China, Reino Unido y Rusia entre otros, han creado entidades dedicadas a la ciberdefensa, e incluso han llegado más allá, creando ciberejércitos (Aguilar, 2010, p. 31). El ciberespacio, ciertamente, formará parte de cualquier guerra que se produzca en el futuro.

"Mañana no estaremos en el ciberespacio, seremos el ciberespacio." Paul Rexton Kan.

A su vez, la comunidad internacional también se ha basado en un marco jurídico para intentar castigar estos ataques por medio de la posición única del acto de agresión en el Estatuto

de Roma, donde se concreta en el Artículo 8 bis adoptado en Kampala, que define el crimen de agresión individual como la planificación, preparación, inicio o ejecución de un acto de agresión por parte de una persona en posición de liderazgo. En gran medida, implica el requerimiento mínimo de que éste constituya una violación manifiesta a la Carta de las Naciones Unidas. Cumplidos estos requerimientos y aunque la tipificación de los ciberataques como crimen de agresión, podría llevarse a cabo con el respaldo de la voluntad de los Estados que proyecten en sus agendas internacionales, la necesidad de frenar esta amenaza jurídicamente, aun no se ha hecho, lo cual, representa una ventana legal a través de la que cualquier fuente de ciberataque contra un Estado, podría llegar a ser declarada impune, aun en caso de ser identificada.

El continuo proceso entorno a los conceptos y definiciones del crimen de agresión ha sido lento y se ha consolidado como un limitante para la adaptación del mismo en actos tales como los ciberataques, sin embargo, ha de tenerse en cuenta que las condiciones de los ciberataques implican un impacto semejante, o en algunos casos superior a los causados por confrontaciones o ataques convencionales de tipo militar y este concepto influye claramente en la posición de los Estados y de los organismos multilaterales en temas de seguridad y defensa nacional.

Seguridad Nacional y su relación con el ciberespacio, la ciberguerra y el ciberataque.

Tras la previa contextualización de la influencia del ciberespacio en la guerra, es menester definir la interrelación de con la Seguridad Nacional para aterrizar el tema y encausarlo al objetivo del presente trabajo.

De lo anterior se desprende que tras la difusión de la tecnología, además de los beneficios para la humanidad, se han generado serios problemas relacionados con la posibilidad de un inesperado ataque cibernético y la inminente amenaza de una ciberguerra, cuyas consecuencias podrían ser nefastas para el orden y la Seguridad Nacional.

De acuerdo con el Secretario de Defensa de los Estados Unidos y ex Director de la CIA, León Panetta: *"Lo cierto es que existe la capacidad cibernética para tumbar nuestras redes eléctricas y/o paralizar el sistema financiero de nuestro país. Por lo tanto, considero que tenemos que estar preparados no solo para defendernos contra esta clase de ataques sino también, en caso necesario, para ser agresivos"* (Fuentes, 2012, p. 3), se puede deducir que la preocupación que se tiene con respecto al impacto que genera los ciberataques en un Estado, en este caso Estados Unidos, es que afecta la estabilidad y seguridad dela mayor parte de los Estados en el sistema internacional.

Por tal razón, no se debe subestimar su poder destructivo, todos los Estados son vulnerables a la posibilidad de un ataque sorpresivo. Es necesario reforzar las defensas cibernéticas como parte de la estrategia militar y a partir de este hecho crear hito para que haya normatividad jurídica y se pueda proceder ante un posible caso de ciberataque amparado por el derecho internacional y los convenios internacionales existentes.

La incidencia del ciberespacio, ciberguerra y ciberataque en la Seguridad Nacional, consiste en que la principal afectación es el impacto negativo que tiene para un Estado ser vulnerable a los ciberataques, ya que muchos de los procesos que hace, son a través del ciberespacio. En este orden de ideas, se mencionan especialmente las amenazas a la infraestructura crítica, la psicología humana, y . ciberespacio. Dentro de los posibles sabotajes se encuentra: el sabotaje de los servicios públicos, la paralización de la red de transporte ferroviario o la interrupción de la energía eléctrica, ataques a reactores nucleares, entre otras. Estas afectaciones suponen un serio quebranto para la normalidad y seguridad de la sociedad (Caro, 2010, p. 59).

Al pensar que un arma cibernética puede afectar gravemente la infraestructura de un Estado, es pertinente traer a colación el caso de Irán, en el cual se constató que con la intrusión de un malware, denominado *stuxnet* al sistema informático del reactor nuclear de Busher en Irán, se interfirió sobre la estructura del mundo real (BBC News, 2010); ataque que en la actualidad se le atribuye a Israel[2].

En cuanto a la psicología humana, se puede inferir que tales afectaciones se dan a causa del caos organizacional y civil que se pueden generar, entre otras, ante la falta parcial o total de los sistemas tecnológicos que facilitan la supervivencia de una sociedad, siendo la población la directamente afectada debido a que se pone en riesgo el funcionamiento adecuado de la misma. Ejemplo de este tipo de afectaciones puede ser el "pánico virtual" causado por la supuesta noticia del colapso del Banco Davivienda en Colombia. Hace algunos años miles de usuarios del banco Davivienda retiraron sus ahorros por cuenta de un rumor en el que se señalaba que la entidad sería intervenida. Al final se descubrió que el correo provino de un comerciante de Buenaventura, quien terminó en la cárcel por el hecho. El monto retirado en tres días superó los mil millones de pesos (El País, 2013).

La dimensión del armamento hace referencia a la nueva generación de tecnología militar, como los aviones no tripulados, tanques aviones, etc. Este nuevo desarrollo militar tecnológico está a merced del ataque de un hacker quien lo puede manipular obteniendo consecuencias letales. A pesar de la superioridad tecnológica que puedan tener los ejércitos, los Estados más vulnerables pueden llegar a ser atacados, ya que fácilmente podrían estar o ser permeados por sus enemigos (Gaitán, 2012, p. 23).

---

[2] Esta es una clase de ataque que ya ha sido revisada en diversas investigaciones, y catalogada como una de las formas más poderosas de emplear la informática con un arma.(Gaitán, 2012, p. 18)

El dilema de los Estados

Es claro que los efectos de los ciberataques sobre la seguridad nacional pueden llegar a ser desastrosos, es una amenaza latente que prioriza la necesidad de modificar las agendas de seguridad de los Estados (según sea su percepción de amenaza), sin embargo y dado su alcance hay un vacío que no permite que los Estados respondan efectivamente ante tales amenazas.

El problema generalizado que tienen los gobiernos es que limitan la respuesta que deben tener ante posibles ataques ya que la fuente es un computador. Si de cierta manera se tuviera establecido o tipificado el ciberataque, el Estado agredido podría acceder con la fuerza o con una queja ante el organismo encargado, eso cada país lo determina.

El dilema es que dependiendo de cómo se conciba un ciberataque se cuestiona el hecho de que sea o no una agresión. Sin embargo el efecto de agresión inicial es el mismo, debido a que al verse afectada una fuente de la cual el Estado depende para su sustentación, el resultado no afecta en la misma magnitud si la agresión es cibernética o física. Lo que se debe hacer es mirar cual fue la condición, cuál fue el impacto y si eso determina que sea o no una agresión, el medio es irrelevante.

En el escenario estratégico, el objetivo de las tecnologías informáticas y el ciberespacio es destruir y desarticular los centros de gravedad del adversario o enemigo para deshabilitarlo en el conflicto (Gaitán, 2012, p. 24). Según Clausewitz el Centro de Gravedad constituye fuente de fortaleza moral y física a nivel estratégico, son los puntos más vulnerables del enemigo, pueden ser varios pero hay que identificarlos muy bien para que el ataque sea el camino directo a la victoria.

Adicionalmente, es importante tener en cuenta que en el marco de la seguridad nacional la esencia de los ciberataques es ofensiva, defensiva y de inteligencia en el ciberespacio (Instituto Español de Estudios Estratégicos, 2010). Estos ataques son tan eficaces que alcanzan cualquier objetivo en el mundo en tiempo real exponiendo a redes y sistemas a ser interrumpidos o tomados por un hacker o por un código dañino automático.

Con lo anterior se resalta la Ciberdefensa donde no solo depende de las Fuerzas Militares, depende las instituciones gubernamentales e internacionales, organismos de seguridad privados, inclusive de los mismos ciudadanos ya que "no puede seguir siendo un tema fuera de la agenda gubernamental, ni tampoco, no ser considerada al interior de los esfuerzos de las Instituciones militares para preservar la defensa y la seguridad del Estado" (Gaitán, 2012, p.136). Por ello los Estados deben trabajar en la construcción de modelos de ciberdefensa que ayuden a contener las amenazas a las que se puede enfrentar en un futuro.

Estados Unidos y Alemania han construido modelos de ciberdefensa; por un lado Estados Unidos con el *"America's Cyber Future: Security and Prosperity in the information age"*, ha erigido su ciberdefensa sobre los siguientes pilares: Adoptar una estrategia de seguridad y protección global del ciberespacio; forjar una agenda internacional para la seguridad cibernética; establecer al interior de la política estadounidense una declaratoria sobre ciberdefensa; elevar los costos para los atacantes cibernéticos; prepararse para el futuro de la Internet; construir capacidad institucional necesaria para coordinar las responsabilidades del Gobierno de EE.UU, para el ciberespacio; mejorar la supervisión de las actividades gubernamentales de los EE.UU., en el ciberespacio; proteger la infraestructura critica de la Nación y aprovechar la energía innovadora del sector privado para la Seguridad Cibernética". (Gaitan 2012, p. 124).

El Ministerio Federal del Interior, en el documento "Cyber Security Strategy for Germany" también se basa en la creación de algunos pilares para construir y apoyar su ciberdefensa.

"La protección de la infraestructura informacional critica, asegurar las tecnologías informacionales en Alemania; fortalecer la seguridad de las tecnologías informáticas en el sector público; contar con un centro nacional de respuesta cibernética; contar con un Consejo Nacional de Seguridad Cibernética; mantener el control efectivo del crimen en el ciberespacio; generar acciones coordinadas para asegurar la seguridad cibernética en Europa y la red mundial; uso de tecnología información de confianza; la capacitación del personal de las autoridades federales en conocimientos informativos y contar con herramientas apropiadas para responder a los ataques" (Gaitán, 2012, p.278).

De esta manera, y teniendo en cuenta su importancia en el nuevo orden mundial, es menester fortalecer mecanismos de prevención, contención y respuesta de los Estados para no poner en riesgo la seguridad nacional de un Estado o bien para sancionar a los que afecten la seguridad tanto del Estado como de los ciudadanos.

Hoy por hoy los Estados deben sumar a su larga lista de amenazas las que se pueden materializar a través del ciberespacio al ser este el medio más eficaz para que su funcionamiento sea más eficiente, por consiguiente se está haciendo cada vez más estrecha la relación de la seguridad nacional con el ciberespacio y por ende con sus tintes negativos como los ciberataques, la situación entonces se pone aún más interesante al proceder desplegando una serie de capacidades orientadas a enfrentarlos, pero este será un tema que se trate más adelante.

CAPÍTULO II

Caracterización de la amenaza

Con el fin de poder caracterizar la amenaza a la que se enfrentara Colombia y así definir las capacidades que deben ser adoptadas en la estrategia nacional de ciberdefensa, en este capítulo se analizarán los ciberataques que más relevancia han tenido en la última década; estos son los casos de Estonia, Georgia, China e Irán. Los cuales ejemplifican el impacto ocasionado en el ámbito político, económico y social. El grado de afectación de las amenazas, producto de la ciberguerra son equivalentes o mayores a las generadas por armas convencionales y nucleares. Este fenómeno se da, principalmente, porque a través de las acciones ejecutadas en el escenario del ciberespacio llegando incluso a paralizar la infraestructura crítica y por ende todo el país desde cualquier lugar del mundo. Por ende es posible que quién ejecutó tal acto jamás sea descubierto, se mantenga en la distancia y así no pueda ser capturado.

Es tal el impacto de estos eventos que países como Estados Unidos han dado prioridad a declarar la infraestructura digital como "un activo estratégico nacional", se traduce en una preparación frente a un escenario de ciberguerra (Aguilar, 2010, p. 21). Gran Bretaña por su parte estableció políticas de ciberseguridad creando el GCHQ, un centro de operaciones equivalente a la NSA (National Security Agency) estadounidense. De igual manera, China piensa en las guerras de la segunda mitad del siglo XXI. Muchos otros países están organizándose para la ciberguerra; entre ellos, Rusia, Israel, Corea del Norte, etc. El ciberespacio, ciertamente, formará parte de cualquier guerra que se produzca en el futuro (Aguilar, 2010, p. 31).

Planteado entonces este nuevo escenario de batalla que se vale del uso de los computadores y la comunicación en red, se infiere que se explotan las falencias estratégicas de

seguridad para alcanzar los objetivos que se encuentran normalmente detrás de ellas explotar boicotear más fácilmente las redes de información de los Estados y en consecuencia, procesos que son vitales para su subsistencia (Gaitán, 2012, p. 30). Esto siempre bajo el supuesto de impactar la psicología del ser humano y desarticular la logística estatal, factores que particularizan a esta nueva corriente de amenazas.

La globalización como catalizador de las nuevas tecnologías se ha revelado como un artilugio de doble cara que, por un lado, demuestra efectividad y facilidad para interconectar las redes y comunicaciones, pero por el otro, es un escenario idóneo para que el anonimato sea el cómplice de las más atroces acciones que afectan al Estado hasta el punto de volver inservible su capacidad de respuesta y colapsar la infraestructura critica que sostiene a la sociedad. La dependencia de las tecnologías informáticas ha sido tal que se objeta la autonomía del Estado de funcionar efectivamente, y se pone a merced de la voluntad de aquellos que con facilidad pueden violentar las porosas fronteras cibernéticas a través de un computador, incluso llegando a causar más daño que con un arma nuclear.

Ciberataque a Estonia

Para ilustrar los impactos de los ciberataques se analizará el ataque cibernético sufrido en Estonia, considerado el mayor ataque cibernético de la historia.

En el 2007, Estonia sufrió el peor ataque cibernético, A groso modo, 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 por varios días. Para ahondar en el análisis de este caso, es menester conocer a profundidad los factores que influyeron para que se llegara hasta tal punto.

El 15 de abril del 2007 el gobierno de Estonia decidió remover del centro de Tallin el monumento del soldado soviético de bronce conmemorativo de los soldados caídos durante la Segunda Guerra Mundial, lo cual generó un fuerte enfrentamiento diplomático con Rusia. En consecuencia, el 26 de abril comenzó el ataque cibernético a las 10: 00 pm. Al final de toda la primera semana todas las páginas web gubernamentales y de los diferentes partidos políticos habían sido bloqueadas. Para la segunda semana todos los medios de comunicación quedaron completamente desconectados, haciendo imposible que se le informara al mundo lo que estaba ocurriendo. El 9 de mayo a media noche ocurrió el ataque más fuerte. Los hackers desconectaron todo el sistema bancario, bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar. Durante tres semanas, los sitios web del gobierno, los bancos, medios de comunicación y todas las universidades fueron sistemáticamente atacados y desconectados. El 19 de mayo Los ataques se detuvieron y la primera ciberguerra llegó a su fin. Estonia inmediatamente acusó al gobierno de Rusia, pero nada ha podido ser demostrado (Ministerio de Defensa Nacional de España, 2009, p. 3)

Este caso pone al descubierto la vulnerabilidad de un Estado ante un ataque cibernético a las redes que se encuentran interconectadas, esto debido a la extensión del uso del internet y la dependencia a las infraestructuras tecnológicas e informativas. Las consecuencias de este tipo de agresión son nefastas, ya que ponen en riesgo el sistema bancario del Estado, los medios de comunicación y en general los epicentros que dan estabilidad a la nación.

Quizá el factor más importante a tener en cuenta, y como se dijo anteriormente, por la afectación y trascendencia, es la que se hace a la psicología del ser humano. Sí el ataque logra afectarla, el efecto será tan devastador que el Estado quedará indefenso, sin capacidad de respuesta y la sociedad se verá gravemente involucrada. Por ejemplo, un ataque a Wall Street que

afecte por un día sus operaciones, causaría la perdida de decenas de millones de dólares, pues la desconexión de ese día, generará desconfianza de la operación de inversiones bursátiles durante mucho tiempo para los inversionistas.

Al tener en cuenta que la atribución del ataque es casi imposible, el reto para el Estado es cada vez mayor, ya que le será difícil señalar a quien cometió el ataque pero sobretodo comprobarlo. Por tal razón, es de vital importancia considerar las amenazas ciberespaciales en las agendas de seguridad, sino en la totalidad, en gran parte de los países del mundo. Esta característica del ciberataque no le fue ajena a Estonia, quien pese a tener pruebas del origen del ataque, al tratar de involucrar a Rusia, no se pudo comprobar la participación del Gobierno. El gobierno Ruso afirmó que el ataque debió provenir de ciudadanos indignados, pero sin la participación del mismo.

> *Estonia dio a entender que pudo identificar algunos ataques a oficinas del gobierno ruso, pero no estableció de hecho ningún enlace gubernamental directo. Rusia mantuvo siempre que los ataques vinieron de cibernacionalistas renegados, que actuaban directo a su propio sentido de patriotismo deformado pero no por órdenes de ninguna oficina o agencia gubernamental oficial. Es más un testimonio de estados de percepción pública global que nadie hoy en día cree la versión rusa de los ataques y da por sentada la versión estonia –nunca hubo una prueba irrefutable que demostrara que la política gubernamental formal rusa fuera la culpable principal de los ataques estonios (Crosston, 2012, p. 27)*

Los daños trascendieron límites al vulnerar periódicos, teléfonos móviles, sistemas de respuesta de emergencia y el banco más grande del Estado. Además, un esfuerzo de ataque concentrado se apuntó a las oficinas del presidente, del primer ministro, del parlamento y del

ministerio de asuntos exteriores (Crosston, 2012, p. 27). Ante la escala de este tipo de ataques, es menester observar que el nivel de la amenaza es tal que pone de manifiesto la necesidad, no solo de mejorar la infraestructura para la ciberdefensa, sino, de tipificar estos ciberataques como acto de agresión para que se pueda considerar cualquier esfuerzo para tomar medidas defensivas o punitivas contra el agresor.

Posterior al ataque del 2007, Estonia dispone de una estrategia de seguridad publicada en mayo del 2008, en la que se plantea como objetivo reducir las vulnerabilidades de su ciberespacio a través de la implementación de los planes nacionales específicos (entre 2008-2013) y de la colaboración internacional (Romero, 2010, p. 289).

Las fronteras del ciberespacio vistas y analizadas a partir de casos como el de Estonia, son definidas como de fácil acceso, frágiles y porosas, vulnerables ante la perspicacia y capacidad de daño de cualquiera que tenga la facilidad de acceder a un computador y con un nivel necesario de conocimientos que le permita de la manera más cómoda y efectiva desarticular la base de un Estado hasta el punto de colapsar su infraestructura y afectar directamente a la población social, política y económicamente.

Ciberataque a Georgia

A su vez, es necesario analizar el caso del ciberataque a Georgia, siendo el primer caso en el que se combinan operaciones militares y operaciones cibernéticas. Al igual que el caso de Estonia, la Federación Rusa estuvo detrás de la coordinación de las ciber operaciones (Aguilar, 2010, p.330). Es un claro es un ejemplo de cibercampaña que apunta a un conflicto armado.

Para tal efecto deben tenerse en cuenta los antecedentes del ataque. El 7 de agosto de 2008 se inició la Guerra de Osetia del Sur entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia por el otro; con un ataque, que por sorpresa, realizaron las Fuerzas Armadas de Georgia contra

Fuerzas Separatistas. Este hecho provocó la reacción inmediata de Rusia, que consideró el hecho un ultraje contra ciudadanos rusos fuera de las fronteras y considero su obligación defenderles de tal ultraje. Al día siguiente, el 8 de agosto de 2008, los rusos iniciaron una serie de operaciones militares en territorio de Osetia del Sur, extendiéndose posteriormente a otras regiones de Georgia y al Mar Negro.

El 9 de agosto de 2008, el presidente de Georgia, Mikheil Saakashvili declaró el estado de guerra, al considerar los hechos acontecidos como una agresión Militar por parte de la Federación Rusa contra Georgia. Tres días más tarde, el 12 de agosto de 2008, el Presidente de la Federación Rusa, Dmitri Medvédev, decreta el fin de las operaciones militares rusas en territorio georgiano y acepta el plan de paz propuesto por la Unión Europea; plan que entre otras cosas obliga a las Fuerzas a volver a las posiciones anteriores al comienzo del conflicto (Ganuza, 2010, p 197).

Inicialmente se efectuaron ataques DDoS (ataque distribuido de denegación de servicios) de pequeña escala contra sitios web oficiales de Georgia, el primer ataque se registró en junio del 2008 en la fase del pre conflicto y en el marco de las tensas relaciones entre Rusia y Georgia. Para la fase del conflicto armado, los ataques fueron bien organizados y coordinados. Durante los cinco días que duró el conflicto armado se sucedieron ciberataques contra sitios web pertenecientes al Presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias.

A medida que el conflicto armado se intensificaba, incrementaba el número de ciberataques, los cuales debilitaron la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto; y debilitaron la capacidad de información y de comunicación entre el Gobierno y los ciudadanos. Además, a través de la ciberpropaganda,

trataron de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

Coincidiendo con la finalización del conflicto armado, el 12 de agosto de 2008, las operaciones cibernéticas sufrieron una importante reducción en número e intensidad pero el conflicto en el ciberespacio, parecía no estar incluido en el acuerdo de paz y las ciber operaciones continuaron hasta el 28 de agosto. El fin de las operaciones cibernéticas no se debió a ningún tipo de acuerdo, sino a la falta de rentabilidad de los ciberataques.

A diferencia del caso de Estonia, los ciberataques a Georgia tuvieron influencia directa en el desarrollo de las operaciones armadas y las redes sociales fueron usadas como elemento para reclutar voluntarios. El objetivo era provocar la pérdida de la capacidad operativa y de confianza en las instituciones políticas militares y financieras del país y bloquear la capacidad de comunicación entre dichas instituciones, Georgia y el mundo exterior. Los objetivos políticos se concretaron en los sitios web del Presidente de la República de Georgia, del Parlamento, del Ministerio de Asuntos Exteriores, del Ministerio de Ciencia y Educación, de Instituciones Educativas. Los objetivos militares se concretaron en los sitios web del Ministerio de Defensa. Los objetivos financieros se concretaron en los sitios web del Banco Nacional de la República de Georgia y de la mayor institución bancaria del país (TBC) Y los objetivos de comunicaciones se concretaron en los sitios web y foros de las principales agencia de comunicaciones, agencias de noticias y televisión (Ganuza, 2010, p 199).

Ciberataque a Estados Unidos

Otro ciberataque de gran relevancia es el caso de Estados Unidos donde se indica que los diferentes organismos expertos en la seguridad estadounidense, con frecuencia han acusado a China de hacer jaqueos masivos.

Aunque el argumento de China sea de carácter defensivo es importante resaltar uno de los ataques más importantes causados por este país, el cual se nombró Operación Titan Rain o Lluvia de Titanes. "Esta iniciativa fue puesta en práctica por el gobierno chino y el Ejército Popular de Liberación a partir del año 2002, con el fin de jaquear los sistemas informáticos gubernamentales y de industria nacional de países como Estados Unidos de Norteamérica y Alemania entre otros". (Gaitán, 2011 p. 11).

Lo que pretendía China era "extraer o desarrollar operaciones para controlar centros de almacenamiento de información clasificada gubernamental, estratégica e industrial de los Estados afectados" (Gaitán, 2011 p, 11). Los hackers de Titan Rain consiguieron tener acceso a varias redes informáticas estadounidenses, tales como: Lockheed Martin, Laboratorio Nacional Sandia, Redstone Arsenal y la NASA.

Los expertos en seguridad trabajaron bastante para detectar de donde provenían los jaqueos. Un ejemplo de ello fue, "Shawn Carpenter era un analista de seguridad para Sandia National Laboratories, donde buena parte del arsenal nuclear estadounidense es diseñado. Logró rastrearlos hacia la provincia sureña de Guangdong, en China". (Barrueto, 2009).

Esos sucesos ocurrieron en el 2002 y más adelante "estudios realizados al respecto en el 2007, concluyeron que mediante esta operación, China ya había logrado jaquear (piratear) más de veinte terabytes (1.024.000.000'000.000 Gigabytes equivalen a 1 Terabyte) de información prioritaria" (Gaitán, 2011, p.11). Por otro lado también se demostró que "un grupo de hackers chinos entrenados en el ciberespionaje, lograron descargar aproximadamente entre 10 y 20 terabytes de información sensitiva del Departamento de Defensa de Estados Unidos a través de Non-Secure Internet Protocol Router Network (NIPRNet). (Gaitán, 2012, p. 80). Es así que la

operación Titan Rain detectó como China adquiría información de toda índole, sin embargo vuelve a jugar el factor conocido como "atribución", debido a que no se logró demostrar la participación del gobierno chino en estas actividades.

A finales de la década de los 90, Estados Unidos acuso a China de infiltrar las instalaciones nucleares de Estados Unidos… China recluta y apoya a algunos de los piratas locales más brillantes, llamados "honkers". Los "honkers", en su descarado patriotismo virtual, creen en la filosofía de que la "mejor defensa es una ofensa capaz". No se consideraran ellos mismos empleados necesarios del gobierno ni miembros de la comunidad de inteligencia china; simplemente creen que China necesita protegerse de sus adversarios. (Crosston, 2012, p. 28).

Estas acciones son muy peligrosas, ya que las intenciones pueden afectar aspectos muy sensibles. La información que se filtró era privilegiada y secreta. De tal manera que "Titan Rain es una de las amenazas de ciberespionaje más invasivas que las redes estadounidenses han enfrentado, ya que han comprometido redes de comunicación de bastante importancia como algunos planes de vuelo del ejército. (Barrueto, 2009).

Ciberataque a Irán

Por último, el ciberataque a Irán se ejecutó en el año 2010 donde "la problemática del desarrollo del programa nuclear de Irán para los países occidentales y principalmente para Israel se recrudeció. Esto propicio el desarrollo del Ciberataque denominado por la comunidad científica como Stuxnet, el cual ha sido el arma virtual más compleja desarrollada hasta el momento para atacar la infraestructura critica del Estado". (Gaitán, 2011, p.13).

Se creó una ciber-arma denominada como Stuxnet la cual invadió los sistemas informáticos que controlan específicamente la infraestructura critica de Irán. Este viajó por el ciberespacio hasta llegar a los sistemas informáticos que controlan al reactor nuclear Bushehr instalación en dónde los servicios de inteligencia de otros Estados han denunciado, se encuentra el centro de operaciones del Gobierno de Mahmoud Ahmadinejad para la posible construcción de armamento nuclear. (Gaitán, 2011, p.13).

El Stuxnet se activó desde cada una de las computadoras en las cuales se había alojado anónimamente, y así el ataque fue perpetrado. El gusano, una vez inició su ofensiva, fue programado para que buscara específicamente los sistemas informativos que controlaban el comando y control reactor nuclear de Bushehr (Gaitán 2012, p, 83).

El ciberataque por medio del virus lo que logró fue "controlar el sistema de operaciones de la instalación, asumió el control de este y lo llevó a operar bajo comandos erróneos y desestabilizadores que ultimaron un daño tal, que el reactor no pudo ser puesto en actividad". (Gaitán, 2011, p.13). Vale aclarar que "Al igual que los casos europeos, las investigaciones efectuadas plantean a Estados Unidos e Israel como los posibles ejecutores del Stuxnet, no obstante, los dictámenes no son fiables y concretos en la actualidad" (Gaitán, 2011, p.13).

Es importante tener en cuenta que "según los análisis de las autoridades y sectores de defensa e inteligencia iraníes, el gusano, con la capacidad de reproducirse rápidamente por el ciberespacio y por terminales conectadas, entró a la red informática de Irán por medio de una (USB). Las Intenciones de crear esta arma, no solo ponen en alerta a países como Irán, ya que puede afectar a cualquier país. "El arma se difundió por la red mundial hacia miles de procesadores, que incluso se encontraban en países como India, China y Pakistán, y así dar espera

a la ejecución del ataque programado con el que se fue diseñado para afectar la infraestructura del Estado". (Gaitán 2012, p, 83).

Al final del ataque se puede constatar que, hasta el presente, el reactor todavía no ha podido ser inaugurado por el gobierno de Ahmadinejad. Desde un principio mantuvo como objetivo la infraestructura crítica nuclear iraní (Gaitán 2012, p, 83). Lo preocupante en este contexto es que con un ataque de estos pueda explotar algún reactor tan solo con oprimir un ENTER, afectando a miles de personas. La facilidad de los ciberataques permite crear una cantidad de hipótesis sobre esta nueva amenaza.

Experiencias que construyen

Es así que al analizar estos cuatro casos de tantos ciberataques que se dan regularmente, se puede inferir que la amenaza es real y que la afectación ha sido en todos los ámbitos políticos, económicos y sociales. La Ciberguerra que existe va más allá de la guerra convencional, no porque la guerra convencional se vaya a quedar atrás, sino porque la ciberguerra puede ser considerada por muchos Estados menos conflictiva y con maniobras orientadas a resultados directos y en centésimas de segundos. Otras agresiones además de la que fue víctima Estonia han sido analizadas por diferentes autores, como Myriam Dunn Cavelty quien en 2015 identifico métodos empleados y blancos atacados en diferentes hechos presentados en el ciberespacio.

Tabla 2. Agresiones de nivel internacional en el ciberespacio

EVENTOS REALES		
EVENTO	MÉTODO ATAQUE	BLANCOS
ESTONIA 2007	DEFACEMENT DE SITIO WEB DENEGACIÓN DE SERVICIO DISTRIBUIDA (BOTNETS)	GOBIERNO SECTOR PRIVADO MEDIOS DE COMUNICACIÓN
GEORGIA 2008	DEFACEMENT DE SITIO WEB ATAQUE DDOS	GOBIERNO SECTOR PRIVADO MEDIOS DE COMUNICACIÓN
UCRANIA 2013	DEFACEMENT DE SITIO WEB ATAQUE DDOS DATA DUMP CAMPAÑA Y PROPAGANDA DE DESINFORMACIÓN RUPTURA E INFILTRACIÓN DE INTERNET Y TRAFICO DE TELEFONÍA MÓVIL	GOBIERNO SECTOR PRIVADO MEDIOS DE COMUNICACIÓN
COREA - (SUR, NORTE) 2013	ATAQUE DDOS DEFACEMENT DE SITIO WEB MALWARE QUE BORRA EL REGISTRO PRINCIPAL DE ARRANQUE	SECTOR PRIVADO MEDIOS DE COMUNICACIÓN
GAZA 2014	DEFACEMENT DE SITIO WEB DATA DUMP ATAQUE DDOS EN SITIOS ISRAELÍES PHISHING DIRIGIDO	GOBIERNO SECTOR PRIVADO

Fuente: Adaptado del artículo "The normalization of cyber – International relations (Cavelty, 2015)

Los ciberataques dan oportunidades para camuflarse y lograr grandes éxitos económicos, políticos, diplomáticos y militares. "Haciendo un cálculo sencillo de costos-beneficios, la ciberguerra es mucho más económica que la guerra convencional, por lo que es discutible que su popularidad crezca exponencialmente con el tiempo" (Crosston, 2012, p. 28).

En conclusión, tras el conocimiento y análisis de los casos del presente capitulo, se puede inferir que la amenaza del ciberataque es una constante en la actualidad, que de manera sigilosa viene alterando la seguridad y defensa de los Estados. Ante tal eventualidad no hay cabida para ignorar tan especial amenaza, la cual se vuelve caldo de cultivo para terroristas, fanáticos, delincuentes, enemigos, entre otras amalgamas de sujetos que van en contra bien sea de un Estado o de un factor en particular. La tabla No.3 hace una caracterización de las amenazas que se pueden llegar a materializar a través de acciones en el ciberespacio.

Tabla 3: Caracterización de amenazas

NIVEL NACIONAL / INTERNACIONAL			
POSIBLES AUTORES	ATAQUES	TENDENCIAS	BLANCOS
CRIMINALES	CIBER ESPIONAJE	INFRAESTRUCTURA	GOBIERNO SECTOR PRIVADO MEDIOS COM. SECTOR DEFENSA
TERRORISTAS	RANSOMEWARE	DISPOSITIVOS MÓVILES (BYOD)	
HACKERS PATRIOTAS	DEFACEMENT	IoT (I.A. - DISP SALUD)	
GRUPO DE HACKERS	ROBO INFORMACIÓN	REDES SOCIALES	
HACKTIVISMO	DENEGACIÓN DE SERVICIO	CONFORMIDAD ESTATAL	
NACIÓN O ESTADO	ATAQUE DIRIGIDO	COMPUTACIÓN EN LA NUBE	
CRIMEN ORGANIZADO	ATAQUE KINETICO	BULLETPROOF HOSTING	

Fuente: (Forero, 2016). https://www.tlu.ee/en

La voluntad de los Estados se convierte en la pieza clave para enfocar el siguiente paso en esta lucha contra la impunidad cibernética, e impulsado por estas consecuencias producto de estos ciberataques históricos, no se debe dar espera a más factores que influyan en la necesaria respuesta de la comunidad internacional a tal afectación producto del ciberespacio.

Es así, como en varios países se han puesto en práctica estrategias militares para la protección y defensa del ciberespacio como un dominio de guerra. Es importante resaltar que dichas estrategias son relativamente recientes y se ajustan a las necesidades específicas de cada país; por lo cual estas pueden servir como modelo de referencia, sin embargo para el caso nacional se debe diseñar una que se ajuste a la situación actual y a los requerimientos que plantee el ciberespacio, especialmente dentro de los sectores relacionados con la infraestructura crítica cibernética.

La estrategia adoptada por Colombia deberá basarse en el desarrollo de grupos de capacidades que conlleven principalmente a prevenir, detectar, neutralizar y contrarrestar acciones maliciosas o ataques que se desarrollen en o a través del ciberespacio, poniendo en riesgo la seguridad nacional.

Como base de referencia para la consecución del objetivo de este trabajo, se sintetizan las estrategias que la investigación ha permitido identificar a nivel mundial, dentro del concepto de diseño de una metodología de ciberseguridad y ciberdefensa nacional, basada en el desarrollo de capacidades.

Tendencias mundiales

Actualmente existen países y organizaciones que han fortalecido sus capacidades cibernéticas, adoptando estrategias que permiten hacer frente a las diferentes amenazas en el ciberespacio; a continuación se presentará información sobre algunas de las más contundentes.

OTAN

La organización del Tratado del Atlántico Norte (OTAN), es una Alianza vinculada a la defensa de América del Norte con un conjunto de países de Europa Occidental, que reconoce el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado y está conformada por los países de Albania, Alemania, Bélgica, Bulgaria, Canadá, República Checa, Croacia, Dinamarca, Estados Unidos, Estonia, Eslovaquia, Eslovenia, España, Francia, Grecia, Hungría, Islandia, Italia, Letonia, Lituania, Luxemburgo, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, Rumania y Turquía. Esta alianza se ha organizado militarmente bajo unos parámetros estándar, que le permitirían en determinado momento lanzar operaciones que permiten hacer frente a amenazas comunes; el ciberespacio como un dominio de guerra nuevo, no es ajeno al planeamiento militar combinado[3], por lo cual esta organización adoptó una política mejorada contra la delincuencia cibernética, la cual requiere del desarrollo de actividades estratégicas y operacionales específicas y tácticas para todos los demás elementos.

[3] Operaciones Combinadas: Las que se llevan a cabo por fuerzas militares de dos o más naciones aliadas que actúan en conjunto para cumplir con una única misión.

Dicha estrategia se basa en 5 factores específicos, los cuales se constituyen en principales ejes de acción, ellos son:

Gobernanza en Internet – Ciberdiplomacia

Gobernanza de Internet se basa en una infraestructura de autorregulación, en que el internet creció ascendentemente con un mínimo de gobierno e influencia del sector público. En internet, voluntarios y expertos se organizan para impulsar la arquitectura y desarrollar el protocolo de internet en *selforganising*[4] con estructuras tales como la Junta de arquitectura Internet (IAB) o Internet Engineering Task Force (IETF). La parte del internet de seguridad cibernética es una de los temas tratados en la gobernanza de internet pero, a pesar de distintas iniciativas, no solo del cuerpo organizacional impulsa la tasa de progreso en seguridad, las principales áreas de actividad se relacionan con pro-acción/prevención, incluyendo la normalización de opciones de seguridad en los protocolos, el desarrollo de ciberseguridad especialmente diseñado protocolos, describir y estandarizar buenas prácticas tácticas operacionales.

Una de las más importantes organizaciones de gobernanza de internet es ICANN, este ente es responsable de coordinar las actividades para asegurar la funcionalidad del internet global, de enrutamiento y denominación de infraestructura. Una de sus principales funciones dentro del espectro de la gobernanza y seguridad de internet, es la lucha contra delitos como el conocido *Phishing*[5]. Estas acciones develan la estrategia acogida a nivel mundial donde cada vez

[4] Selforganising: Protocolo auto organizado, seguro y fiable para redes de sensores inalámbricas

[5] Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

más, una respuesta a Ciber ataques contra la infraestructura critica (en particular el encaminamiento de protocolos) puede requerir de una operación a nivel mundial.

Ciberdiplomacia, se considera aquí el compromiso de estado formal general de los procesos diplomáticos de una nación en el tema general de la seguridad cibernética global. En particular, esto se refiere a la actividad multilateral o bilateral dirigida a gestionar relaciones de estado para-estado en el ciberespacio. En el marco de las Naciones Unidas, para el caso del grupo de expertos gubernamentales (GGE) han estado trabajando en cuestiones de derecho internacional de los conflictos armados en el ciberespacio y actualmente están elaborando principios de normas y estándares de comportamiento aceptable estado.

Manejo de crisis y protección de infraestructura critica (CIP *por sus siglas en ingles*)

La gestión de crisis de la seguridad cibernética consta de al menos un área operacional y una función sobre todo táctica que abarca la preparación (por ejemplo, entrenamiento y ejercicios), respuesta, recuperación y cuidado del crecimiento/seguimiento de elementos del ciberseguridad incidente el ciclo de gestión. En el nivel táctico, un equipo nacional de respuesta a incidentes (CERT/CSIRT) se requiere que preferiblemente esté totalmente vinculado a la estructura de gerencia nacional del incidente de emergencia en el político estratégico.

Incidentes cibernéticos graves pueden conducir a grandes disturbios y alteración de la sociedad. Incidentes por ejemplo en sectores de infraestructura crítica (como de energía y telecomunicaciones) pueden tener un grave impacto a nivel nacional en el ciberespacio, por otra parte, la capacidad de gestión de emergencia/incidente nacional está estrechamente relacionada con la comunicación de crisis nacional, una función que viene en

práctica para comunicar a la sociedad y a la población sobre un incidente de ciberseguridad grave a nivel nacional.

Operaciones Militares Cibernéticas

Las funciones de ciberseguridad dentro del dominio militar difieren de nación a nación, como la definición exacta de las operaciones militares Ciber también será diferente. En general, este mandato puede incluir una gama muy amplia de los mandatos, no todos que sea aplicable en cada país. En primer lugar, esto incluye la Ciberdefensa – la protección de sus propios sistemas de las TIC, generalmente con un tipo CERT/CSIRT (equipo de respuesta de incidente de seguridad). En segundo lugar, puede incluir opciones de para las operaciones estratégicas Ciber – la posibilidad de una guerra cibernética sobre la lucha contra capacidad del enemigo. En tercer lugar, puede incluir campo de batalla cibernético capacidades – aquellas que se pueden implementar dentro de un campo de batalla operacional y táctico medio ambiente (por ejemplo de un sistema de defensa aérea enemigos).En cuarto lugar, puede incluir los esfuerzos de modernización de las capacidades militares más tradicionales, como los asociados con la guerra centrada en la red (NCW). Es importante tener en cuenta que el mandato puede no sólo ser nacional: una organización militar cibernético puede recibir un mandato para apoyar a los aliados de la nación (por ejemplo, dentro de la OTAN) en una extensión de su tarea de seguridad común. Aparte de Ciberdefensa (recuperación de preparación y respuesta), esto puede incluir también las capacidades de ataque preventivo contra una amenaza presente y contraataque (respuesta) o incluso un mandato capacidad ofensiva.

En caso de una emergencia nacional, algunas naciones tienen disposiciones legales para que los militares puedan ayudar en la gestión de emergencias y proveer seguridad interior. Por lo tanto, algunas de las capacidades de seguridad cibernética militar pueden ser para proteger

el ciberespacio de la patria en caso de que la respuesta a la crisis normal agote sus recursos para hacer frente a una crisis de seguridad cibernética. Sin embargo, la cadena operacional/táctica y control de la capacidad de Ciber militar siempre es generalmente subordinado a las autoridades de respuesta civil.

Contrainteligencia

Distinguir espionaje cibernético, desde el crimen informático y ciber actividades militares actividades no es incontrovertible. De hecho, todos dependen de vectores similares de ataque y tecnología similar. En la práctica, sin embargo, casos graves de espionaje (ambos sobre la propiedad intelectual secretos de gobierno) están en una clase propia. Al mismo tiempo, puede ser muy difícil determinar con certeza si el autor es un estado o un grupo criminal operando en nombre de un estado, o de hecho intervenir en nombre propio.

Independientemente de quién está realmente detrás del ataque, Ciber espionaje representa probablemente la parte más perjudicial de la Ciber delincuencia (si está incluido en la categoría). Ciberespionaje, cuando se dirige hacia los Estados, también hace que sea necesario desarrollar política exterior con específicos mecanismos de respuesta capaces de contrarrestar cualquier ataque de naturaleza. Al mismo tiempo, las actividades de contrainteligencia por ejemplo (detección y lucha contra las intrusiones de Ciber más sofisticadas) muy a menudo dependerán de otros tipos de actividad de la inteligencia ofensiva sino también extenso intercambio de información entre socios internacionales.

Contra – cibercrimen

El mandato contra-cibercrimen se compone de un conjunto amplio de organizaciones. En los niveles de políticas y estrategias, el Ministerio de Justicia participa en el plano nacional y a

menudo internacional, en el desarrollo y mantenimiento de la legislación de seguridad Ciber. Del mismo modo, el Ministerio del interior a menudo gestionará los recursos de la policía. A diferencia de otros mandatos, sin embargo, algunas de estas capacidades residen a nivel gubernamental y no sólo en la responsabilidad del gobierno central de prevención del delito cibernético es un problema multi-ángulo. Desde la perspectiva económica, asuntos del Ministerio de economía pueden administrar conciencia en seguridad cibernética en los niveles y desarrollo de programas operativos contra el delito cibernético. Tenga en cuenta que este se superpone con la educación. Desde la perspectiva de gobierno, seguridad del estado y Ciber prevención del delito es una cuestión organizativa en todos los Departamentos de gobierno y agencias. En la actualidad, las Naciones cada vez más asignan esta responsabilidad estratégica y operativa a un jefe de seguridad informática (CIO o CISO) que tiene que desarrollar, mantener y supervisar la seguridad de la información y cibernética de todo el gobierno y las políticas.

Desde el punto de vista de asegurar la provisión de servicios al público en general, organizaciones no gubernamentales de servicio como ISP pueden activamente interrumpir la propagación de malware y otras actividades delictivas cibernéticas.

Para poder afrontar las amenazas cibernéticas que se presenten dentro de las líneas de acción anteriormente mencionadas, se hace indispensable desarrollar grupos de capacidades que permitan contar con unos elementos clave para enfrentar amenazas cibernéticas, estos elementos son:

Pro – acción

Se define como las actividades que reducen o eliminan las causas estructurales de la inseguridad. Pro acción comprende llevar a cabo una evaluación del riesgo nacional (NRA) para

el dominio del ciberespacio, establece un marco jurídico para la seguridad cibernética y un marco organizativo.

Prevención

En un contexto de gestión de emergencias esto se ha definido como acciones para evitar, intervenir o impedir que un incidente se produzca. Para el propósito aquí usamos una definición ligeramente distinta: acciones para prevenir riesgos que se conviertan en conjunto de incidentes o para reducir los efectos de posibles incidentes. Las medidas de seguridad preventivas Ciber reducirán la vulnerabilidad del ciberespacio global y NCS individuales en particular.

Preparación

Se define como "la planificación, capacitación y ejercicio" o como "un ciclo continuo de la planificación, la organización, el entrenamiento, el equipamiento, el ejercicio, evaluar y tomar acción correctiva en un esfuerzo por garantizar la coordinación eficaz de respuesta a incidentes.

Respuesta

Aborda los efectos inmediatos y a corto plazo y además previene el daño después de que ocurre un incidente.

Recuperación

Esto abarca actividades y programas realizados durante y después de la respuesta que están diseñadas para devolver a la entidad a su estado habitual o a uno normal.

Acciones posteriores y seguimiento

Tiene en cuenta el impacto psico-sociológico de un incidente (partes de) la población, cubre incidentes y gestión de incidencias investigación (como el hallazgo de hecho y de la escritura de lecciones identificadas), así como análisis forense, investigación criminal y la persecución de los sospechosos.

La gestión de incidencias de seguridad proviene del entendimiento de las lecciones identificadas durante la preparación (a través de acciones posteriores y seguimiento) las cuales se convierten en lecciones aprendidas. Posteriormente se adaptan como una estrategia y política (acción pro), para sentar las bases en la prevención o revisar medidas y enfoques, para ayudar a desarrollar e implementar las medidas de preparación nuevas o modificadas (p. ej. Programa de ejercicios), o puede ser útilmente empleada para implementar y capacitar, cambiando procedimientos y procesos que forman parte del elemento de respuesta a incidente del ciclo.

Cada uno de estos elementos influye sobre las líneas de acción como se muestra a continuación:

Figura 1 - Relación entre elementos y mandato (Alexander Klimburg (Ed.), 2012)

Fuente: Alexander Klimburg (Ed.). (2012). *National Cybersecurity Framework Manual.* Tallin,

Estados Unidos

En coordinación con otras agencias del Estado, el Departamento de Defensa es el responsable de defender la seguridad y los intereses de la Nación de ataques, incluyendo aquellos que pueden ocurrir en el ciberespacio. De una forma consistente con las normas nacionales e internacionales, el Departamento de Defensa procura detener ataques y defender a Estados Unidos de adversarios que pretendan dañar sus intereses nacionales en tiempos de paz, crisis o conflicto.

Es así como en 2011 el Departamento de Defensa diseña y pone en ejecución la guía de operaciones en el ciberespacio la cual se concentra en desarrollar las capacidades necesarias desarrollar acciones de Ciberseguridad y ciberoperaciones efectivas que permitan defender las redes, sistemas e información del Departamento de Defensa, proteger a la nación de ciberataques de gran impacto y apoyar los planes de operaciones y de contingencias.

El departamento que dedica su esfuerzo dentro del gobierno federal de los Estados Unidos para lograr este objetivo es "ciberseguridad", y este debe operar en coordinación con otros departamentos y agencias, socios y aliados internacionales, Estados y gobiernos locales, y lo más importante, el sector privado, desarrollando tres actividades principales:

Intercambio de información y coordinación interagencial

Con el fin de asegurar y consolidar los intereses de Estados Unidos en el ciberespacio, el Departamento de Defensa procura compartir los conocimientos y coordinar con las agencias del

gobierno de forma integrada en una amplia gama de actividades. Una de las más recurrentes es cuando el Departamento de Defensa detecta actividades cibernéticas maliciosas que pueden afectar importantes redes y sistemas vitales para la seguridad nacional, económica y pública. En esta situación el Departamento de Defensa apoya a otras agencias como el FBI o el Departamento de Seguridad Nacional u otras entidades interesadas, así como a otros países mediante el intercambio de información, indicadores técnicos o potenciales ataques.

De esta forma el intercambio de información puede mejorar significativamente la capacidad para que una organización de pueda defender a si misma contra una gran cantidad de ciber ataques. Adicionalmente esta actividad permite la sincronización de operaciones, la realización de lecciones aprendidas y el diseño de mejores prácticas de Ciberseguridad. Esto incluye el manejo de incidentes y la respuesta de los equipos de defensa de redes.

Construir puentes de comunicación con el sector privado

Desde desarrolladores de aplicaciones hasta proveedores de servicios de internet, las compañías privadas producen los bienes y servicios que componen el ciberespacio. El Departamento de Defensa trabaja con el sector privado para construir estas redes, proveer servicios de ciberseguridad e investigas y desarrollar capacidades avanzadas. El Departamento de Defensa se ha beneficiado del sector privado a través del tiempo. Hacia el futuro, este seguirá trabajando cercanamente al sector privado con el fin desarrollar y comercializar nuevas soluciones de ciberseguridad que permitan la protección de los intereses de Estados Unidos.

Construcción de alianzas, coaliciones y convenios en el exterior.

El Departamento de Defensa está comprometido con el desarrollo de una amplia gama de actividades orientadas a mejorar la seguridad cibernética y la capacidad de desarrollar operaciones cibernéticas en el exterior. Por esta razón la estrategia de ciberseguridad de los Estados Unidos concibe la actividad de prestar ayuda a sus aliados para entender las amenazas a las que se enfrentan y para construir las capacidades necesarias que les permitan defender sus redes y su información. De la misma forma los aliados de Estados Unidos y los convenios que se logran establecer, son una fuente de ayuda que ha permitido complementar capacidades de ciberseguridad y aumentar las propias de Estados Unidos, las cuales son empleadas en el diseño de estrategias y la cimentación de coaliciones para contrarrestar actividades cibernéticas de potenciales adversarios. Desde el punto de vista estratégico, esta forma de trabajo en equipo que bien puede ser descrita como una coalición unificada, envía el claro mensaje de que Estados Unidos está alineado junto con sus aliados en una operación colectiva de defensa en el ciberespacio.

La estrategia establece principios y procesos que buscan ejercer gobierno en el proceso de planeamiento, desarrollo y del uso de las capacidades de forma efectiva, además busca asegurar que las ciberoperaciones sucedan de forma legítima cumpliendo con los valores que Estados Unidos promulga nacional e internacionalmente. De esta manera, el Departamento de Defensa cumple tres misiones principales en el ciberespacio: defender sus propias redes, sistemas e información, estar preparado para defender a los Estados Unidos y sus intereses contra ciberataques de consecuencias significativas y por último, bajo las instrucciones directas del

Presidente o del Secretario de Defensa, debe proveer capacidades cibernéticas orientadas a soportar las operaciones militares convencionales y los planes de contingencia.

Por último, el Departamento de Defensa se planteó cinco objetivos estratégicos a cumplir con el desarrollo de misiones en el ciberespacio.

- Crear y tener en permanente alistamiento unidades y capacidades para conducir operaciones en el ciberespacio.
- Defender la red del Departamento de Defensa, asegurar sus datos, y mitigar los riesgos de las misiones.
- Estar preparado para defender la seguridad interna y los intereses de Estados Unidos de un ataque cibernético disruptivo o destructivo, con importantes consecuencias en el funcionamiento del Estado.
- Diseñar y mantener cursos de acción viables en el ciberespacio y planear la forma de usar estas opciones para controlar el escalamiento del conflicto cibernético o convencional y para dar forma al entorno del conflicto en todas sus etapas.
- Construir y mantener sólidas alianzas y asociaciones internacionales para disuadir las amenazas comunes, así como para aumentar la seguridad y la estabilidad internacional.

España

España al igual de la mayoría de los países, ha motivado su empeño en desarrollar estrategias de ciberdefensa en los hechos que ocurrieron en Estonia durante el año 2007, sin embargo a diferencia de otras naciones, esta ha enfocado su esfuerzo principal en la generación de la base legal que permite desarrollar las acciones en el ciberespacio de forma legítima.

Es así como en la actualidad han regulado este tema en profundidad mediante normas como las leyes recogidas en la "Guía Legal de Respuesta Jurídica frente a los Ataques contra la Seguridad de la Información" publicada por Inteco, en la que se relacionan las amenazas, las medidas de protección y las medidas legales relativas a los ataques, o el conjunto de artículos del código penal y leyes que tratan de manera directa o indirecta el tema del terrorismo. Por otro lado, en cuanto a los principales planes y estrategias relacionados con la seguridad nacional y la ciberdefensa, los más destacados son los siguientes:

- Directiva de Defensa Nacional de 2004.
- Plan Nacional de Protección de las Infraestructuras Críticas.
- Desarrollo del Centro de Alerta Temprana Antivirus (CATA).
- Desarrollo de diversos CERT´s (públicos y privados).
- Esfuerzos realizados por el CCN para la mejora de la seguridad de la información en la Administración Publica.
- MoU del 14 de mayo de 2008 para la participación de España en el Centro de Excelencia de Ciberdefensa Cooperativa.

Con una base legal fuerte y sustentada, España integró y delegó responsabilidades a diferentes organismos del Estado, generando un sistema de participación proactiva para la atención de los incidentes cibernéticos que atentan contra su población y sus infraestructuras críticas, así:

Ministerio del Interior: Tiene asignadas, entre otras, las siguientes responsabilidades:

- La preparación y ejecución de la política del Gobierno en con la administración general de la seguridad ciudadana.
- La promoción de las condiciones para el ejercicio de los derechos fundaméntales, especialmente en relación con la libertad y seguridad personal, en los términos establecidos en la Constitución Española y en las leyes que los desarrollen.
- El mando superior, la dirección, y la coordinación de las Fuerzas y Cuerpos de Seguridad del Estado.
- El ejercicio de las competencias legalmente atribuidas sobre protección civil.

Dentro del Ministerio del Interior, existen diversos grupos o unidades relacionadas con actividades de Ciberdefensa entre los que destacan:

La Dirección General de Infraestructuras y Material de Seguridad que es el órgano encargado de desarrollar el Plan Nacional de Protección de Infraestructuras Críticas.

Grupo de Delitos Telemáticos de la Guardia Civil, cuya misión encomendada es la de llevar a cabo todas aquellas investigaciones relacionadas con la delincuencia informática que le encomienden las Autoridades judiciales, o que conozca por comunicaciones y denuncias de los ciudadanos, que por su importancia o relevancia social, dificultad técnica o número de afectados, aconsejen la dedicación de los recursos materiales y humanos más técnicos de la Guardia Civil.

Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, destinada a responder a los retos que plantean las nuevas formas de delincuencia como son la pornografía infantil; estafas y fraudes por Internet; fraudes en el uso de las comunicaciones; ataques cibernéticos; piratería, etc.

Su misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unos y otros a disposición judicial. Para poder desarrollar su labor, las herramientas" que utilizan son: la formación continua de los investigadores; la colaboración con instituciones públicas y privadas; la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana.

El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia, es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifrado, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la administración especialista en este campo.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), promovido por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. Este Instituto desarrolla, entre otras, iniciativas de seguridad tecnológica, accesibilidad e inclusión en la sociedad digital y soluciones de comunicación para particulares y empresas.

Dentro del ámbito de ciberdefensa, España participa activamente en el Centro de Excelencia de Ciberdefensa Cooperativa ("*Cooperative Cyber Defence Centre of Excellence*", CCD COE) que la OTAN ha establecido en Tallín, Estonia, tras la firma del MoU del 14 de mayo de 2008.

El CCD COE es una organización multinacional que proporciona Investigación, desarrollo y servicios de formación a la OTAN, entre otras cosas. Está abierto a la participación de todos los miembros de la OTAN y además puede firmar acuerdos con organizaciones ajenas a la OTAN, como universidades, empresas, etc.

En la actualidad España participa en esta organización ocupando el cargo de Jefe de Entrenamiento y Doctrina, centrando su trabajo en las siguientes áreas fundamentales de la Ciberdefensa:

- Desarrollo de doctrinas y conceptos.
- Formación y concienciación.
- Investigación y desarrollo.
- Análisis y lecciones aprendidas.
- Consulta

Tendencias regionales

Brasil

La estrategia de seguridad de información y comunicaciones, y de seguridad cibernética *(Estratégia de Segurança da Informação e Comunicações e da Segurança Cibernética)* de la administración pública federal de Brasil, está vinculada a una amplia estructura del planeamiento general estratégico del gobierno de Brasil.

Esta estrategia se desarrolla en el marco de la instrucción normativa GSI/PR No 01/2008 del gabinete de seguridad institucional de la Presidencia de la Republica, mediante la cual se busca desarrollar mejores prácticas en el área de seguridad de la información y ciberseguridad, y las principales metas y objetivos estratégicos a alcanzar en el año 2018 llegando a ser estos la base de las acciones futuras y especificas en el área de ciberdefensa. Algunas de las recomendaciones y cursos de acción que define esta estrategia son:

- Todas las políticas públicas desarrolladas alrededor de la ciberseguridad y la seguridad de la información, deben estar abiertas a amplias discusiones que sean comprensibles para todas las partes interesadas. Estas propuestas deben tener en consideración todos los parámetros legislativos relevantes establecidos tanto a nivel nacional, como en las normas internacionales.
- El respeto a los derechos humanos, especialmente al derecho de la libre expresión y la protección de la privacidad, deben ser incorporados en el conjunto de principios y objetivos que orientan la estrategia.
- Se deben introducir y desarrollar directrices para las discusiones multisectoriales que lleven a decisiones de políticas nacionales en seguridad de la información y ciberseguridad.

- Cualquier entrenamiento o programa de formación en el área, no debe dar una importancia desproporcionada a la defensa de la soberanía nacional, el entrenamiento debe ser debidamente alineado con el respeto de los derechos humanos, las necesidad de transparencia y/o al acceso de la información.

El ciberespacio junto con las amenazas nucleares y aeroespaciales, fueron señaladas por esta estrategia como tres de las áreas más estratégicas que requieren ser protegidas. A pesar que el concepto de ciberseguridad no cuenta con una definición clara a nivel internacional, la estrategia de Brasil incluye otros conceptos parcialmente similares que cuentan con connotación militar como ciberdefensa, seguridad de tecnologías de la información y prevención de cibercrimen.

Es así como las Fuerzas Armadas de Brasil han venido fortaleciendo el concepto de seguridad en el ciberespacio orientado a la protección del país contra ataques cibernéticos. Para ello, en septiembre de 2012 Brasil creo el centro de defensa cibernética (CDCiber) y el centro de comunicación social del Ejército de Brasil, delegándoles la responsabilidad de coordinar e integrar las actividades de defensa cibernética bajo la supervisión del Ministerio de Defensa, desde donde el CDCiber afronta todas las actividades de protección del ciberespacio junto a los 200 miembros que hacen parte de las tres ramas de las Fuerzas Militares (Ejército, Armada y Fuerza Aérea), y otras agencias de seguridad.

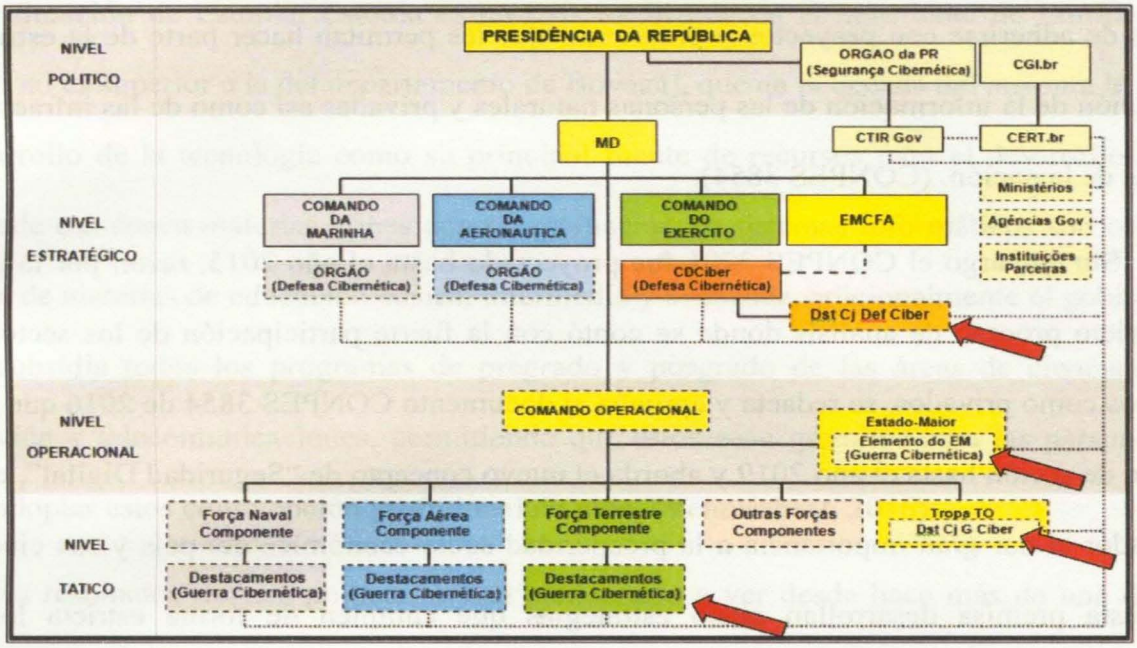
En general la doctrina de defensa cibernética de Brasil, reconoce cinco capacidades en la estructura de operaciones de información como lo son inteligencia, cibernética, operaciones de apoyo a la información, comunicación social y guerra electrónica, que deben ser tenidas en cuenta en los niveles de planeamiento y conducción de las operaciones militares como se muestra en la siguiente gráfica.

Figura 2 - Estructura de operaciones de información (Article 19, 2016)

Fuente: *Análise da Estratégia de Cibersegurança.* São Paulo.

Por último, el concepto del sistema de mando de defensa cibernética concibe la existencia de entes que cumplen funciones para la seguridad del ciberespacio en todos los niveles de planeamiento, encontrando un órgano de ciberseguridad de la Presidencia de la Republica como mayor ente coordinador del País, compuesto por los diferentes equipos de respuesta a incidentes informáticos (CERT) de las organizaciones públicas y privadas. En el nivel estratégico se encuentran órganos de ciberdefensa en cada uno de los comandos de las fuerzas militares. El estado mayor de guerra cibernética está localizado en el nivel operacional donde se evalúan los cursos de acción a seguir para enfrentar las amenazas cibernéticas, se definen los objetivos militares y se toman decisiones de procedimiento. Finalmente, en el nivel táctico se crearon destacamentos de guerra cibernética en cada uno de los componentes Naval, terrestre y Aéreo encargados del desarrollo de las operaciones de información, como se muestra en la siguiente gráfica.

Figura 3 - Sistema de mando de defensa cibernética (Article 19, 2016)



Fuente: *Análise da Estratégia de Cibersegurança.* São Paulo.

Visión nacional

Entre otros, los eventos internacionales descritos en el capítulo anterior llamaron la atención del Estado Colombiano llevándolo a tomar iniciativas que le permitieran fortalecer la capacidad de proteger a sus ciudadanos contra los delitos informáticos y la infraestructura crítica digital del país.

Es así como en el año 2011, Colombia redacta la primera iniciativa oficial para hacer frente a las nuevas amenazas emergentes que se sustentan en la constante y rápida evolución de la tecnología, esto lo hace a través del documento conocido como Consejo Nacional de Política Económica y Social (CONPES 3701/2011), con el cual se emitieron los lineamientos para la política de ciberseguridad y ciberdefensa del Estado. Como resultado de esta iniciativa, hoy el

país cuenta con entidades que cumplen funciones específicas orientadas a la seguridad y defensa nacional en el ciberespacio, adicionalmente sembró en las entidades públicas y privadas el interés de adherirse con proyectos y programas que les permitan hacer parte de la estructura de protección de la información de las personas naturales y privadas así como de las infraestructuras críticas de la nación. (CONPES 3854).

Sin embargo el CONPES 3701 fue proyectado hasta el año 2015, razón por la cual bajo un estricto proceso de análisis donde se contó con la fuerte participación de los sectores tanto públicos como privados, se redacta y aprueba el documento CONPES 3854 de 2016 que proyecta su plan de acción hasta el año 2019 y aborda el nuevo concepto de "Seguridad Digital", el cual es innovador al dar gran importancia a la prosperidad socio-económica del país y sus ciudadanos. Bajo esta premisa desarrollan cinco estrategias que cumplen de forma estricta los cuatro principios rectores que se formulan en ese documento, estos son: Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos, adoptar un enfoque incluyente y colaborativo, asegurar una responsabilidad compartida y adoptar un enfoque basado en la gestión de riesgos. (CONPES 3854).

Aunque las estrategias desarrolladas en el CONPES 3854 son aplicables en el escenario actual, se realizara una nueva revisión y actualización en el año 2019. Por otro lado, esta política al igual que la desarrollada por su antecesora sigue siendo muy pasiva, lo cual no disminuye su viabilidad para la obtención de los objetivos propuestos, pero si limita fuertemente la capacidad de desarrollo e innovación a corto, mediano y largo plazo del Estado.

En primer lugar, a pesar que la política acoge el área de formación de los ciudadanos en todos los niveles académicos, esta se limita estrictamente al conocimiento de las amenazas en el ciberespacio y a los procedimientos que se deben realizar para detectar, prevenir y actuar ante los

incidentes o delitos ya presentados, mas no una educación orientada a inculcar en las nuevas generaciones la cultura del desarrollo y empleo de la tecnología, como ejemplo de esto se puede tomar la situación de Estonia. Estonia es un país localizado en el nororiente de Europa (cuya extensión no es superior a la del departamento de Boyacá), que en la década del noventa le aposto a el desarrollo de la tecnología como su principal fuente de recursos para el desarrollo, es así como desde esa época materias afines con programación de sistemas informáticos son comunes en el plan de materias de educación básica, intermedia y avanzada, adicionalmente el gobierno de Estonia subsidia todos los programas de pregrado y posgrado de las áreas de ciencias de la computación y telecomunicaciones, permitiendo que estos sean gratuitos para las personas que deciden adoptar estos como opción profesional de vida. (Venturebeat, 2016).

Los resultados de esta política se han comenzado a ver desde hace más de una década, grandes aplicaciones como Skype fueron desarrolladas en ese país, esto sumando a que actualmente es un gobierno completamente electrónico donde cada uno de sus ciudadanos pueden acceder a los servicios provistos por este de forma rápida y segura a través de tarjetas de identificación (cedulas) electrónicas, además de hacer transacciones con el Estado u organismos privados sin limitación de tiempo o espacio. (e-estonia.com)

Segundo, la política de Estado orientada al desarrollo de sistemas de computación ha llevado a las diferentes generaciones de estonios a dominar el idioma lógico usado para la programación, siendo este la base del desarrollo de las aplicaciones informáticas, esto facilita la implementación de una política de desarrollo de sistemas de seguridad digital propio, no como lo propone el CONPES objeto de este análisis donde se superpone la adquisición de toda la tecnología requerida para dar forma a las estrategias y líneas de acción planteadas en la política de seguridad digital.

En conclusión, la orientación de la política de seguridad digital se ha concebido bajo la perspectiva de un escenario reactivo donde una vez se presenta el incidente, se toma la acción correctiva, coercitiva y de recuperación mediante el modelo de gestión de incidentes que debe ser presentado por el Coordinador Nacional de Seguridad Digital bajo la tutoría del Departamento Nacional de Planeación.

Por otro lado, la adopción de una perspectiva en la que a mediano y largo plazo el país cuente con un recurso humano especializado y sobretodo completamente inmerso en el idioma digital de programación abrirá la puerta a la multiplicación del desarrollo de tecnologías con patente nacional, optimizando la inversión de recursos y llevando los productos colombianos al mercado internacional.

CAPÍTULO III

Operaciones militares en el ciberespacio; capacidades de ciberseguridad y ciberdefensa para las fuerzas militares

Pensar en que una fuerza militar deba incursionar en el ciberespacio para generar estabilidad y seguridad en las infraestructuras críticas que hoy en día soportan sus operaciones en él, no es una idea nueva. La militarización del ciberespacio ha sido un tema profundamente tratado en escenarios políticos internacionales, por ende la pregunta correcta en este caso es, ¿Cómo hacerlo?

Lo primero y más importante es definir cuáles van a ser las capacidades que una fuerza militar legítima, requiere para enfrentar los retos que día a día se le presentaran en el ahora conocido *quinto dominio de la guerra*. Para ello dentro de la hoja de ruta de las Fuerzas Militares, no se encuentran articuladas de manera conjunta las capacidades de ciberseguridad y ciberdefensa de Ejército, Armada y Fuerza Aérea, teniendo como consecuencia esfuerzos aislados, falta de estandarización de técnicas, tácticas y procedimientos, fallas en el planeamiento de los recursos para licenciamiento y compras de equipos.

Sin embargo, desde el año 2014, la política de seguridad y defensa del Estado Colombiano "Todos por un nuevo país", recoge una serie de objetivos e iniciativas que propenden por la optimización de los recursos y empoderan a las fuerzas militares para que desarrollen las capacidades que sean necesarias con el fin de hacer frente a las nuevas expresiones del crimen organizado y el terrorismo, así como proteger las infraestructuras criticas cibernéticas de la nación.

Política de seguridad y defensa del Estado Colombiano "Todos por un nuevo país"

Objetivo No. 4

Combatir las nuevas y tempranas expresiones de crimen organizado que amenacen la seguridad y el funcionamiento transparente del Estado, garantizando el control territorial y usando todas las capacidades de la Fuerza Pública.

Estrategia 4.4

Fortalecer las estrategias de lucha contra el terrorismo, así como los Centros de Operaciones Especiales para la Protección de la Infraestructura (COPEI) existentes con medios y personal y crear nuevos COPEI donde sea requerido.

Objetivo No. 5

Garantizar la soberanía e integridad del territorio nacional, protegiendo los intereses nacionales.

Estrategia 5.8

Formular un plan para la consolidación y fortalecimiento del Comando Conjunto Cibernético (CCOC) quien además tendrá que identificar y catalogar la infraestructura crítica digital que permita terminar el mapeo de la misma y establecer los planes de protección para esa infraestructura, objetivos, alcances, prioridades y roles.

Siguiendo la senda proyectada por el gobierno nacional, las fuerzas militares desarrollaron en el año 2014 un tanque de pensamientos que entre otros, género como producto una serie de objetivos estratégicos a ser logrados en el año 2030, y estableció las iniciativas estratégicas para ejecutar en el periodo de gobierno actual, estas últimas serán la base sobre la que se soportaran las capacidades cibernéticas, entre otras, que el brazo armado del Estado debe desarrollar para la defensa y protección del mismo.

Objetivos Estratégicos 2030 e Iniciativas Estratégicas 2015-2018 de las Fuerzas Militares de Colombia.

Objetivo Estratégico No. 2

Alcanzar y mantener la superioridad en todas las operaciones a través de la integración de las capacidades militares.

Objetivo Específico 2.3

Adquirir la superioridad militar en el ciberespacio a través de la integración de las capacidades de Ciberseguridad y Ciberdefensa de las FF.MM.

Iniciativas:

2.3.1 Desarrollar y fortalecer las capacidades de defensa, explotación, respuesta y resiliencia frente a las amenazas cibernéticas.

2.3.2 Realizar vigilancia tecnológica para estar acorde con el contexto estratégico global.

Objetivo Estratégico No. 5

Contribuir al desarrollo sostenible del país mediante el empleo de capacidades militares.

Objetivos Específicos 5.1

5.1 Apoyar a las entidades del Estado y a las Comunidades empleando las capacidades miliares.

Iniciativas:

5.1.3 Contar con un conjunto de procedimientos estandarizados para el empleo de las capacidades militares.

Bajo el fundamento político y organizacional sustraído de los textos de planeamiento estratégico nacional y militar vigentes, las fuerzas militares buscan desarrollar, ampliar y fortalecer las capacidades de ciberseguridad y ciberdefensa del Comando Conjunto Cibernético (CCOC) y las Unidades Cibernéticas de las Fuerzas Militares en el periodo 2016 – 2022, garantizando el direccionamiento estratégico a través de personas, procesos, plataforma tecnológica operativa, que permita responder con prontitud a la amenaza cibernética que pone en riesgo la integridad territorial, la independencia, la soberanía y el orden constitucional.

Para ello se requiere que las capacidades a desarrollar estén orientadas a tener componentes como:

Establecer el sistema de Comando y Control para el desarrollo de las operaciones de Ciberseguridad y Ciberdefensa de las Fuerzas Militares en los niveles estratégico, operacional y táctico.

Desarrollar y fortalecer capacidades estratégicas de inteligencia y contrainteligencia en el ciberespacio a través de la recolección, análisis, procesamiento y difusión de información.

Planear, conducir y desarrollar operaciones conjuntas, coordinadas, combinadas e interagenciales en el Ciberespacio, para el cumplimiento de la misión constitucional de las Fuerzas Militares.

Desarrollar y fortalecer los recursos logísticos que permitan la consolidación de las capacidades del Comando Conjunto Cibernético y las Unidades Cibernéticas de cada una de las Fuerzas.

Fortalecer el marco jurídico y la doctrina institucional que soporten el desarrollo de operaciones de Ciberseguridad y Ciberdefensa a fin de contribuir a garantizar la legitimidad del accionar de las Fuerzas Militares en el Ciberespacio.

Fortalecer los procesos de gestión del talento humano en Ciberseguridad y Ciberdefensa, con el propósito de garantizar el cumplimiento de la misión.

Establecer estrategias que permitan desarrollar planes y programas de capacitación y entrenamiento para el personal que conforma el Comando Conjunto Cibernético y las Unidades Cibernéticas de las Fuerzas Militares.

Desarrollar capacidades, establecer estrategias y estructuras adecuadas que permitan dirigir y coordinar las acciones de los involucrados en materia de protección y defensa de infraestructuras críticas cibernéticas.

Fomentar y fortalecer la investigación, desarrollo e innovación (I+D+i) en Ciberseguridad y Ciberdefensa en las Fuerzas Militares, buscando concentrar esfuerzos en

desarrollo de nuevas capacidades humanas y tecnológicas que permitan el desarrollo de la industria militar en materia cibernética aportando a su auto sostenibilidad y autonomía.

Sistema por capacidades

El manual de Ciberdefensa Conjunta para las Fuerzas Militares FFMM 3-18 Restringido, establece las capacidades especificas operacionales que deben desarrollar las fuerzas militares para la ejecución de operaciones militares en el ciberespacio, así mismo, procura que las capacidades queden organizadas por áreas de capacidad denominadas como Ciberseguridad y Ciberdefensa, que hacen parte del sistema de capacidades Cibernético. La figura No. 4 permite observar de forma gráfica el diagrama de bloques que define al sistema cibernético.

Figura 4. Sistema de capacidades cibernéticas.

Fuente: (Fuerzas Militares de Colombia, 2017).

Como se observa en la figura anterior, las áreas de capacidad están compuestas por las capacidades específicas que le dan el enfoque operacional a las unidades que desarrollan operaciones militares en el ciberespacio, cada una de ellas conlleva el desarrollo de actividades

definidas, es así como en el área de capacidad de Ciberseguridad encontramos las siguientes actividades:

Defensa pasiva:

1. Sensibilización.
2. Detección y análisis de ataques cibernéticos.
3. De aseguramiento de redes y sistemas.
4. De Evaluación de Infraestructura.
5. De Análisis y Evaluación de Vulnerabilidades.
6. De apoyo a la gestión de Infraestructura.
7. De visibilidad y Seguimiento.
8. Análisis y Evaluación de Código.
9. Análisis y Gestión de Riesgos.

Gestión de incidentes cibernéticos:

1. Análisis de Incidentes.
2. Respuesta a incidentes en sitio.
3. Soporte en la respuesta.
4. Coordinación en la respuesta.
5. Manejo de Vulnerabilidades.
6. Manejo de Artefactos.

Protección infraestructura crítica cibernética:

1. Alertas y Advertencias.
2. Sensibilización.
3. Apoyo al manejo de Incidentes Nacionales.

4. Apoyo al manejo Vulnerabilidades Críticas.
5. Apoyo al manejo de Artefactos Especiales.
6. Resiliencia.

Por otra parte, en el área de capacidad de Ciberdefensa se localizan las siguientes actividades:

Defensa activa:

1. Infiltración.
2. Infección.
3. Denegación de Servicio.
4. Contra la integridad de datos.
5. Degradación de servicios.
6. Inutilización de servicios.
7. Aplicación de código diseñado a la medida.
8. Recuperación.

Inteligencia y contrainteligencia:

1. Obtención de información fuentes abiertas.
2. Explotación.
3. Sistemas de Engaño.
4. Análisis de Malware.
5. Consecuencia de la situación.
6. Análisis Forense.

Defensa de la infraestructura critica cibernética:

1. Prevención y mitigación de ciberataques.
2. Defensa Activa.
3. Aplicación de Artefactos Especiales.

Homologación con la estrategia OTAN

Figura 5 – Relación entre elementos y mandato (Alexander Klimburg (Ed.), 2012).

Fuente: *National Cybersecurity Framework Manual.* Tallin,

Tras el análisis realizado de todo el compendio teórico de este documento, se hace importante tomar el modelo de ciberseguridad desarrollado por la OTAN como se aprecia en la figura No.1, para orientar y extractar las capacidades y actividades que pueden complementar la estrategia de ciberdefensa de las Fuerzas militares de Colombia que está inmersa en el **CONPES 3854 "Estrategia de Seguridad Digital del Estado Colombiano".**

La estrategia de ciberseguridad de la OTAN se basa en cinco ejes sobre los cuales se soportan una serie de actividades que funcionan como parte del ciclo de gestión de incidentes cibernéticos. El modelo Colombiano actual por lo cual se sugiere adoptar estos ejes pero orientados a cubrir las necesidades del sistema militar de conducción de operaciones militares, como se puede ver en la tabla No. 4.

Tabla 4. Propuesta de ejes para el modelo Colombiano de ciberdefensa. (Cardenas, 2019)

EJES OTAN	EJES MODELO COLOMBIANO
Gobernanza en Internet – Ciberdiplomacia	Gobernanza Internet / Ciberdiplomacia
Manejo de crisis y CIP	Comando y control
Operaciones Militares Cibernéticas	Gestión de crisis
Contrainteligencia	Infraestructuras Criticas
Contra – cibercrimen	Operaciones militares en el ciberespacio
	Inteligencia y contrainteligencia
	Coordinación y logística
	Colaboración, compartir información y protección de datos.
	I+D+i y Educación

Fuente: Elaboración Propia

Como se observa en la tabla No. 2, la propuesta para el modelo de ciberdefensa de Colombia, acoge algunos ejes del modelo OTAN y adiciona unos nuevos que son necesarios para la gestión efectiva de incidentes cibernéticos. Es así como se mantienen los ejes de (gobernanza, Ciberdiplomacia, protección de infraestructuras críticas y operaciones militares en el ciberespacio), se complementa el eje (inteligencia y contrainteligencia), y se adicionan los ejes (comando y control, coordinación y logística, colaboración, compartir información y protección de datos e I+D+i y educación).

Siguiendo con la base del modelo OTAN, se deben adoptar los grupos de capacidades del mismo, especificando las actividades que componen a cada uno de estos grupos como lo presenta la tabla No. 3.

Tabla 5. Actividades por capacidad (Cardenas, 2019).

Proacción	1	Estrategia	Respuesta	22	Respuesta a incidentes
	2	Política, procesos y procedimientos		23	Manejo de Incidentes
	3	Acuerdos internacionales		24	Análisis de incidentes
	4	Ejercicios cibernéticos		25	Mitigación
	5	Apoyo internacional		26	Toma de Decisiones en Tiempo Oportuno
	6	Marco Jurídico		27	Defensa Activa
	7	Marco Organizacional		28	Sistemas de Decepción o Engaño
Prevención	8	Sensibilización	Recuperación	29	Gestión de Recuperación
	9	Educación / Entrenamiento		30	Continuidad
	10	Manejo de Vulnerabilidades	Control y seguimiento	31	Manejo de Artefactos
	11	Monitoreo de Seguridad		32	Análisis Forenses
	12	Valoración Dinámica del Riesgo		33	Investigación
	13	Prevención y mitigación de ciberataques		34	Judicialización
	14	Obtención de información fuentes abiertas		35	Análisis de mejoras
	15	Conciencia de la situación		36	Alertas y Advertencias
	16	Controles de seguridad		37	Avance Estratégico
Preparación	17	Visibilidad y Seguimiento			
	18	Vigilancia Tecnológica			
	19	Detección y Análisis de Ataques Cibernéticos			
	20	Escalamiento y comunicación			
	21	Análisis de Malware			

Fuente: Elaboración Propia

Determinadas e identificadas las actividades de las capacidades adoptadas, se procede a identificar la relación que tienen estas capacidades con cada uno de los ejes establecidos para el modelo de ciberdefensa de las fuerzas militares de Colombia, esta actividad se realiza mediante una matriz de correlación como se puede apreciar en la tabla No.4.

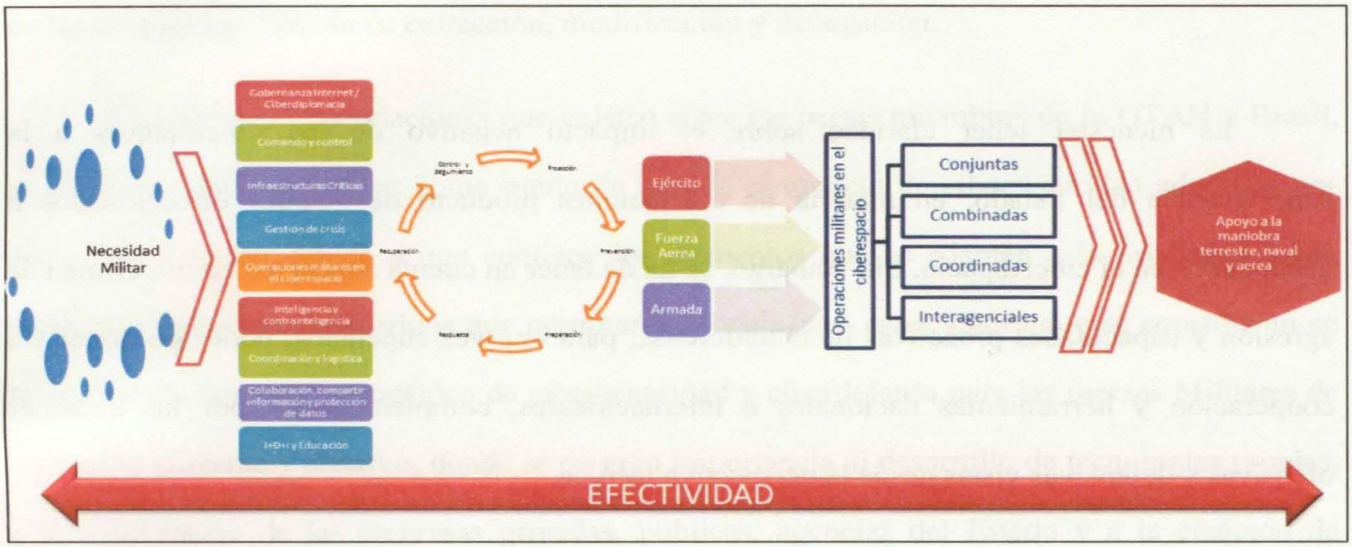
Tabla 6. Matriz de correlación ejes – capacidades. (Cardenas, 2019)

	Proacción	Prevención	Preparación	Respuesta	Recuperación	Control y Seguimiento
Gobernanza Internet/ ciberdiplomacia	X	X	X	X	X	X
Comando y Control		X	X	X	X	
Gestión de Crisis			X	X	X	X
Infraestructuras Críticas		X	X	X	X	
Operaciones Militares en el Ciberespacio		X	X	X	X	
Inteligencia y C/I		X		X		X
Coordinación y Logística	X	X	X	X	X	X
Colaborar, compartir información y protección de datos	X	X	X	X	X	X
I+D+i y Educación		X				X

Fuente: Elaboración Propia

De esta forma se propone que el concepto estratégico de ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia, debe adoptar e implementar las 37 capacidades propuestas en este documento, reunidas en los seis grupos de capacidades descritos y regidas por los nueve ejes estratégicos establecidos para orientar la ejecución de las mismas en pro de alcanzar los objetivos plenamente establecidos.

Figura 6 - Concepto Conjunto de Ciberdefensa (Cardenas, 2019).



Fuente: Elaboración Propia

Finalmente se propone el concepto graficado en la figura 6, donde ante la necesidad militar se enmarca en el empleo de los 9 pilares durante el proceso de ciberdefensa con alta efectividad, todo esto para emplear las capacidades de la Fuerza Aérea, el Ejército y la Armada Nacional en el marco de operaciones militares conjuntas, combinadas interagenciales y coordinadas en el ciberespacio, como apoyo a la maniobra terrestre, aérea y naval.

Conclusiones

Es menester tener claridad sobre el impacto negativo de los ciberataques a la supervivencia del Estado, en materia de afectaciones producto de ataques direccionados o gestionados en el ciberespacio. Sin embargo, se ha de tener en cuenta conceptos como, crimen de agresión y capacidades proactivas de ciberdefensa, para una vez superados, poder gestionar vía cooperación y herramientas nacionales e internacionales, complementadas por las acciones ofensivas y defensivas vistas desde la perspectiva técnica.

Con base en la investigación realizada sobre como los países tomados como muestra de análisis conciben la relación ciberespacio – seguridad nacional, se evidencia que las estrategias adoptadas llegan a ser semejantes en cuanto a metodología, evidenciándose esto en la base del respeto a los derechos fundamentales.

Así mismo, se observa que estas difieren en la concepción de las capacidades necesarias para enfrentar efectivamente los retos a los que las naciones se enfrentan en el ciberespacio, siendo esto visible en países como Brasil y Estados Unidos los cuales centran su estrategia en el entorno de ciberseguridad dando gran importancia a las operaciones de información, mientras otras como España e incluso organismos multilaterales como la OTAN definen las capacidades en tres áreas fundamentales (Defensa, Explotación y Respuesta).

De forma adicional se evidencia que los países y el organismo multilateral objeto de este análisis, coinciden profundamente en la percepción de la participación proactiva de todas las entidades públicas y privadas tanto nacionales como internacionales en la defensa de sus

intereses, pues es la información el activo a defender en integridad, autenticidad y disponibilidad, de los ataques que buscan su extracción, modificación y denegación.

Considerando las relaciones que existen entre los países miembros de la OTAN y Brasil, se considera oportuno tomar como punto de partida el modelo de ciberseguridad adoptado por dicha organización debido a que contiene los elementos que se adaptan a la necesidad local, realizando los ajustes requeridos que permitan construir unas capacidades que se constituyan en la base de un concepto estratégico de ciberseguridad y ciberdefensa para las fuerzas Militares de Colombia eficiente y efectivo, donde se de gran importancia al desarrollo de tecnologías propias, a la cooperación de las empresas privadas, publicas, agencias del Estado y a la creación de canales de comunicación especializados para compartir información y lecciones aprendidas de los incidentes atendidos.

No sincronizar los esfuerzos de los organismos militares y civiles tiene como consecuencia aspectos negativos que a corto y mediano plazo se traducen en sobrecostos e inversiones ineficientes de los recursos públicos.

El desarrollo de estas capacidades se centra principalmente en el recurso humano y en ese sentido el proceso de selección se vuelve relevante para las Unidades de Ciberdefensa de las Fuerzas Militares, así mismo el crecimiento de estas unidades se vuelve un imperativo tras la implementación de las capacidades propuestas en este documento.

Referencias bibliográficas

Aguilar, L. (2010). *biblioteca virtual de defensa*. (I. E. Estratégicos., Productor) Recuperado de http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

Alemañ, R. (2012). *ALU*. Recuperado de http://www.alu.ua.es/r/rac6/buscadores/indice.html

Alexander Klimburg (Ed.). (2012). *National Cybersecurity Framework Manual.* Tallin, Estonia: NATO CCD COE Publication.

Article 19. (2016). *Brasil: Análise da Estratégia de Cibersegurança.* São Paulo.

Cardenas, N. (2019). Concepto Conjunto de Ciberseguridad y Ciberdefensa.

Cavelty, M.(2015). The normalization of cyber - International relations. *Strategic Trends*.

CCDCOE. (s.f.). *Nato Cooperative Cyber Defence Center of Excelence*. Recuperado de https://ccdcoe.org/cyber-definitions.html

Chang, W.(2012). La Guerra en el Ámbito Cibernético. En A. &. Power, Cyber Warfare Amenaza Mundial. *Journal en español*, 24, 83-90.

CONPES 3701. (2011). *Consejo Nacional de politica Económica y Social.* Bogota DC: República de Colombia.

Forero, C. (2016). *Universidad Tecnologica de Tallin.* Recuperado de https://www.tlu.ee/en

Fuerzas Militares de Colombia. (2017). *Manual de Ciberdefensa Conjunta FFMM 3-18 restringido.* Bogota: Imprenta Militar.

Gaitán, A. (2011a). Computadores e internet en la guerra interestatal: ¿La consolidación de un nuevo poder militar en el siglo XXI? s.

Gaitán, A. (2011b). Computadores e internet en la guerra interestatal: ¿La consolidación de un nuevo poder militar en el siglo XXI2, 22-34. Bogota DC, Colombia: s.

Gaitán, A. (2011c). Computadores e internet en la guerra interestatal: ¿La consolidCentro de Estudios Estratégicos sobre Seguridad y Defensa CEESEDEN.

Ganuza, N. (2010). LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN. *Instituto Español de Estudios Estratégicos. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, 21-46.

Hernandez, F.(2013). *LOS CIBERATAQUES COMO CRIMEN DE AGRESIÓN.* trabajo de grado "Especialización en Derecho Internacional de los Conflictos Armados", Escuela Militar de Cadetes General José María Córdova, Bogota DC.

Tablas y figuras

Tabla 1 - Definición de capacidades cibernéticas (Aguilar, 2010) 8
Tabla 2. Agresiones de nivel internacional en el ciberespacio 29
Tabla 3: Caracterización de amenazas 30
Tabla 4. Propuesta de ejes para el modelo Colombiano de ciberdefensa. (Cardenas, 2019) 63
Tabla 5. Actividades por capacidad (Cardenas, 2019). 64
Tabla 6. Matriz de correlación ejes – capacidades. (Cardenas, 2019) 65

Figura 1 - Relación entre elementos y mandato (Alexander Klimburg (Ed.), 2012) 38
Figura 2 - Estructura de operaciones de información (Article 19, 2016) 49
Figura 3 - Sistema de mando de defensa cibernética (Article 19, 2016) 50
Figura 4. Sistema de capacidades cibernéticas (Fuerzar Miliatres de Colombia, 2017) 59
Figura 5 - Relación entre elementos y mandato (Alexander Klimburg (Ed.), 2012) 62
Figura 6 - Concepto Conjunto de Ciberdefensa (Cardenas, 2019) 66