Propuestas de creación de una Brigada Cibernética para el Ejército Nacional de Colombia

Diego Luis Sanabria Rodríguez

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

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL DE LAS FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

TITULO:

PROPUESTA DE CREACIÓN DE UNA BRIGADA CIBERNETICA PARA EJÉRCITO NACIONAL DE COLOMBIA

ALUMNO:

CORONEL. DIEGO LUIS SANABRIA RODRÍGUEZ

DIRECTOR:

STEVEN JONES CHALJUB

MAGISTER EN CIBERSEGURIDAD CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE MAGISTER EN CIBERSEGURIDAD CIBERDEFENSA

BOGOTA-COLOMBIA

2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

UNA MIRA HACIA LA CREACIÓN DE LA BRIGADA DE CIBERDEFENSA EN EL EJERCITO NACIONAL DE COLOMBIA FRENTE A LA DEFENSA Y PROTECCIÓN MULTIDIMENCIONAL DEL CIBERESPACIO

Coronel Diego Luis Sanabria Rodríguez[1]

RESUMEN

La seguridad multidimensional amplia el concepto de seguridad y defensa de las américas, teniendo como objetivo fundamental la protección contra las amenazas militar externas, problemas políticos, económicos, del medio ambiente y la seguridad humana. Dentro de esa agenda de seguridad hemisférica, emergen nuevos campos de combate y defensa dando importancia a la protección de las infraestructuras criticas digitales de los Estados. Por lo anterior el presente texto busca identificar el aporte de la construcción de una Unidad de Ciberdefensa, a la seguridad del estado Colombiano, por medio de la conformación una Brigada Cibernética, un Centro de Planeación de Operaciones Cibernéticas, un Arma Cibernética nueva para integrar al personal y unas formulas ciberneticas para realizar Operaciones en Ciberespacio.

Palabras Claves. Seguridad Multidimensional, Seguridad y Defensa Nacional, Ciberespacio, Ciberdefensa, Ciberseguridad, Ciberguerra, Ciberdelincuencia, Cibermercenarios, Ciberterrorismo, Brigada de ciberdefensa, Ejército nacional, Colombia.

---

[1]Estudiante Maestria en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra.

PRESENTATION: ONE LOOKS TOWARDS THE CREATION OF THE CYBER DEFENSE BRIGADE IN THE NATIONAL ARMY OF COLOMBIA IN FRONT OF THE DEFENSE AND MULTIDIMENSIONAL PROTECTION OF CYBERSPACE

Colonel Diego Luis Sanabria Rodríguez[1]

ABSTRACT

Multidimensional security broadens the concept of security and defense of the Americas, with the fundamental objective of protecting against external military threats, political, economic, environmental and human security problems. Within this agenda of hemispheric security, new fields of combat and defense emerge, giving importance to the protection of digital critical infrastructures of the States. Therefore, the present text seeks to identify the contribution of the construction of a Cyber Defense Unit, to the security of the Colombian state, through the creation of a Cybernetic Brigade, a Cybernetic Operations Planning Center, a new Cybernetic Weapon to integrate the personal and some cybernetic formulas to perform Operations in Cyberspace.

Keywords. Multidimensional Security, National Security and Defense, Cyberspace, Cyberdefense, Cybersecurity, Cyberwar, Cybercrime, Cybermercenaries, Cyberterrorism, Cyber Defense Brigade, National Army, Colombia.

---

[1]Master student in Cybersecurity and Cyberdefense, The War College.

I. INTRODUCCIÓN

En los últimos años el concepto de Seguridad y Defensa nacional ha tomado un nuevo rumbo donde ya no se limita a las amenazas tradicionales, sino se ha ampliado dándole paso a nuevas amenazas que afectan la estabilidad de los Estados, ese nuevo concepto ha sido denominado Seguridad Multidimensional (Alda y De Sousa, 2015).

Esta nueva visión de seguridad ha sido definido y legitimado por organizaciones estatales de la región como la OEA, la cual tiene como pilar fundamental el ser garante de la seguridad de los pueblos de las Américas y a partir del año 2003 mediante la declaración sobre seguridad hemisférica adopto el termino seguridad multidimensional el cual amplio el concepto de seguridad y defensa de las naciones. Para el año 2005 fue creada la secretaria Multidimensional (SSM), lo que permite avanzar en el fortalecimiento de la cooperación en la seguridad y el desarrollo de políticas regionales lo que permitiendo estar más preparado para enfrentar las amenazas presentes y futuras (Organización de Estados Americanos, 2011).

La Seguridad Multidimensional es la protección de los seres humanos y la multidimensionalidad de los conflictos en el campo de la seguridad hemisférica donde se ataca las amenazas desde las causas que lo originan y extiende el concepto de seguridad donde no solo individualizaba las amenazas de tipo militar externas, ahora involucra en este nuevo concepto problemas políticos, económicos, medio ambiente, seguridad humana y nuevas amenazas que van más allá del plano fisico como las ciberamenazas (Organización de Estados Americanos, 2011).

Precisamente esta última amenaza es en la que se centrara este trabajo, ya que el ciberespacio es llamado el quinto dominio de la guerra después del dominio terrestre, marítimo, aéreo y el espacial, y con el avance de la tecnología este plano toma vital importancia para proteger los intereses nacionales del país, haciéndose necesarias unidades de ciberdefensa especializadas en ciberataques ciberterrorismo, ciberdelincuencia y defensa de los sistemas informáticos, debido a que toda la infraestructura crítica de un país está conectadas a internet y un ataque exitoso contra estos sistemas generaría pánico en la población o importantes pérdidas económicas, confirmando que la ciberdefensa es un aspecto esencial y estratégico para la defensa nacional (Candela, 2014).

En la historia del ser humano siempre ha estado presente en la guerra, ya sea por cuestiones de violación de derechos humanos, desigualdad, política, ideología, territoriales o poder.

El conflicto está integrado por estrategias de combate, armamento y campo en la que se desarrolla la batalla. Por esta razón cada país tiene ejércitos que tiene como objetivo el dominio militar en diferentes ámbitos tales como: el terrestre, el aéreo, el naval, el espacial y el nuevo dominio que es el ciberespacio (Joyanes, 2010).

En la actualidad la sociedad depende de la conexión de internet para desarrollar actividades incluso la infraestructura crítica de la nación está conectado a este medio. El ciberespacio puede ser utilizado como un campo de batalla ya que, con una computadora, una conexión a internet y conocimientos técnicos es posible robar y borrar información de otro equipo así mismo atacar la infraestructura crítica de los países. Estos avances tecnológicos han generado enormes retos para la defensa y la seguridad dado que los cibercriminales de hoy emplean varias técnicas para robar información. Estos pueden infiltrarse en las empresas, en las entidades bancarias, en los gobiernos entre otros y causar daños a equipos (Pastor, Pérez, Arnáiz & Taboso, 2009).

Los cibercriminales introducen malware maliciosos como: gusanos, botnets, virus, troyanos, spyware, adware, spammers etc. Los ataques cibernéticos son cada vez más sofisticados, dado que utilizan técnicas de sigilo para permanecer oculto por mucho tiempo. Esto aumenta la complejidad puesto que reduce la posibilidad de que las victimas descubran que son atacadas ya que los cibercriminales utilizan algoritmos complicados para evitar ser descubiertos, es decir a diferencia de las armas convencionales donde puedes mirar al cielo y ver la bandera o insignia del atacante, las armas cibernéticas no dejan rastro del remitente, es decir no es fácil identificar la procedencia de la amenaza (Gómez, 2010). Por lo tanto, se considera una nueva estrategia ofensiva, estos nuevos ejércitos con nuevas armas, cobrarán un tipo nuevo de víctimas. Es algo que va mucho más allá del ataque convencional. Antes todas las guerras tenían una naturaleza cinética, arrojar una bomba supone un movimiento, que un tanque dispare proyectil es otro movimiento. Pero, una ciberguerra no implica movimiento, no sabes quién lo ataco, puedes estar muy seguro quien pudo ser, pero, no tienes pruebas suficientes.

Sumado a lo anterior, se encuentran las creencias sociales que juegan un papel importante en la percepción de la seguridad por parte de la ciudadanía, ya que el limitado conocimiento sobre las amenazas cibernéticas, no permite identificar el riesgo de un ataque grave; esto se puede identificar en el auge de las redes digitales, donde la mayoría de personas comparten información

sin pensar que se han convertido en armas, otro ejemplo son los programas informáticos, a los que la gente puede tener fácilmente acceso, para hurtar información valiosa, por lo tanto, todos somos soldados ya que, todos salimos perjudicados con un ataque cibernético puesto que el internet se ha convertido en un arma que puede perturbar el funcionamiento de toda una nación, con el siempre echo de hacer clip en un anuncio, abrir una foto de alguien que conoce, entrar a una página web de ayuda a las víctimas de una catástrofe natural, el ordenador queda infectado (Sierra del Valle, 2011). y por lo tanto no se mide el riesgo de un ataque cibernético y las bandas criminales se aprovechan de esto para generar daño a las infraestructuras robando información, los hackers usan softwares maliciosos para robar contraseñas, acceder a cuentas, infectar a ordenadores.

La revolución tecnología ha generado un impacto social al traer beneficios, pero también causa amenazas y retos para la seguridad principalmente para los Estados ya que entre estos desafíos se encuentran: el ciberterrorismo, las ciberamenaza, el crimen organizado, el ciberespionaje y la infraestructura crítica que ante agresiones se utilizan como un vehículo para interferir en las actividades de los ciudadanos, de los gobiernos y de las instituciones. Según el Conpes 3701 (2011) Colombia ocupa el quinto lugar de ser el país que tiene más ciberataques. En el 2017 se reportaron 198 millones de ataques cibernéticos que han generado pérdidas por 6.179 millones de dólares. Colombia cuenta 13.000 dispositivos en la que genera promedio 542.465 ataques cibernéticos diarios. De los cuales se registraron los siguientes ciberataques: en el sector financiero 39,56 %, empresas públicas y privadas 35, 55%, el gobierno 15,4 % y las telecomunicaciones 25,5%.

La ciberdefensa es un aspecto esencial y estratégico para la defensa nacional. El uso de las comunicaciones y tecnologías de la información se han incorporado en el diario vivir de la nación forzando el crecimiento y el desarrollo de las actividades económicas y sociales. Revolucionando mundo al aportar beneficios, pero también provoca riesgos a las que están expuestos los ciudadanos, la industria y el gobierno. Amenazas que son unos de los mayores retos a solucionar para mantener la seguridad y defensa nacional.

En virtud de lo anterior se formula la siguiente pregunta ¿Cómo podemos diseñar o crear una Brigada de ciberdefensa que garantice la defensa y |protección de la información y la infraestructura crítica de una nación?

Aunque el internet tenga ventajas también tiene desventajas pues se ha convertido en una amenaza real para los ciudadanos puesto que la red es un arma que se encuentra prácticamente al alcance de cualquiera. El transporte, los aviones, las instalaciones energéticas y cientos de otros equipos potencialmente peligrosos funcionan a través de medios informáticos que podrían ser manipulados a distancia por personas que decidiera utilizarlo como armas (Stel, 2014).

En los últimos años se ha presentado más una veintena de episodios que podría ser calificado de ciberguerra y el número aumenta cada día. Según Barrio (2015) un ejemplo es Stuxnet que a mediados de julio de 2010 expertos en seguridad descubrieron un virus informático el que se había infiltrado en una maquinaria de una fábrica, gracias a este virus destruyo gran parte de la infraestructura critica de una central nuclear podría haber provocado un desastre comparable al de Chernóbil.

Fenómenos como estos ponen en manifiesto el potencial que tiene estas acciones para destruir infraestructura crítica y conocer información secreta de estados, gobiernos, personas, organizaciones públicas y privadas además pone en peligro la economía de un país.

De acuerdo con lo anterior el presente trabajo tiene como objetivo presentar un visón sobre la necesidad que tienen los países de tener un Ejércitos Cibernéticos entrenado en ciberguerra y con capacidad de realizar operaciones militares en el ciberespacio. Y en particular para el Ejército de Colombia es necesario tener una Brigada de Ciberdefensa que neutralice las amenazas cibernéticas que afecta la infraestructura crítica de la nación y que proteja la información de diferentes amenazas. También busca definir un ciber soldado mediante la creación de una nueva especialidad de combate.

Para realizar este análisis se iniciar contextualizando al lector sobre los principales constructos que componen el dominio cibernético:

1.1 El Ciberespacio

"Ciberespacio es el quinto dominio de la guerra" . Según la doctora Lany kass, directora del Air forcé cyberespace task forcé de USAF, el ciberespacio no es ni una misión ni una operación, es un escenario estratégico, operacional y táctico. Así las cosas, el ciberespacio debe comprenderse de manera estratégica ya que solo así es posible entender también de que manera puede ser utilizado para las intervenciones entendidas como guerra cibernética o ciberguerra (Butler, 2011).

Unos de los primeros autores que definieron el termino ciberespacio fueron, Wiener y Gibsom (1948), quienes lo consideran como la idea de que los humanos pueden interactuar con máquinas y que el sistema resultante proporciona un entorno alternativo de interacción. A pesar del paso del tiempo estas palabras se han extendido en los círculos profesionales y académicos, hasta el día de hoy. Años más tarde, autores como Clarke and knake´s en su libro Cyber war: the next threat to National segurity and what to do about it" (2010), afirman que el ciberespacio es dominio tanto físico como virtual, sin límites claros, donde hasta la fecha, no existe ninguna ley o doctrina internacional que rige el ciberespacio global. Además, como consecuencia de la revolución de las tecnologías de la información, el ciberespacio es el quinto dominio el cual las personas pueden interactuar en armonía, cooperación y/o conflicto. Considerar el ciberespacio, como un quinto dominio de la guerra, ha sido objetivo común de reflexión de múltiples expertos y agencias públicas y privadas nacionales e internacionales y se vislumbra. Por último, el Departamento de Defensa de EEUU considera el ciberespacio como «un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores (Departament of Defense, 2009).

Ahora bien, para contexto de las fuerzas militares de Colombia, el ciberespacio se definirá como un ámbito estratégico, operativo y táctico a fin de aplicar medidas de prevención, disuasión, contención, explotación, protección, reacción y respuesta, que permitan fortalecer las capacidades de Ciberdefensa para enfrentar las amenazas o incidentes cibernéticos que puedan afectar la infraestructura critica del país y poner en riesgo la integridad territorial, la independencia, la soberanía, el orden constitucional y en general los intereses del estado (Clake y Knake, 2010).

1.1.1 Características del ciberespacio. Este escenario, posee unas características que lo hacen altamente diferenciable a los dominios de la tierra, mar, aire y espacio , las cuales favorecen la clandestinidad, el anonimato, fácil acceso, poco ningún control gubernamental , rápido flujo de información, indetectable , ubicuidad y fácil ejecución, efectividad e impacto, bajos costos y reducido de riesgo para el atacante. Así como alto impacto por el poder en términos de la capacidad de destrucción, disrupción , mal funcionamiento o toma de control de sistemas tecnológicos y sus consecuencias, y también por la rentabilidad en términos

económicos y políticos por parte de personas, industrias y estados, constituyendo la amenaza cibernética convergente para el hemisferio y en una preocupación presente y futura para los estados más aún. Cuando la dependencia tecnológica es una realidad inevitable, con la cual necesariamente tendrá que convivir los ciudadanos y la sociedad (Clake y Knake, 2010).

1.2 Definiciones conceptuales

Con el objetivo de que el lector tenga una mejor idea y comprensión del tema, a continuación, se describirán algunos de los conceptos más relevantes:

1.2.1 Ciberterrorismo. Son personas o grupos criminales que usan el ciberespacio para cometer crimines o delitos es decir el ciberterrorismo es el uso disruptivo de la tecnología de la información por parte de grupos terroristas para promover ideologías o políticas. Estos atacan a redes, a sistemas informáticos, sistemas financieros entre otros (Poveda & Torrente, 2016).

1.2.2 Ciberguerra. La guerra cibernética implica que las naciones o estados usan la tecnología de la información para penetrar en las redes de otras naciones y causar daños o interrupciones. Los ataques cibernéticos son ejecutados principalmente por piratas informáticos. Un ataque puede comprometer datos valiosos, degradar la comunicación y perjudicar los servicios de infraestructura critica (Gómez, 2017).

1.2.3 Ciberespionaje. El ciberespionaje son organizaciones, personas, gobiernos entre otros que a través del internet o el ciberespacio pretende, espiar, manipular y secuestrar información en otras palabras el ciberespionaje es la práctica de utilizar la tecnología para obtener información secreta de estados o gobiernos para sacar un provecho económico, social, político entre otros (Sánchez, 2013).

1.2.4 Cibermercenarios. Son piratas informáticos o hackers contratados por distintos actores incluso gobiernos para lanzar ofensivas cibernéticas. Los cibermercenarios son personas expertas en informática que tiene la habilidad de hacer softwares maliciosos, de modificar o hacer páginas

web para estafar a los usuarios y robar información (Walt, 2013). (ATAQUE A ESTONIA. HACCION DE GUERRA)

II. GENERALIDADES DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD

2.1 Definición de Ciberdefensa

Podríamos definir la Ciberdefensa como el conjunto de acciones encaminadas a proteger la información digital para asegurar los usos del ciberespacio y negarlo al adversario. Este concepto ha sido definido por varios autores, a continuación, cada uno de ellos dan su punto de vista:

El Instituto Español de Estudios Estratégicos (como se citó en Peralta, 2015) dice que:

> La Ciberdefensa, es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional, normalmente está orientada a contrarrestar el uso de internet con fines terroristas, los actos de guerra cibernética, hechos afines con objetivos de guerra y el espionaje (p. 6).

Para Newmeyer (2015): "la Ciberdefensa se considera como la adopción de tecnologías, prácticas y estrategias que buscan contrarrestar los ataques sobre los sistemas tecnológicos de información y data" (p.79).

Camacho (2016) establece que "el concepto de ciberdefensa se enmarca en el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición" (p. 7).

2.2 Propósito de la ciberseguridad

El propósito de la ciberdefensa es fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la seguridad de la información. La ciberdefensa busca prevenir, coordinar, atender, controlar, generar recomendaciones y regular emergencias cibernéticas para

afrontar amenazas y riesgos que atenten contra la seguridad de la nación (Documento CONPES 3701, 2011).

Debido a los sistemas de información y telecomunicaciones y a los ciberataques cibernéticos se vuelto cada vez más importante proteger toda información proveniente de: empresas, instituciones, gobierno etc. Pues albergan una información valiosa para el correcto funcionamiento de la comunidad. El propósito de la ciberseguridad es fijar directrices generales del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a la nación seguridad y progreso a través de una adecuada coordinación (Gobierno de España, 2013).

2.3. Principios Rectores de la Ciberdefensa

A continuación en la Tabla 1, se presenta la descripción a profundidad los principios rectores de la ciberdefensa:

Tabla No. 1 Principios de la ciberdefensa

Liderazgo Nacional y Coordinación de Esfuerzos	El ámbito y la complejidad de los desafíos del ciberespacio requieren, además de un liderazgo nacional decidido, la adecuada coordinación de las capacidades, recursos y competencias involucradas.
Responsabilidad Compartida	Todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de sentirse implicados con la ciberseguridad. Para ello, se hace precisa una intensa coordinación de los diferentes organismos y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información.
Proporcionalidad Racionalidad y Eficacia	Es necesario gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas, que habrán de ser elementos habilitantes de la confianza y

	no trabas al desarrollo de nuevos servicios.
Cooperación Internacional	El carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación global, ya que muchas de las posibles medidas sólo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los distintos países.

Fuente: Tabla tomada del Gobierno de España. (2013). Estrategia de Ciberseguridad. p. 16.

2.4. Amenazas

Gracias a los avances tecnológicos ha permitido que varias personas que tiene conocimiento de informática se aprovechen de estos medios para poder espiar, robar información a estados, secretos de empresas o para destruir maquinaria u objetos físicos que están conectados a computadoras, que cada vez es más fácil acceder a ellos por medio del internet. Cuando no se garantiza una adecuada protección a la información se genera una serie de amenazas que puede ser causadas por: cibercriminales, espías, hacktivistas, atacantes interiores entre otras. Existen cuatro clases de amenazas entre ellas tenemos:

- Amenazas de los bienes de las personas
- Amenazas de los bienes de los bienes de las organizaciones
- Amenazas de los bienes de los bienes virtuales
- Amenazas en la infraestructura

La multiplicidad de ataques pone en amenaza la infraestructura crítica de un país. Existen estados que disponen de capacidades militares y de inteligencia para realizar ciberataques que colocan en riesgo la seguridad de la nacional (Ver Figura 1) (Gobierno de España, 2013).

Figura No. 1 Riesgos y Amenazas a la Ciberseguridad Nacional

Fuente: Tabla tomada del Gobierno de España. (2013). Estrategia de Ciberseguridad. p. 11.

2.5. Características Ciberataques

Según el Gobierno de España (2013) los ataques derivados de estas amenazas, denominados ciberataques, tiene una serie de características tales como:

Tabla No. 2 Características

Bajo Coste	Muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido.
Ubicuidad y Fácil Ejecución	La ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.
Efectividad e Impacto	Si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la falta de sensibilización y formación pueden facilitar este adverso resultado.
Reducido riesgo para el atacante	La facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificultad la persecución de la acción.

Fuente: Tabla tomada del Gobierno de España. (2013). Estrategia de Ciberseguridad. p. 10.

Por lo anterior, se procederá a explicar algunos ejemplos de amenazas mediante malware maliciosos:

Iloveyou. Según Peter (2014) fue creado por dos programadores filipinos Reonel Ramones y Onel de Guzmán. Apareció el 4 de mayo del 2000 infecto a 50 millones de computadoras y genero 550.000 millones de dólares en perdida. Este virus se transmite a través de un email que llegaba al correo con el asunto Iloveyou que era una carta de amor y cuando se hacía doble clic los archivos se reemplazaban por JS, .JSE, .CSS, .WSH, .SCT, .HTA, JPG y JPEG después lo eliminaba y se insertaba un código malicioso. Los archivos MP3 y .MP2 los ocultaban y generaba archivos con el mismo nombre del virus para que la persona ejecutara de nuevo el código malicioso. Luego, tomaba la libreta de direcciones de gmail y se reenviaba a todos los contactos el correo Iloveyou. Por último, descargaba un troyano llamado wingfix.exe y se introducía en los registros de Internet Explore. La computadora pasaba ser víctima puesto que podía ser manipulada por otro usuario. Este virus causo bastante mal e incluso muchas entidades

gubernamentales y bancarias quedaron fuera de servicio ya que tuvieron que desconectarse de la red de internet para poder evitar la propagación del virus.

Code Red. El Code Red fue descubierto por primera vez en el año 2001 por eEye Digital Security. El gusano es capaz de ejecutarse por completo en la memoria con un tamaño de 3.569 bytes. Una vez infecte procederá a realizar cien copias de sí mismo. Luego lanzará un ataque de denegación de servicio en varias direcciones IP. Este ataque permite tener acceso a la máquina en la que el cibercriminal puede averiguar, robar y manipular información (Berghel, 2015).

Sasser. Cuadra (2016) afirma que Sasser se descubrió por primera vez en el año 2004 fue creado por el estudiante de informática Sven Jaschan. El Sasser aprovechó la vulnerabilidad del desbordamiento de búfer de Windows para ralentizar y bloquear el sistema operativo. Esto llevó a más de un millón de infecciones afectando infraestructuras críticas como: líneas aéreas, transporte público, hospitales etc. En general se estima que el daño costó $ 18 mil millones de dólares.

Conficker. También conocido como Downup o Downadup es un gusano de autoría desconocida que apareció por primera vez en 2008. Infecta a computadoras que tiene fallas en el sistema operativo para crear un botnet. Conficker **infecto más de 9 millones** de computadoras en todo el mundo. Una vez infecte el gusano bloquea la actualización de Windows, desactiva antivirus y bloquea las cuentas del usuario. Luego procede a instalar el software que convertirá a la computadora en un esclavo botnet para estafar dinero al usuario (Giles, 2009).

Zeus. Es un caballo de Troya hecho para infectar computadoras y realizar crimines. La mayoría de las computadoras se infectaron **mediante descargas directas** o por phishing. En 2009 logró poner en peligro miles de computadoras de grandes corporaciones, multinacionales y bancos como Amazon, Oracle, Bank of América, Cisco etc. El troyano Zeus roba información de redes sociales, correo electrónico y contraseñas de cuentas bancarias. Cerca de $ 70 millones de dólares fueron robados (Flores, Asanza & Berrones, 2014). (CIBERECRIMEN Y CIBERDELITO)

Stuxnet. Para Kenney (2015) Stuxnet es un virus que se cree que fue creado por Estados o Países para afectar la infraestructura crítica de las bases nucleares iraníes. Se estima que Stuxnet ha logrado arruinar una quinta parte de las centrífugas nucleares de Irán. En junio de 2010 en Irán el virus Stuxnet infecto a 14 compañías y una planta de uranio además el cibercriminal podía espiar a las computadoras y también manipular las maquinas. (CIBER GUERRA).

Flashback. El troyano fue descubierto por primera vez en 2011 por la empresa de antivirus Intego. Se propaga mediante el uso de sitios web que contienen un código JavaScript. Una vez instalado el Mac se convierte en un botnet. Más de 600.000 Macs fueron infectados (Joyanes, 2010). (CODIGO DE COMPUTADORA)

Virus de Facebook. Las redes sociales juegan un papel importante en el desarrollo de las personas. Por lo tanto, no es de extrañar que los ciberdelincuentes decidieran utilizar las redes sociales para hacer delitos cibernéticos. Se detectaron actividades maliciosas en Facebook en 2014, pero en el año 2017 se empeoró. Varias versiones de Facebook causaron estragos en la red pues intentan robar credenciales de Facebook y piratear cuentas de usuarios (Fiscarra, 2017).

Virus Android. En febrero de 2016 los especialistas en seguridad notaron una nueva amenaza del malware que se propagaba a través de mensajes de texto. Este malware intenta robar información personal a los usuarios (Pérez, 2018).

Ransomware WannaCry. se puede definirse como el secuestro de datos el 12 de mayo del 2017 ransomware WannaCry infectó más de 200.000 computadoras en 150 países incluido las infraestructuras de hospitales, fábricas, escuelas y tiendas. Este virus encripto datos del equipo y lo infectado sin dejar acceso al usuario y para poder desencriptar la información se requería de realizar un depósito a una cuenta por medio de una moneda virtual conocida como Bitcoin (Chen & Bridges, 2017).

Ataques DDoS. Los ataques de denegación de servicio distribuido (DDoS) es un grupo de sistemas también conocidos como ordenadores zombie que atacan a un solo objetivo para causar una denegación de servicio a los usuarios esto crea un enorme flujo de mensaje y solicitudes que

se lanzan en el ordenador de la víctima para que sobrecargue y de esta forma se cierre o valla más lento como resultado se les niega el servicio a los verdaderos usuarios. Una manera típica de lograr un ataque de (DDoS) es que el cibercriminal explote alguna vulnerabilidad del sistema de la víctima y lo convierta botmaster después este identifica otros sistemas vulnerables y los infecta a través de spam o e-mail cuando se controla lo suficiente se convierte en un Bonnet o un ejército zombie se les manda instrucciones para que ataque a un objetivo específico. El ataque (DDoS) utiliza varios dispositivos con conexiones repartidas por todo el mundo por lo que es muy difícil averiguar quién es el responsable pues no se está tratando con un solo atacante (García, 2016).

Botnet. Los botnets (robots de la red) son redes o grupos de PC infectados y controlados por un atacante de forma remota (Garcia, 2018).

Exploit. Son programas que se aprovecha de las vulnerabilidades que tiene el sistema operativo para provocar un comportamiento no autorizado o imprevisto en los ordenadores (González & Vázquez, 2015). (HERRAMIENTA DE INTELIGENCIA)

Adware. Es un programa que muestra avisos de publicidad engañosa la cual busca recolectar datos personales de los usuarios (Garcia, 2018).

Phishing. El Phishing es una forma de fraude por internet en donde un estafador se hace pasar por una empresa o envía un correo electrónico que anima a las personas a revelar datos personales y confidenciales como contraseña de tarjeta de crédito, datos bancarios, nombres, direcciones entre otros (Garcia, 2018).

Debido a lo anterior organizaciones, empresas y el estado se han visto obligados a invertir una mayor cantidad de recursos para fortalecer la capacidad de ciberdefensa.

2.6. Definición de Infraestructura Crítica

En cuanto la definición de infraestructura crítica puede tener diferentes conceptos puesto que cada país lo definen de manera diferente de acuerdo a sus necesidades, en entre ellas tenemos:

Huerta (2015) define la Infraestructura Crítica como:

> Aquella infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Es decir, por infraestructura crítica se considera toda aquella infraestructura que da soporte a servicios críticos tales como los relacionados con energía, salud, transporte, entre otras (párr. 2).

El Plan Nacional de Protección de Infraestructuras Críticas las define como:

> Aquellas instalaciones, redes, servicios, y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas (párr. 3).

En otras palabras, la infraestructura crítica es esencial para los ciudadanos ya que, de ella se puede suplir las necesidades básicas como salud, la integridad física, la seguridad, y el bienestar social y económico de la población. Si se destruye o afecta redes eléctricas, hidráulicas, transporte etc. Estos tipos de ataques ocasionan que los "sistemas y redes detengan una región o la electricidad de un país e interrumpir los servicios públicos, sistemas críticos y líneas de producción que pueden llevar al caos y daños irreparables" (ACIS, párr. 1, 2015).

La infraestructura que ha sido designada como crítica son: la energía, la industria nuclear, las tecnológicas de la información, los transportes, los suministros de agua, el suministro de

alimentos, la salud, los sistemas financieros, la industria química, el espacio, los recursos y la administración.

2.6.1. Protección de la de infraestructura Crítica. Para proteger la infraestructura crítica ACIS (2015) afirma que la mejor estrategia de seguridad para estos sistemas es la aplicación de varias capas que incluye un perímetro de despliegue de plataformas para acomodar los rasgos de seguridad y supervisión de los protocolos del sistema de control industrial. Las tuberías, sistemas de calefacción y de refrigeración, electricidad etc.

Son supervisados y controlados con el control de supervisión y el protocolo de adquisición de datos del SCADA. La CCI y el sistema SCADA permite la recolección de datos y análisis la cual ayuda automatizar el control del equipo como la tubería y válvulas. Un componente clave de defensa son las capas del dispositivo SCADA pues con este sistema busca reducir las amenazas de la infraestructura crítica.

Mediante el uso de datos las organizaciones tienen la ventaja de defender las redes contra amenazas cibernéticas antes de la conexión de la red. Se deben implementar capas adicionales como firewall, prevención de intrusiones, antivirus y técnicas de caja de arena ya que, una estrategia de seguridad eficaz debe detectar los ataques en tiempo real para después proporcionar información al forense para investigar las posibles amenazas.

Esto protegerá mejor los aparatos SCADA y los hará menos vulnerables a los ataques. Los hackers se hacen más inteligentes por lo tanto es esencial implementar estrategias y sistemas para proteger la red y los servicios que controlan para proteger no solamente las organizaciones sino también a la población.

2.6.2. ¿Cómo otro Estado protege la infraestructura crítica? En cuanto la protección de la infraestructura critica, es una preocupación que afecta a varios Estados o gobiernos puesto que, estas infraestructuras son de suma importancia para el desarrollo humano. Como es el caso de España, Estados Unidos y Brasil:

2.6.2.1. España. España creo el Decreto 704 de 2011 y la Ley 8 de 2011 que tiene como fin establecer medidas para la protección de las infraestructuras críticas, es decir, la infraestructura es la clave para el funcionamiento de un país. España cuenta con 3.500 infraestructuras consideradas como crítica, aunque, algunas listas son secretas, para garantizar la protección por ellos se originó las siguientes instituciones:

El Centro Nacional para la Protección de las Infraestructuras Críticas y la Secretaría de Estado de Seguridad del Ministerio del Interior es el responsable de determinar cuáles infraestructuras deberán ser catalogadas dentro de esta sección. También coordinar acciones y estrategias para asegurar las infraestructuras con operadores privados y agentes locales. El Plan de Seguridad de Operador es el que detalla la política de seguridad, el análisis de riesgos físicos y lógicos sobre el uso de medidas de seguridad, tanto preventivas como reactivas y el Plan de protección compila una serie de documentos con la finalidad de ayudar a todos los actores para la toma de medidas de emergencia en caso de un ataque (Iglesias, 2016).

Para garantizar la seguridad de la información en España creo el Mando Conjunto de Ciberdefensa que es una institución del jefe del Estado Mayor de la Defensa de España que tiene como propósito garantizar la disponibilidad, integridad y confidencialidad de la información del estado y de las personas. Entre sus funciones tenemos las siguientes:

- Dirige y coordina en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los ejércitos.

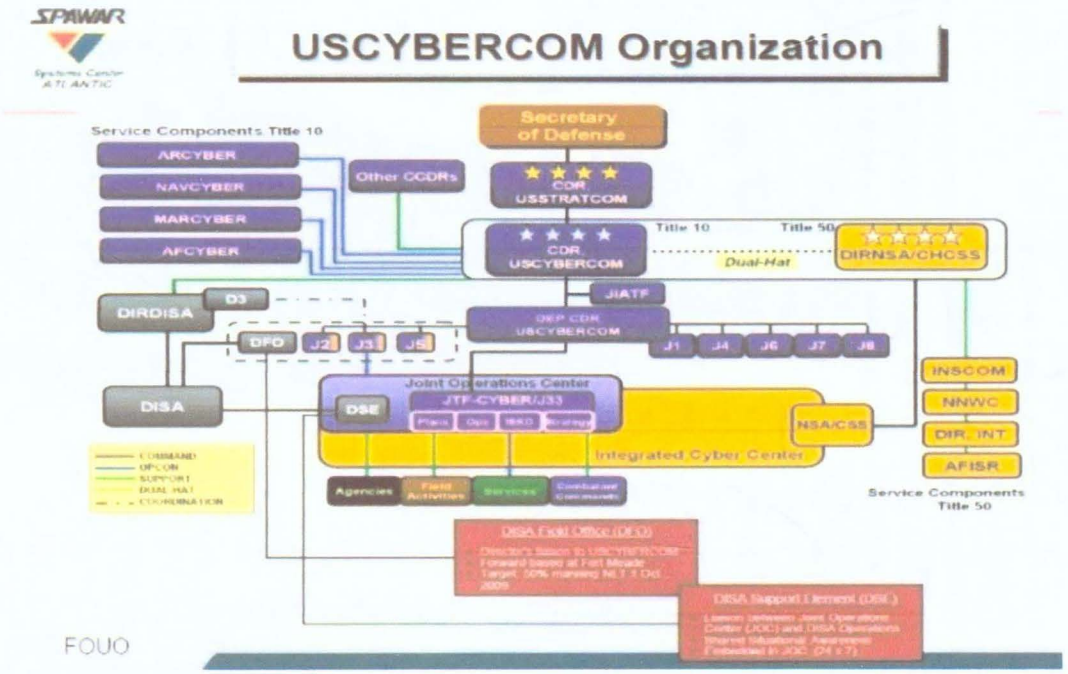
- Ejerce la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresores que puedan afectar a la Defensa Nacional.

- Define, dirige y coordina la concienciación, la formación y el adiestramiento especializado en esta materia.

- Es responsable del desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones y de la dirección y el control de cumplimiento de estas políticas (Gobierno de España, 2015).

2.6.2.2. Estados Unidos. Debido al avance del internet y los ataques cibernéticos Estados Unidos se vio en la necesidad crear un Cibercomando Militar la cual fue creado en el año 2010 este órgano tiene como misión proteger los sistemas informáticos frente ataques que son generados por otros gobiernos. El Cibercomando tiene como función planear, coordinar, integrar, sincronizar y dirigir operaciones de defensa de redes de información (Belt soluciones de seguridad global, s. f).

Figura No. 2 Estructura del Cibercomando Militar de Estados Unidos



Fuente: Imagen tomada de Belt soluciones de seguridad global

2.6.2.3. Brasil. El Comando de Defensa Cibernética de Brasil tiene como finalidad planificar, dirigir y controlar las actividades operacionales y de tecnología ya que, es un conjunto de acciones defensivas, exploratorias que busca proteger los sistemas de información.

Figura No. 3 Comando de Defensa Cibernética de Brasil

Fuente: Imagen tomada Jornadas CD16 Contribución de la Ciberdefensa a la Seguridad Nacional

2.7. La importancia de una Unidad Brigada Cibernética para Colombia

Vivimos en un mundo interconectado en donde el intercambio de datos es una necesidad para la mayoría de los ciudadanos que encuentre en internet. Pues se convirtió en la mejor herramienta para realizar actividades tales como: búsqueda de información, enviar correos electrónicos, comprar en línea, ingresar a redes sociales etc. Sin embargo, en el ciberespacio se expone a varios riesgos como el robo de datos, claves entre otros.

Para garantizar la seguridad y la infraestructura nacional el Gobierno Colombiano por medio del Documento Consejo de Política Económica y Social (Conpes 3054 del 2016) delego al Ministerio de Defensa ejercer la seguridad. Pero para logar esto, es necesario fortalecer las capacidades técnicas y tecnológicas si no también articular todos los esfuerzos civiles para que sea seguro el ciberespacio y confiable para las entidades públicas, privadas y los ciudadanos.

Este grupo está encabezado por el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) la cual, coordina todos los aspectos de ciberseguridad y ciberdefensa para

garantizar la protección de la infraestructura critica del Estado y los temas de cooperación, gestión e intercambio de información.

El Comando Conjunto Cibernético (CCOC) está conformado por las Fuerzas Militares y las unidades cibernéticas, del Ejercito Nacional, Armada Nacional y la Fuerza Área de colombiana. Proporciona la defensa del país a través de estrategias que permite prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses de la Nación. Cibernético Policial está encargado de la ciberseguridad del territorio colombiano recibiendo información, apoyo y protección ante los delitos cibernéticos, además desarrolla valores de prevención, atención, investigación, judicialización de los delitos informáticos para su operación se incorporó el comando de atención inmediata virtual para recibir todas las denuncias.

Para lograr esto se necesita de capacitación, sensibilizar, pero la más importante es cooperar. Fortalecer el intercambio de información entre todas las entidades nacionales e internacionales nos permite construir mancomunadamente un ecosistema más seguro, así como prevenir, reaccionar y mitigar las amenazas digitales. En Colombia el incremento de incidentes detectados entre el año 2014 y 2015 fue de 40% y su tendencia es creciente. Posicionando a nuestro país como uno de los más preparados y capacitados para enfrentar este tipo de actividades delictivas.

2.8. Antecedentes

Estos últimos años se han generado varios ataques cibernéticos de lo cual, pueden llegar a ser peligrosos pues, si no contamos con una unidad Ciberdefensa nos encontramos en una situación de vulnerabilidad y además estos virus tienen como objetivo paralizar completamente el país es decir que, amenaza la seguridad de la nación. Estos sucesos lo han realizado varios autores como crimen organizado, terroristas dado que, su costo es mínimo relativamente es fácil (Ministerio de Defensa, 2009).

En 1999 se comenzó a reportar numerosos ataques a dominios colombianos y tanto fue así que para el año 2002 se reportó 50 amenazas en diferentes sitios web y esto siguió prosperando que en el 2009 se recibe ataques más sofisticados según el Ministerio de Defensa Nacional (2009):

> El sistema financiero vio comprometidos alrededor de 50 millones de dólares que desaparecieron de las cuentas bancarias de personas naturales y jurídicas. En términos generales, de enero a julio de 2009 la Policía Nacional ha atendido 836 casos relacionados con amenazas cibernéticas, que van desde el robo de identidad, hasta los hurtos electrónicos, accesos abusivos a sistemas informáticos y pérdida de información sensible en las organizaciones (p. 1).

El Ministerio de Defensa Nacional (2009) afirma que ha sufrido múltiples ataques en la infraestructura, pero afortunadamente estos han sido neutralizados, sin embargo, es necesario avanzar cada día más y contar con nuevas tecnologías y personal especializado en estos temas para mejorar la defensa ya que, cada vez crean sistemas sofisticados para impedir la protección y de esta manera producir daño a la infraestructura digital. Documento Conpes 3701 (2011) indica que: Colombia ocupó el quinto puesto entre los países más afectados por esta red (ver figura 3).

Tabla No. 3 Lista de países más afectados por los ataques cibernéticos

No.	PAÍS	%
1	INDIA	19.14
2	MEXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	COLOMBIA	4.94
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55

No.	PAÍS	%
11	PERU	2.42
12	IRAN	2.07
13	ARABIA SAUDI	1.85
14	CHILE	1.74
15	KAZAKHSTAN	1.38
16	EMIRATOS ARABES	1.15
17	MARRUECOS	1.13
18	ARGENTINA	1.10
19	ESTADOS UNIDOS	1.05

Fuente: Tabla tomada del Documento Conpes 3701, P6.. (2011).

2.9. Instituciones que Garantizan la Ciberdefensa en Colombia

2.9.1. Centro de Operaciones de Seguridad Cibernética (SOC). Boto (2010) señala que: "El SOC es un centro donde se gestiona la seguridad de una organización" (p.3). El cual está

conformado por un grupo de especialistas en seguridad informática y dispositivos electrónicos, es importante que el ejército patrocine campañas para fomentar que los soldados, cadetes y altos rangos militares estudien en academias que se especialicen en ciberseguridad, informática forense que busquen formar agentes especializados para afrontar la Ciberdefensa. Un Centro de Operaciones Cibernéticas para el ejército sería una gran ventaja puesto que, en nuestro país dicho centro se encuentra de forma independiente, que ayudaría como herramienta para los problemas que no pudieran solucionar los centros de seguridad existentes en el país.

2.9.2. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). Según el Documento CONPES 3701 (2011) "El centro de coordinación de seguridad informática en Colombia está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas" (p.12). Colombia cuenta con el Centro de Coordinación de Seguridad Informática CSIRT-CCIT (2016) "Que tiene la función de atender incidentes de seguridad informática, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas" (p. 1). Este sistema "es un punto de contacto nacional, mediante el cual la comunidad nacional e internacional puede comunicarse con las más grandes empresas proveedoras de Internet" (CSIRT-CCIT, 2016, parr.5).

2.9.3. Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT). Es una entidad del Estado encargada de coordinar el tema de la Ciberseguridad y Ciberdefensa en el territorio colombiano, el COLCERT (2013) fue creado para "la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional" (parr.1). El grupo de respuestas a emergencias cibernéticas (2013) tiene las siguientes funciones:

A. Coordinar y asesorar a CSIRT'S entidades tanto del nivel público, como privado y de la sociedad civil para responder ante incidentes informáticos.

B. Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.

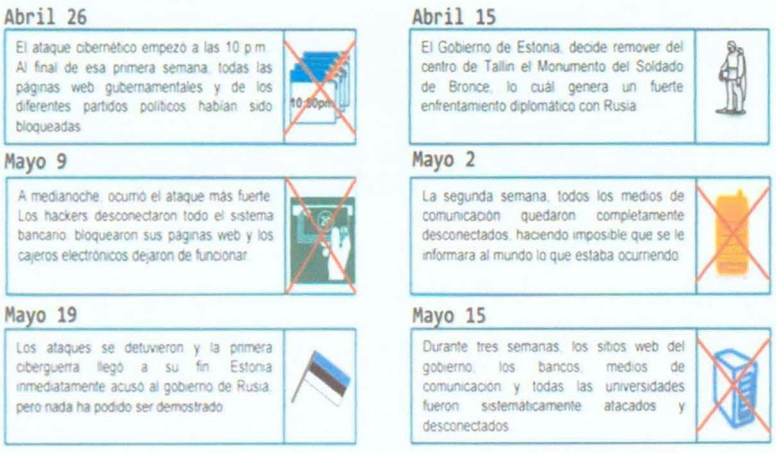
c. Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta técnica. (parr.4).

2.9.4. Comando Conjunto Cibernético (CCOC). El presente comando cumple con las funciones de "la defensa cibernética del Estado, responder a los ataques cibernéticos, asegurar la protección de la infraestructura crítica y defender las redes informáticas militares" (Dialogo Revista Militar, 2016, parr.8). El Comando Conjunto Cibernético ha sido posible por medio de la alianza de las fFuerzas Militares y la ayuda de expertos en Ciberdefensa.

2.10. Casos de Ciberdefensa

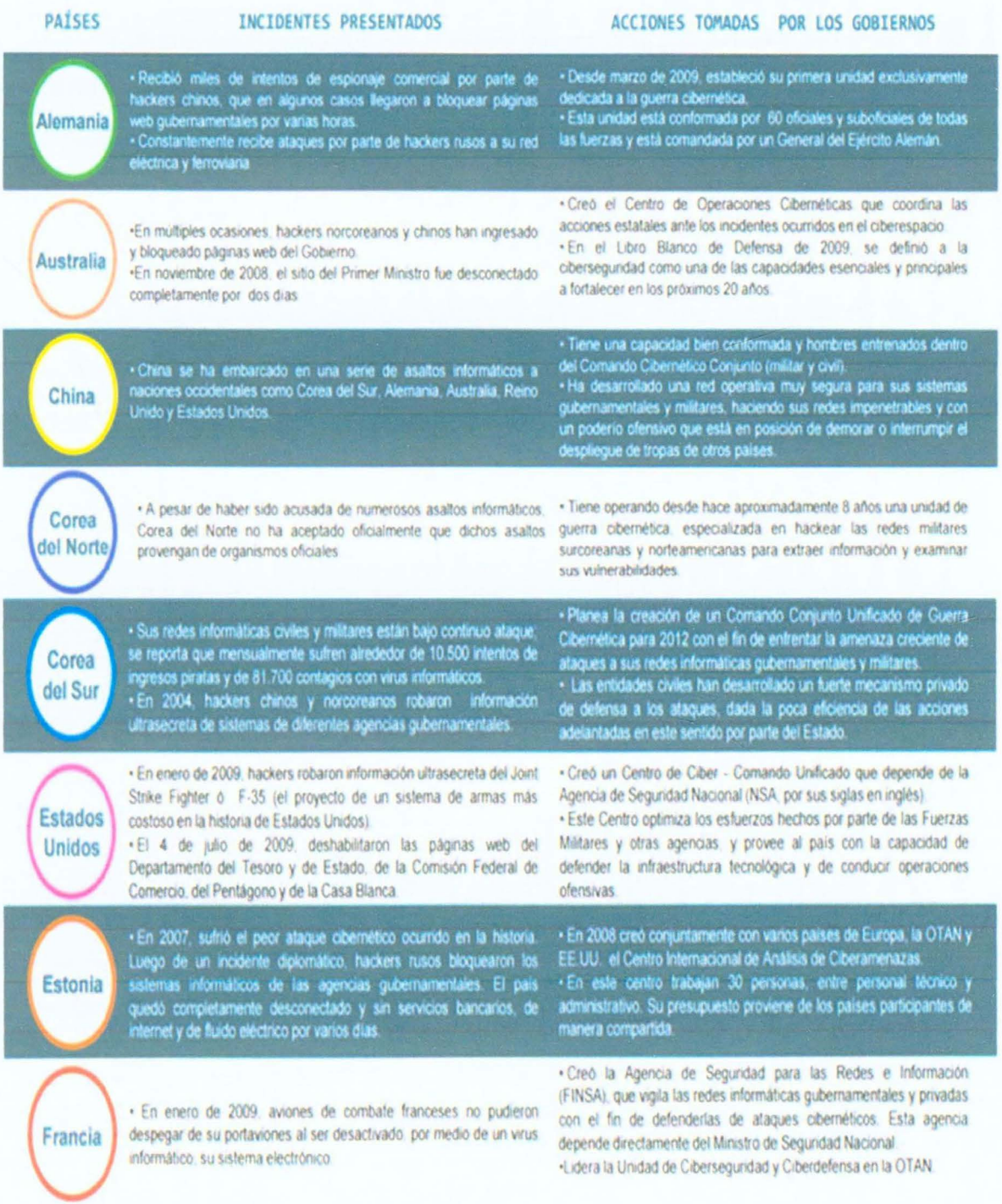
2.10.1. Estonia. Fue uno de los casos más representativos de estos ataques pues, en el año 2007 Estonia sufrió el primer ataque cibernético en el cual, afecto la presidencia, el parlamento, los ministerios, los partidos políticos y bancos. Este ataque genero una crisis que requirió de la intervención de la Organización del Tratado del Atlántico Norte. Debido a este suceso en el 2008 se creó el Centro de Excelencia para la Cooperación en Ciberdefensa con el fin de proteger a sus miembros de este tipo de ataques y entrenar al personal militar, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad (Documento Conpes 3701, 2011).

Figura No. 4 Ataque cibernético de Estonia



Fuente: Imagen tomada del Ministerio de Defensa Nacional. (2009). p. 3.

Figura No. 5 Casos de ataques cibernéticos



Fuente: Imagen tomada del Ministerio de Defensa Nacional. (2009). p. 2.

2.11. Ejército Nacional de Colombia

1.11.1. Importancia de una Brigada Cibernetica para el Ejército Nacional de Colombia. Actualmente el Ejército Nacional de Colombia no cuenta con una unidad de Ciberdefensa en el cual, esta institución puede estar en una situación de vulneralidad pues, cada día se aumenta las amenazas y ataques cibernéticos en desmedro de la seguridad nacional. Utilizando la intervención de las comunicaciones o a veces neutralizando los sistemas de mando y control para bloquearlo. Por lo tanto, es necesario crear una unidad de Ciberdefensa para el Ejército Nacional de Colombia además tiene como función proteger la soberanía de Colombia contra cualquier amenaza interna o externa. Es por ello, que todo:

> Estado soberano tiene la obligación de proteger su infraestructura cibernética. Cualquier deterioro en la misma, no sólo afectaría al ciudadano común, sino también numerosos aspectos gubernamentales, industriales y del comercio. Algunos tipos de amenazas cibernéticas son: el espionaje, robo, sabotaje de servicios, terrorismo informático, operaciones de información entre otros (Ministerio de Defensa, 2009, p. 1).

2.11.2. Objetivos de una Brigada Cibernetica para el Ejército Nacional de Colombia. El objetivo es crear una unidad de Ciberdefensa para el Ejército Nacional de Colombia, la cual pueda proteger la infraestructura crítica de la institución y del país asignado bajo su responsabilidad. Esta unidad se realiza operaciones de defensa pasiva y defensa activa en todo el territorio Nacional. El principal objetivo de la Unidad de Ciberdefensa del Ejército Nacional de Colombia es que forme parte del control y protección de los datos informáticos del Estado colombiano debido a que, el mundo digital al ser tan libre podría originar que organizaciones criminales y terrorista atentara contra la nación.

El Documento CONPES 3854 (2016) Considera importante "involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas" (p.3). Generando la posibilidad de incluir en la protección del ciberespacio colombiano. La directiva permanente, en las políticas de seguridad de la información para el Sector Defensa (2014) ha apoyado "la creación de los respectivos Equipos de Respuesta a Emergencias Informáticas

(CSIRT) y Centros de Operaciones de Seguridad (SOC), con el propósito de apoyar a la gestión" (p.6). Los objetivos de una unidad de ciberdefensa para del Ejército Nacional de Colombia son:

2.11.2.1. Objetivo global. El objetivo general es lograr que el Ejército Nacional de Colombia haga un correcto uso de los sistemas de información y telecomunicaciones, por lo tanto, se debe implementar capacidades de defensa, detección, y respuesta a los ataques cibernéticos. El fortalecimiento de la ciberseguridad genera una confianza para utilizar las TIC. Por esta razón los organismos responsables deben trabajar para garantizar la seguridad y la confiabilidad de la información. Para lograr la protección de la información y las infraestructuras críticas es necesario potenciar, impulsar y reforzar las capacidades militares.

2.11.2.2. Objetivo I. Garantizar que los sistemas de información y telecomunicaciones posean un adecuado nivel de ciberdefensa mediante la implantación de un marco coherente que ayude a proteger la información y la infraestructura critica. Además, se debe mejorar las capacidades militares de defensa y de inteligencia para reforzar la seguridad de la información y de esta manera poder enfrentarse a nuevas amenazas del ciberespacio.

2.11.2.3. Objetivo II. Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones es de suma importancia porque es el patrimonio tecnológico de Colombia y lo podemos definir como aquellos materiales que sustentan la propiedad intelectual que conforma el presente y condicionan en el futuro.

2.11.2.4. Objetivo III. Busca potenciar las capacidades de prevención, detección, reacción, análisis, recuperación y respuesta frente a las actividades del terrorismo ya que las TIC constituye un fin, para las organizaciones terroristas que tiene como propósito atacar los servicios esenciales o infraestructuras críticas.

En ambos casos se deben diseñar mecanismos de prevención, detección, reacción, análisis entre otras para poder enfrentar estas formas de criminalidad, por lo tanto, es necesario el fortalecimiento de la cooperación judicial articulando instrumentos de colaboración e intercambio de información y la armonización de una legislación nacional.

2.11.2.5. Objetivo IV. Sensibilizar a la comunidad en general de los riesgos que origina el ciberespacio pues es una función fundamental promover una cultura de ciberdefensa, que proporcione a todos los actores conciencia y la confianza necesaria para reducir la exposición de ciberataques, mediante la adopción de medidas que garantice una protección a la información.

2.11.2.6. Objetivo V. Tiene como objetivo el Ejército Nacional de Colombia alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas para que la unidad de ciberdefensa garantice una protección a la información y así mismo disponga de un personal cualificado para poder fomentar las capacidades tecnológicas para enfrentar a las diferentes amenazas cibernéticas.

2.11.2.7. Objetivo VI. Ejército Nacional de Colombia busca mejorar la ciberdefensa en el ámbito internacional la cual se promueve esfuerzos dirigidos para conseguir un ciberespacio seguro mediante una colaboración internacional, creando relaciones de confianza para el intercambio de información.

A continuación, se presenta en la Tabla No.4 donde se podrá comprender mejor los temas analizados anteriormente:

Tabla No. 4 Resumen de los objetivos

Objetivos una Brigada de Ciberdefensa para el Ejercito Nacional de Colombia	
Objetivo Global	Lograr que el Ejército Nacional de Colombia haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.
Objetivo I	Garantizar que los Sistemas de Información y Telecomunicaciones posean un adecuado nivel de ciberdefensa y resiliencia.
Objetivo II	Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones.

Objetivo III	Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
Objetivo IV	Sensibilizar a la comunidad en general sobre los riesgos derivados del ciberespacio.
Objetivo V	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita el Ejército Nacional de Colombia para sustentar todos los objetivos de ciberdefensa.
Objetivo VI	Contribuir a la mejora de la ciberdefensa en el ámbito internacional.

Fuente: Tabla tomada del Gobierno de España. (2013). Estrategia de Ciberseguridad. p. 10.

2.11.3. Funciones de una Brigada de Ciberdefensa para el Ejército Nacional de Colombia. Las funciones de la unidad de ciberdefensa del Ejército Nacional de Colombia son:

2.11.3.1. Proteger la información digital compuesta por todos los activos tecnológicos del ejército. Los ataques cibernéticos a páginas gubernamentales han generado que una de las principales preocupaciones del Estado colombiano sea proteger la información confidencial. Que en manos equivocadas podría perjudicar a la seguridad de los entes gubernamentales. Por esta razón, es necesario crear una unidad de Ciberdefensa para el Ejército Nacional para que pueda proteger la información de la misma institución y de los ciudadanos.

2.11.3.2. La realización de operaciones cibernéticas de defensa pasiva y activa con la finalidad de proteger la infraestructura digital del país asignada al Ejército Nacional. Según las políticas de Seguridad de la Información para el Sector Defensa (2014) indican que todo ente que haga parte del sector defensa deberá:

- Proteger los recursos de información y tecnología utilizados para su procesamiento. Frente a amenazas internas y externas, deliberadas o

accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.

- Implementar un Sistema de Gestión de Seguridad de la Información para el Sector Defensa, orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información en las instituciones y entidades del sector. (p.4).

2.12. Capacidades en la Ciberdefensa

1.12.1. Definición. Podemos definir la capacidad militar de ciberdefensa como aquel centro que busca ayudar a reducir los ciberataques producidos por estados extranjeros, organizaciones terroristas, hacktivistas etc. López (2013) indica que "la capacidad militar de ciberdefensa se basa en el concepto de un centro de ciberdefensa que provee el apoyo técnico y la coordinación para poder contrarrestar los ataques cibernéticos y desplegar acciones ofensivas y de respuesta activa" (p. 11). La capacidad en ciberdefensa tiene como finalidad garantizar una protección eficaz frente a las ciberamenazas la cual, incluye aspectos como: organizativos, procedimentales y tecnológicos

2.12.2. Objetivos de la capacidad. Según López (2013) los objetivos de la capacidad son:

- Coordinar servicios de apoyo y creación de políticas.
- Coordinar la capacidad de apoyo a las respuestas ante incidentes de seguridad cibernética
- Ejecutar y coordinar ciberoperaciones.

2.12.3. Responsabilidades de la Capacidad. Para López (2013) las responsabilidades de la capacidad son:

- Preparación de capacidades y garantizar la protección de activos militares y críticos (civiles).
- Analizar los incidentes.

2.12.4. Tipos de capacidades. Para Camacho (2016) tenemos los siguientes tipos de capacidades:

2.12.4.1. Capacidad de análisis y fuga de información. Tiene como finalidad proteger y respaldar la información la cual e provee, direcciona y da soporte a la administración de la información. Con esta capacidad se pretende hacer lineamientos para mantener actualizado los controles de protección de la información, de acuerdo a las necesidades de la Institución y además brinda apoyo en capacitación a las unidades militares con respecto al tema de protección de la información.

1.12.4.2. Capacidad de búsqueda y recolección de Información. Esta capacidad tiene como propósito actualizar la base de datos para averiguar las posibles amenazas que atenta contra la integridad de la información como perdida, daño, fuga etc. Para lograr con este objetivo se realiza una búsqueda y recolección de información para saber después como realizaron el ataque y así mismo capacitar al personal. Al presentarse un ataque se hace una recolección de información para generar un perfil del atacante y lograr neutralizar en tiempo real los ciberataques.

2.12.4.3. Capacidad de planificación, ejecución y mitigación. Esta capacidad tiene como fin diseñar políticas y normas técnicas e internacionales que busquen garantizar la seguridad de la información. Con esta normativa se establece procesos, procedimiento y protocolos en la que hace seguimientos, auditorías, inspecciones y verificaciones del cumplimiento de las políticas de protección de la información. A través de herramientas tales como: software y hardware se puede mitigar la ocurrencia de amenazas cibernéticas.

2.12.4.4. Capacidad de análisis y control. En esta capacidad se analice los sistemas de información con el fin de controlar, implementar, alimentar y actualizar estadísticas de incidentes informáticos y verificar el cumplimiento de las políticas de seguridad mediante inspecciones de seguridad de la información.

Para consolidar la unidad de Ciberdefensa para el Ejército Nacional de Colombia es necesario implementar capacidades con el fin de garantizar la ciberseguridad y Ciberdefensa, por ello en la Tabla No. 3 enuncia las siguientes:

Tabla No. 5 Capacidad de ciberseguridad y Ciberdefensa

Al beneficiarnos de los ilimitados recursos de las redes públicas de datos como internet y de la infraestructura tecnológica interconectada, también nos enfrentamos a nuevos escenarios para el delito, el terrorismo y la guerra, lo cual exige la creación de nuevas herramientas de prevención, reacción y defensa. Para consolidar una capacidad suficiente de ciberseguridad y ciberdefensa, es necesaria una estrategia alrededor de las siguientes áreas de concentración:	
Sistemas Seguros y Resistentes	Estándares y protocolos que permitan proteger los ciberataques a todos los sectores. Esto requiere un buen entendimiento de las posibles vulnerabilidades y sus correspondientes impactos.
Doctrina y Normatividad	Ajuste de los marcos jurídicos y reglamentarios, realizados conjuntamente por instancias públicas y privadas. Generación de una doctrina conjunta para el control de ciberespacio.
Sensibilización y Cambio Cultural	Conciencia generalizada de la importancia del uso del ciberespacio como un medio para alcanzar objetivos de seguridad nacional. Implementación de los cambios de comportamiento y de cultura del

	trabajo que requiere un ambiente seguro.
Roles y Misiones	Definición de funciones y objetivos específicos entre los diferentes componentes teniendo en cuenta su misionalidad y sus capacidades de cada una de estas. Es imperativo, evitar duplicidad de funciones y de gasto de recursos.
Compromiso Internacional	Coherencia del trabajo nacional con el de Estados amigos y organizaciones internacionales relevantes. Revisar la evolución de los temas concernientes al ciberespacio, recoger lecciones aprendidas, compartir buenas prácticas con los aliados estratégicos y proponer enmiendas, si estas son requeridas.
Educación y Capacidades de Investigación y Desarrollo	Fomento de la educación y experticia en temas de ciberseguridad y ciberdefensa. Esto implica entrenamiento específico, acreditaciones y la eventual implementación de una carrera profesional. Estar atento de las tendencias globales y asegurar que los esfuerzos en investigación y desarrollo estén dirigidos y coordinados hacia los objetivos trazados.
Infraestructura y Equipamiento	Capacidades de alertar de manera temprana de los posibles ataques a la infraestructura de información nacional, ya sea pública o privada, por parte de criminales, terroristas u otros estados. Capaz de repeler dichos ataques y de contraatacar estratégicamente el agresor.

Fuente: Tabla tomada de Camacho. (2016). Evolución de la ciberdefensa. p. 16.

2.13. Actividades para garantizar la Ciberdefensa. Vargas (2014). afirma que para garantizar la protección de la información se debe realizar las siguientes actividades:

2.13.1. Según la prevención.

2.13.1.1. Análisis y fuga de Información. Se realiza actividades de análisis para determinar los posibles casos de fuga de información para luego neutralizar dichas amenazas.

2.13.1.2. Búsqueda de fuga de información. Esta actividad tiene como finalidad neutralizar las fugas de información y así evitar la difusión no autorizada, clasificada o sensible.

2.13.1.3. Análisis de la información. En el análisis de la información se hace una gestión de incidentes cibernéticos por medio de softwares para poder neutralizar las amenazas que atenta contra la confidencialidad, disponibilidad o integridad de la información.

2.13.1.4. Desarrollo tecnológico. Se realiza implementación de nuevas tecnologías con el fin de mantener actualizadas las herramientas y garantizar la efectividad de la protección de la información.

2.13.2. Según la de la detección.

2.13.2.1. Contrasabotaje. Por medio de Malware busca detener o neutralizar cualquier actividad de sabotaje hacia los activos de la nación.

2.13.2.2. Contraespionaje. Este tiene como finalidad detectar el robo información, evitando que se materialice el espionaje dirigido para obtener información sobre la infraestructura critica de una nación.

2.13.2.3. Explotación. El objetivo de esta actividad es hacer inteligencia a la amenaza y conocer las capacidades de la misma, y con base a la información estructurar una medida de protección para asegurar la infraestructura tecnológica.

2.13.2.4. Proyectos especiales. El proyecto especial tiene como propósito estar actualizado en los diferentes campos tecnológicos en lo referente a la seguridad de la información y ciberdefensa

2.13.3. Según la neutralización.

2.13.3.1. Mitigación. Para enfrentar los ciberataques cibernéticos se realiza capacitación al personal para que se mantenga actualizados sobre temas de ciberdefensa.

2.13.3.2. Análisis de Riesgos. Se previene las amenazas mediante la evaluación de riesgos.

2.13.3.3. Contra subversión cibernética. Realiza actividades de prevención de ataques hacktivistas aplicando técnicas y tácticas anti desfiguración de sitios web, antiphising, ataques a dispositivos móviles.

III. PROPUESTA DE CREACIÓN DE UNA BRIGADA DE CIBERNETICA PARA EJÉRCITO NACIONAL DE COLOMBIA

3.1. Antecedentes y Desarrollo del Problema

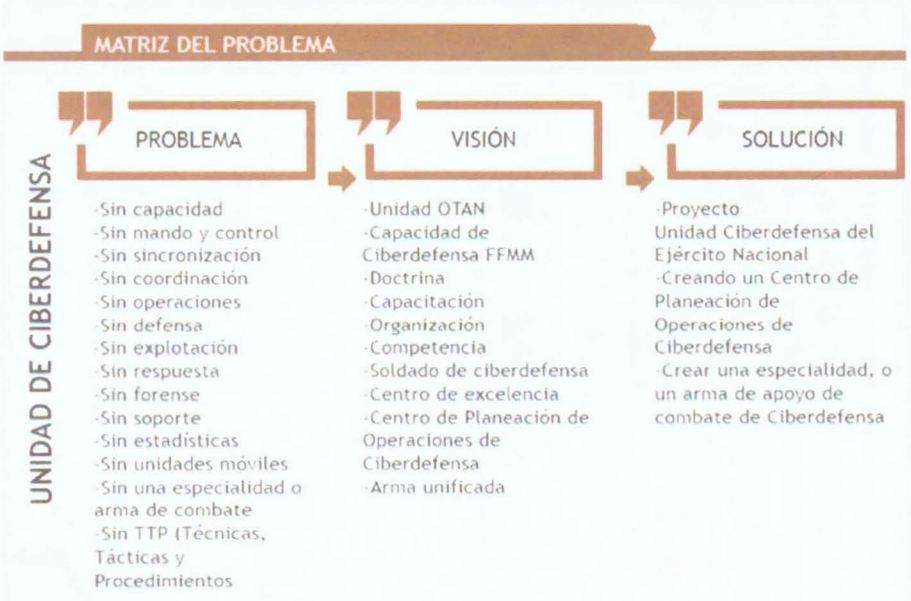
El Internet se ha convirtiendo rápidamente en el medio a través del que podrían producirse grandes catástrofes pues centrales nucleares, cadenas de televisión, infraestructuras militares están conectados a una red de intranet. Lo que más preocupa de esta situación es que algunos ataques son tan sofisticados que ni siquiera se pueda dar dé cuenta de que fueron atacados. Por es de suma importancia que el Ejército Nacional de Colombia cuente con una unidad de ciberdefensa y una nueva especialidad de arma para desarrollar capacidades presentes y futuras hacia el año 2030 qué es la fase 3 de transformación y también para que se pueda defender de estos ataques cibernéticos que antes se consideraba como una guerra cibernética pues ahora es una forma de vandalismo.

Los ordenadores y las redes pueden ser bastantes útiles, pero se pueden utilizar también como armas que atenta contra seguridad de la información de instituciones, estados y ciudadanos. El método que se utilizó para la creación de esta unidad es el comité de revisión estratégico de Innovación (CREI) que usa la planeación por capacidades y la alineación con las variables del DOMPILEM. Como El Ejército Nacional de Colombia no tiene una unidad de Ciberdefensa unificada esto ha generado que las capacidades estén dispersas, debilidades que exista una falta de: organización doctrina, personal, entrenamiento, infraestructura y lo mismo sucede con el apoyo de operaciones Cibernéticas como no está articulada las dos armas se encuentra en encabeza del ejercito que son: Comunicaciones e Inteligencia por lo tanto, el ejército debe incluir las demás armas para tener las capacidades alineadas. El arma de Comunicaciones Militar posee una capacidad doctrinal de inteligencia y la Ciberinteligencia la capacidad es de explotación.

Todas estas falencias ocasionan fenómenos de ciberataque, ciberterror y ciberpiratas, dado que la doctrina es dispersa, las capacidades de ciberdefensa son insuficientes y no está integrada al DOMPILEM, no hay una doctrina basada en roles y misiones de cada arma, el personal es insuficiente, la organización no está acorde a la capacidad, no existe doctrina en: defensa, explotación, respuesta y análisis forense, no tiene laboratorio de ciberoperaciones ofensivas-

defensivas de estabilización y resiliencia, no cuenta con recursos humanos capacitados y no hay una especialidad o cuerpo de ciberdefensa. Los problemas anteriormente mencionados se producen porque que el Ejército Nacional de Colombia no tiene una unidad de ciberdefensa ni tampoco tiene un arma de ciberdefensa con soldado cibernéticos. Por esta razón no hay doctrina, entrenamiento y operaciones de ciberdefensa. Y esto ocasiona que no se pueda articular las capacidades que tiene el ejército en Comunicaciones e Inteligencia (Ver Figura 7).

Figura No. 6 Matriz del problema



Fuente: Elaboración propia del autor.

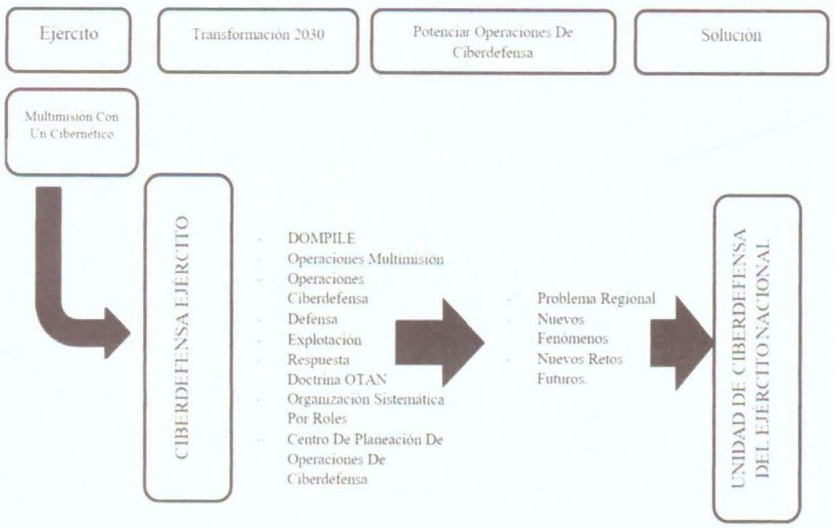
3.2. Visión del Ejército 2030

La visión del Ejército Nacional es tener la capacidad de proteger el Ciberespacio con una unidad que cumpla con los siguientes requisitos:

- Tendrá capacidad de defensa.
- Explotación soporte forense.
- Capacidad soporte.
- Capacidad forense.
- Respuesta y operaciones especiales como elemento estratégico disuasivo.

Matriz de transformación y sincronización de capacidad en Ciberdefensa para potenciar la unidad unificada de mando y sistemática por roles misionales (Ver Figura 8).

Figura No. 7 Matriz de transformación y sincronización de Ciberdefensa



Fuente: Elaboración propia del autor.

3.3. Solución del Proyecto

El proyecto tiene como finalidad hacer una propuesta de creación de una unidad ciberdefensa y un arma de combate para el Ejercito Nacional de Colombia la cual recoja estudios y experiencias de otros ejércitos que han tenido ataques cibernéticos como es el caso del Ejército de Estados Unidos. Estos problemas lo solucionaron a través de la unificación de organizaciones, doctrinas y métodos de operación en el ciberespacio. Todo esto sin perder la identidad y lograr una sinergia operacional.

3.3.1. El Comando Cibernético del Ejército de los EE. UU (ARCYBER). Según Wikipedia (s. f) el Comando Cibernético del Ejército de los EE. UU es un componente de servicio del Ejército USSTRATCOM que apoya el Comando Cibernético de los Estados Unidos. La cual busca dominar información de las operaciones del ciberespacio este comando tiene como

propósito ser el punto de contacto del Ejército para organizaciones externas. Este punto único de contacto consigue un doble control para el Comando Cibernético y el ejército (Ver figura 9).

Figura No. 8 Escudo del Comando Cibernético del Ejército de los Estados Unidos

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos. (s. f).

3.3.1.1. Misión. El Comando Cibernético del Ejército de los Estados Unidos tiene como función dirigir y conducir operaciones de ataques cibernéticas y operaciones ciberespaciales que busca garantizar la protección del ciberespacio y el entorno de la información (Wikipedia, s. f).

3.3.1.2. Organización. Según Wikipedia (s. f) el Comando Cibernético del Ejército de los EE. UU tiene la siguiente organización:

- Comando de tecnología empresarial de la red Army
- El Comando de Inteligencia y Seguridad del Ejército (INSCOM) estará bajo el control operacional de Army Cyber para acciones relacionadas con el ciberespacio.
- 1er Orden de Operaciones de Información (Tierra) (1 ° IO CMD (L)

- 1er Batallón: entrena y despliega apoyo de campo, evaluación de la vulnerabilidad y equipos de sensibilización de OPSEC.

- 2d Batallón - Conduce operaciones de la fuerza cibernética del ejército en centros de entrenamiento militar en todo el mundo.

- 780a Brigada de Inteligencia Militar (Cyber) (párr. 10).

3.3.1.3. Historia. Los oficiales asignados al Comando Cibernético del Ejército de los Estados Unidos asisten a un Cyber Ball del Ejército el 22 de octubre de 2011. El ejército logró una capacidad operativa cibernética inicial en octubre de 2009 al emplear el Comando Estratégico de las Fuerzas Armadas del Ejército y Misiles de Defensa apoyado por NETCOM. El comando originalmente fue anunciado para ser nombrado Comando Cibernético de las Fuerzas Armadas (ARFORCYBER). El comando se estableció el 1 de octubre de 2010 con el nombre de Comando Cibernético del Ejército (Wikipedia, s. f).

3.3.1.3. Escudos y distintivos de ciberdefensa de Estados Unidos. Los escudos de la ciberdefensa de Estados Unidos son:

Figura No. 9 Comando cibedrnetico de Estados Unidos

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 10 Comando cybernetico de ejercito

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 11 Distintivo para el uniforme del comando cybernetico de ejercito

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 12 Distintivo del arma de ciberdefensa

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 13 Distintivo del arma de ciberdefensa para el uniforma nuemro 3

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 14 Distintivo del arma de ciberdefensa para el uniforma camuflado

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

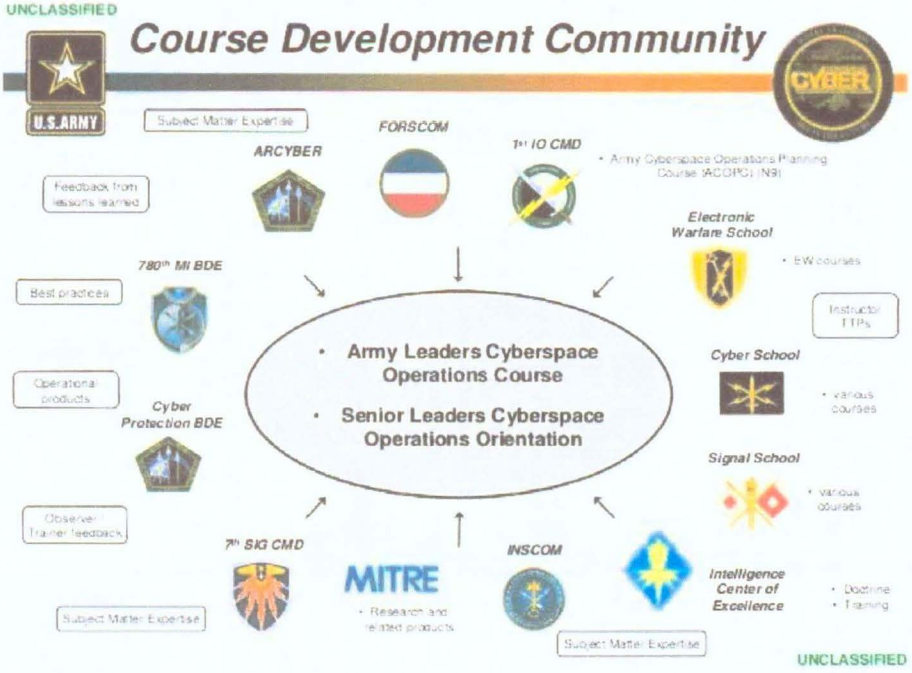
Figura No. 15 Distintivo del cuerpo ciberdefensa

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 16 Escuela de Ciberdefensa

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 17 Cursos de Ciberdefensa

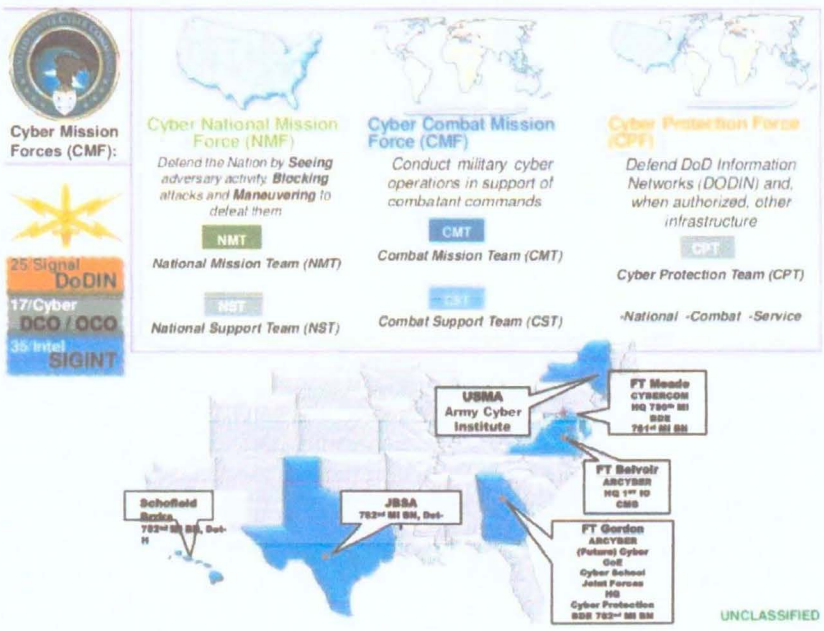


Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 18 Comando Cibernetico del Ejercito

Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

Figura No. 19 Operaciones del Comando Cibernetico del Ejercito



Fuente: Imagen tomada de Comando Cibernetico del Ejercito de Estados unidos (s. f).

3.4. Brigada de Ciberdefensa para el Ejército Nacional

3.4.1. Misión. Brigada de Ciberdefensa para el Ejército Nacional de Colombia tendrá como misión la protección de las infraestructuras críticas cibernética del ejército y asignada a nivel nacional en el ciberespacio fortaleciendo la capacidad de defensa explotación y respuesta con la finalidad de proteger los intereses de la nación, la soberanía, la independencia, la integridad de territorio nacional y el orden constitucional establecido en la Constitución de Colombia.

3.4.2. Visión. La Brigada de Ciberdefensa para el Ejército Nacional de Colombia se conforma como un subsistema estratégico disuasivo para el ejército nacional siendo potencia regional y mundial. Con doctrina educación y entrenamiento que le permita realizar operaciones multidimensional. Teniendo como columna vertebral la investigación, el desarrollo y la innovación.

3.4.3. Objetivos. Los objetivos de la Brigada de Ciberdefensa para el Ejército Nacional de Colombia son:

- Diseñar una organización de Ciberdefensa que integré toda la capacidad de Ciberdefensa del ejército.
- Desarrollar una doctrina de Ciberdefensa.
- Diseñar un manual de Ciberdefensa para el Ejército Nacional de Colombia.
- Reorganizar el personal de comunicaciones y de inteligencia que estén en las capacidades de Ciberdefensa y Ciberinteligencia mediante la creación de una unidad tipo comando y una especialidad de arma de Ciberdefensa.
- Apoyar operaciones de armas combinadas terrestre.
- Organizar el personal de comunicaciones e inteligencia en el sistema de Ciberdefensa.

- Adquirir infraestructura de Ciberdefensa para defensa.
- Unidades de Ciberdefensa (Comando de Ciberdefensa).
- Crear un arma de Ciberdefensa especialidad que agrupe a todo el personal de Comunicaciones e inteligencia.
- Crear una especialidad en el ejército llamada cuerpo, o arma de Ciberdefensa.

3.4.4. Entrenamiento.

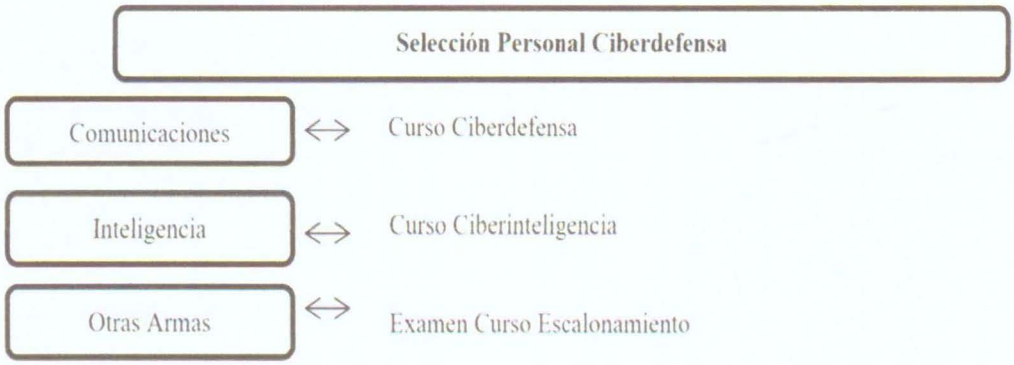
Figura No. 20 Pirámide de entrenamiento

Fuente: Ealboracion propia del autor.

3.4.5. Operaciones Multidominio. La guerra moderna tiene diferentes dominios terrestre, marítimo, aéreo, espacial y Ciberdefensa. Este dominio Cibernético es el nuevo campo de combate. Se debe tener un ejército entrenado y sincronizado que permita realizar operaciones de multidominio de defensa. Además, que sea una organización que cuente con un comando de control unificado la cual se pueda planear y desarrollar operaciones eficaces en el ciberespacio.

3.4.6. Selección de Personal.

Figura No. 21 Personal



- Individual por armas
- Crear una especialidad. (presillas)
- Crear un arma nueva de combate

Fuente: Elaboración propia del autor.

La selección del personal de Ciberdefensa es muy importante para mantener la capacidad. El entrenar un personal es muy costoso y emplearlo mal debilita el subsistema de Ciberdefensa. Las armas del ejército tales como: comunicaciones en ciberdefensa y ciberinteligencia entrenan el personal para desempeñarse en estos roles de dominio Cibernético. Para que la capacidad del subsistema tenga una sinergia que permita al personal estar listo y entrenado para la defensa y seguridad se debe unificar de la siguiente manera:

- Individual por armas (Cómo está hoy en día)
- Crear una especialidad y cuerpo Ciberdefensa
- Crear un arma de Ciberdefensa

3.4.7. Alternativas

3.4.7.1. Individual por arma. Sistema que compone la necesidad de Ciberdefensa cómo son comunicaciones e inteligencia actúan de acuerdo a su rol específico como hasta ahora se está haciendo, pero con los mismos problemas que no hay un ente articulado que permita desarrollar operaciones de Ciberdefensa como un solo cuerpo o arma con un mando unificado. Es difícil de lograr el objetivo teniendo dos armas de apoyo de combate que siempre quiere tener la superioridad y dominio de la capacidad de cibernética. Por esta razón para poder tener Comando y Control unificado planeamiento y eficiencia en la ejecución de operaciones de defensa, explotación y respuesta. Se recomienda tener organizada la unidad de Ciberdefensa del Ejército. Se deben tener en cuenta varios aspectos importantes para esta alternativa:

Mandó unificado qué es el jefe de operaciones del ejército o jefe de Estado Mayor de operaciones y designar un Brigadier General para que articule la capacidad y siendo el comandante del comando de Ciberdefensa. Para lograr planeación de operaciones con roles y misiones unificados sin conflicto se activa el centro de planeación de operaciones de Ciberdefensa el cual debe tener dos oficiales Superiores de Comunicaciones y dos de inteligencia con la finalidad de articular las unidades de Comunicaciones inteligencia en defensa explotación y respuesta. Así como otras capacidades de soporte forense y operaciones especiales, para poder realizar el planeamiento de una operación de Ciberdefensa. Pero si se aprueba la organización de un arma de Ciberdefensa ya no se nombra Inteligencia y Comunicaciones solo personal y el grado requerido.

3.4.7.2. Crear una especialidad de Ciberdefensa. El ejército se debe crear un cuerpo como unidad que integra la capacidad como se hizo con las unidades de fuerzas especiales o actuales de policía militar. Que cuando un miembro integra una de estas unidades recibe unas presillas con la insignia del arma de Ciberdefensa y el grado respectivo según su jerarquía militar.

Esto permite que cada mujer y hombre que ingrese a una unidad de ciberdefensa pueda trabajar en defensa, explotaciones y respuesta, así como en las capacidades adicionales todo esto sin pensar en que son de un arma o de otra, sino que son un solo componente. Eso sería una solución para tener un solo subsistema y se agregaría al centro de planeación de operaciones de

Ciberdefensa igual como la alternativa anterior. Y nombrar un señor Brigadier General que articule el comando y control de la unidad. Para concluir se debe:

- Crear un cuerpo, especialidad o arma de Ciberdefensa.
- Crear un comando de Ciberdefensa.
- Crear el Centro de Planeación de Operaciones de Ciberdefensa.
- Nombrar un general para tener comando y control unificado de la capacidad cibernética del Ejército.

3.4.7.3. Crear un arma nueva. Con la anterior alternativa, el número dos es el paso inicial para crear una nueva arma de Ciberdefensa. Tener un arma de Ciberdefensa sería lo ideal para desarrollar una capacidad unificada. Esto permitirá el crecimiento del subsistema en todas las áreas del DOMPILEM, tener una doctrina, instrucción y entrenamiento, así como infraestructuras y unidades organizacionales con comando y control.

- Doctrina
- Instrucción y Entrenamiento
- Infraestructura
- Organización
- Operaciones
- Perfil de carrera
- Una escuela del arma
- Personal altamente capacitado
- I+D+i
- Independencia tecnológica
- TTP
- Unidades listas en defensa-explotación y respuesta
- Relevos generacionales

Esto se complementa como en las alternativas anteriores con un centro de planeación de operaciones de Ciberdefensa que permita desarrollar operaciones de Ciberdefensa y desplazar

unidades a cualquier teatro de operaciones y apoyar las operaciones multidominio. De las tres alternativas esta es la más recomendable la última debe tener un arma de Ciberdefensa y un centro de planeación de operaciones de Ciberdefensa y nombrar un general lo cual permite regular la capacidad defensa explotación y respuesta empleando unidades móviles con efectos adecuados en apoyo de la misión asignada para proteger la infraestructura crítica del ejército. Para concluir se debe:

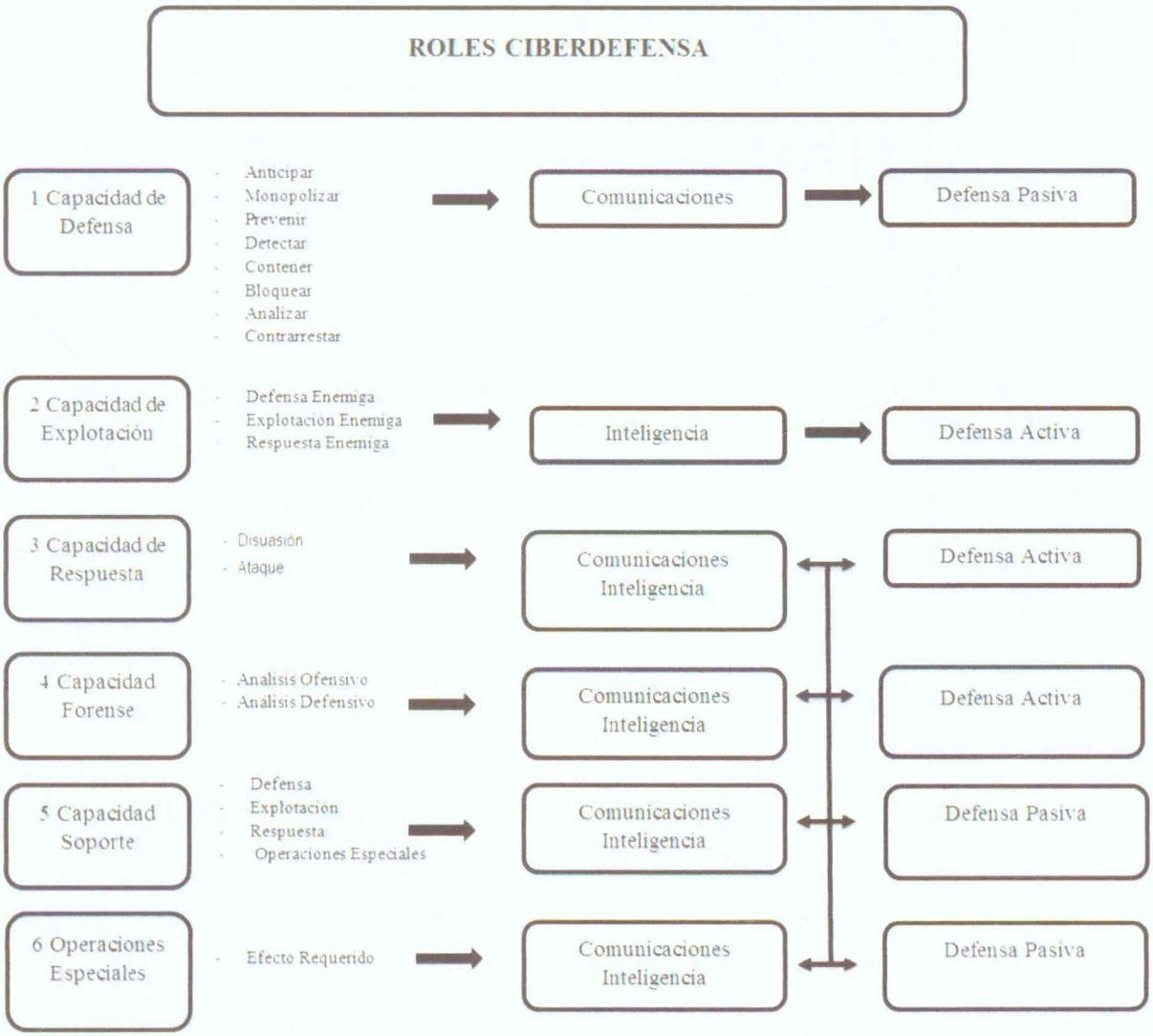
- Nombrar un Brigadier General.
- Crear un arma de ciberdefensa.
- Crear un Comando de Ciberdefensa con un centro de Planeación de Operaciones de Ciberdefensa.

Esta última recomendación es la que otros países ya tomaron, y es como enfrentan las amenazas cibernéticas en el ciberespacio. Los países más avanzados llevan en desarrollo de esta capacidad 7 años, Colombia lleva 5 años en desarrollo lo que significa que la brecha solo es de 2 años, con países más avanzados tomar este ejemplo en organización y operaciones permite cerrar esta brecha, la cual nos permite tener soldados cibernéticos en defensa, explotación y respuesta, un comando de Ciberdefensa o cibernético, un arma de Ciberdefensa y un comandante del comando de Ciberdefensa.

Así mismo, como la escuela que dicta sus respectivos cursos de Ciberdefensa que ya existe y la maestría en la Escuela Superior de Guerra: con lo anterior seriamos ejército modelo en el desarrollo de la capacidad y listos para los nuevos retos y fenómenos operacionales en el ciberespacio.

3.4.8. Roles de Ciberdefensa.

Figura No. 22 Roles



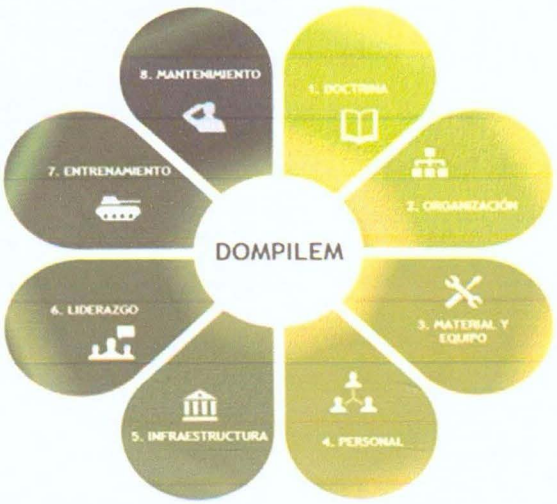
Fuente: Elaboración propia del autor.

Como se muestra en la Figura No. 23 en la actualidad el ejército solo tiene capacidad de defensa y de explotación, las otras capacidades tales como: forense, soporte y operaciones especiales no están integradas a la institución. Estas capacidades deben concentrarse en una unidad cibernética de grado comando con soldados cibernéticos que realice operaciones militares

en el que sincronice el comando y apoye al comandante terrestre para mantener la seguridad y defensa de la nación.

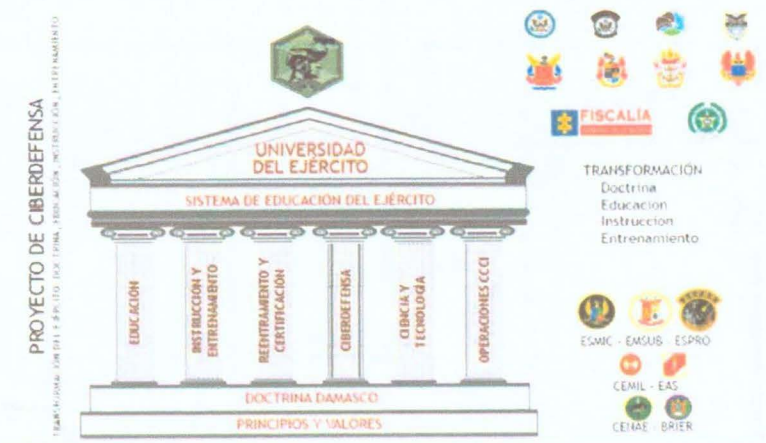
3.4.9. EL CREI. En el año 2016 fue realizado el CREI de Ciberdefensa que determina la cadena de valor y capacidades específicas de defensa de explotación y respuesta. Pero se dejaron por fuera unas capacidades como son: la capacidad de forense, soporte y operaciones especiales (Ver Figura No. 24).

Figura No. 23 Dompilem



Fuente: Ejercito Nacional de Colombia.

Figura No. 24 Proyecto de Ciberdefensa



Fuente: Elaboración propia del autor.

La cadena de valor definida en el trabajo del CREI, también se definió los roles de los subsistemas de inteligencia y comunicación. La capacidad de defensa de explotación y respuesta se dejó unas áreas de capacidad específica por afuera que afectan la capacidad de Ciberdefensa. En defensa pasiva (defensa) y una defensa activa (respuesta de explotación). Dejó por fuera capacidades especificas cómo son capacidad forense, capacidad de soporte y capacidad de operaciones especiales. Estas cuatro capacidades son fundamentales para el desarrollo de una capacidad estratégica real de Ciberdefensa. Las cuales son transversales a defensa pasiva y defensa activa cómo podemos observar en la Figura No. 23.

Es muy importante tener claro que hay capacidades que no son exclusivas de defensa pasiva o defensa activa porque, se requieren en ambas y su forma de actuar es diferente lo que permite que su forma de construcción y empleo táctico técnico y de procedimientos (TTP), son particulares en su usabilidad. Por eso se requiere de un arma de Ciberdefensa. Es muy importante tener una visión holística y flexible del empleo de la capacidad del Ciberdefensa por ser un campo de operaciones desconocido e irregular, de esto depende tener una capacidad de planeamiento mental estratégico, lateral irregular y diferencial.

3.4.10. Alineación de la Educación.

Figura No. 25 Educación

Fuente: Elaboración propia del autor.

Para poder desarrollar una unidad Ciberdefensa para el ejército Nacional de Colombia con capacidades, con un mando, un control adecuado y soldados cibernéticos, es muy importante alinear todo el sistema de Educación militar. Tener en primer lugar el comando de Educación y doctrina con sus unidades operativas menores y sus diferentes escuelas de formación y las escuelas de capacitación. Si no se realiza está alineación recomendada no se puede sostener la organización de un subsistema de Ciberdefensa que permita tener un personal formado, entrenado y capacitado permitiendo los relevos generacionales y el crecimiento de la doctrina de Ciberdefensa y Ciberinteligencia en un solo cuerpo cibernético. Revisemos muy rápidamente la función de las escuelas de formación y escuelas de capacitación y el papel importante que ella realizan siendo el soporte de los sistemas de las armas de combate de un ejército y los conceptos nuevos de armas combinadas, comando y control, interoperabilidad, la polivalencia, la guerra de espectro total, la sincronización, el ejército módulos multimisión. Los multidominios de la guerra y ciberseguridad como elemento estratégico de defensa de un país (Ver Figura No. 26).

3.4.10.1. Escuelas de formación. Tiene la responsabilidad de capacitar oficiales de planear, dirigir y tomar decisiones estratégicas operacionales y tácticas. Estos son la cabeza jerárquica de la pirámide de un Ejército. Por eso es muy importante tener la materia prima que permite la continuidad de los oficiales que dirigen el ejército e integran la especialidad de Ciberdefensa.

Es importante tener oficiales de Comunicaciones y de inteligencia para poder nutrir la especialidad de un arma de ciberdefensa. Con la escuela de suboficiales se cumple el mismo proceso de garantizar la escala de sucesión del mando de las diferentes armas subsistemas de comunicaciones e inteligencia para integrar la unidad de Ciberdefensa del ejército. Se debe tener claridad que cualquier oficial, suboficial, soldado y civil que tenga la competencia y habilidad lo puede hacer después de la selección integral de las unidades de ciberdefensa.

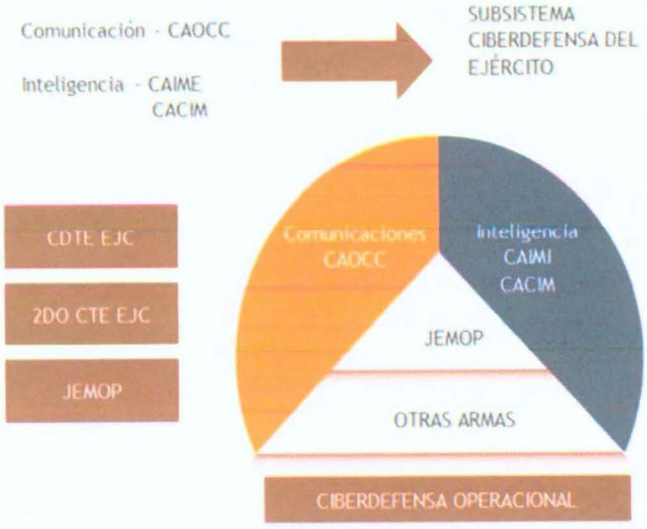
3.4.10.2. Escuelas de capacitación y en las armas. Tiene la función de especializar el militar en competencias propias de armas y subsistemas en cuanto a la especialidad de Ciberdefensa. La escuela de comunicaciones militares y la escuela de inteligencia y contrainteligencia del ejército son las encargadas de capacitar a los hombres que trabajan en ciberdefensa la escuela de comunicaciones dicta el curso de Ciberinteligencia uno para oficiales y otro para suboficiales y la escuela inteligencia y contrainteligencia dicta el curso de Ciberdefensa para oficiales y

suboficiales de la armada inteligencia de esta forma se tienen los cuadros que la unidad de ciberdefensa y ciberinteligencia requieren pero con la connotación grande de debilidad de trabajar en forma separada y no articulado por esta razón se plantea más adelante del centro de planeación de operaciones de ciberdefensa y la creación de un arma con un comandante unificado.

Por otra parte, estas dos escuelas son las encargadas de dictar capacitaciones entrenamiento de ciberdefensa y ciberinteligencia a todas las armas del ejército y seleccionar el personal que pueda integrar las unidades de Ciberdefensa por eso, es tan importante la alineación de la educación del ejército porque es la única forma de fortalecer la institución. Por último, se encuentra la Escuela Superior de Guerra la cual dicta la maestría en Ciberseguridad y Ciberdefensa en la que se capacita los oficiales en el arte de la estrategia al más alto nivel, para comandar las unidades militares y policiales.

3.4.11. Alineación de las Armas (Comunicaciones - Inteligencia).

Figura No. 26 Ciberdefensa operacional



Fuente: Elaboración propia del autor.

Se plantea la integración de las armas de comunicaciones de inteligencia y otra arma para poder conformar el subsistema de Ciberdefensa. Cada subsistema entrena y desarrolla capacidades con roles específicos que ya, fueron tratados en las líneas anteriores y está al

servicio de las operaciones cibernéticas. Teniendo una estructura subordinada con una cadena de comando y control la cual se explica con claridad el empleo de Ciberdefensa y la toma de decisiones del uso de la capacidad de los controles necesarios para evitar mal empleo o violar la ley.

Se plantean seis niveles de autorización para el empleo de la capacidad de Ciberdefensa del ejército en apoyo de las operaciones militares multidimensional. Para la defensa de explotación y respuesta tres complementarios que son: soporte, forense y operaciones especiales. En una operación de defensa y forense la autorización es parte del SOC (Centro de Operaciones de Seguridad) en la parte de defensa.

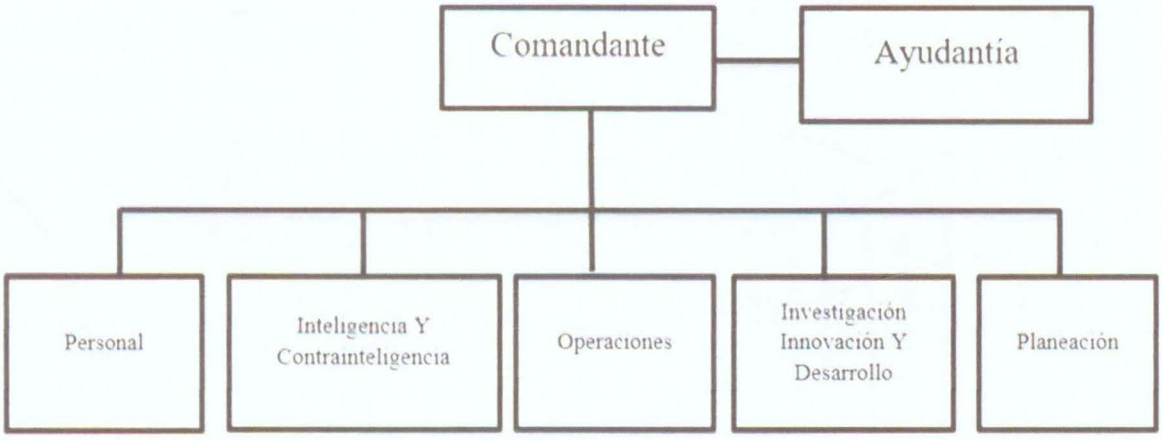
Las otras capacidades deben tener unos niveles de autorización muy estrictos con roles y misiones perfectamente establecido, pero con la flexibilidad, articulación y sincronización que permita el desarrollo de operaciones en tiempo, modo y lugar realizado el efecto ordenado y necesario para apoyar al comandante de la operación.

3.4.12. Jerarquía de Comando, Control y Toma de Decisiones de la Capacidad de Ciberdefensa. El comandante del ejército cuando esté comprometido el nivel estratégico de seguridad, defensa nacional y la infraestructura crítica, debe hacer operaciones de respuesta de ataque en el dominio Cibernético. El comandante del ejército cuando esté comprometido la infraestructura crítica del ejército y su supervivencia digital el Jefe de Estado Mayor de operaciones desarrollan operaciones normales del ejército nacional.

Comandante comando de ciberdefensa del ejercito planea y desarrolla operaciones cibernéticas en apoyo a las operaciones del Jefe de Estado Mayor de Operaciones con tácticas propias de ciberdefensa. Centro de planeación de operaciones de ciberdefensa es el encargado de tener los analistas y planeadores de todas las operaciones de ciberdefensa, con las herramientas adecuadas para cada efecto requerido, en apoyo de una operación militar o en defensa de la integridad digital del Ejército y la infraestructura critica nacional, así como la seguridad nacional.

3.4.13. Organización Unidad Cibernética –Tipo.

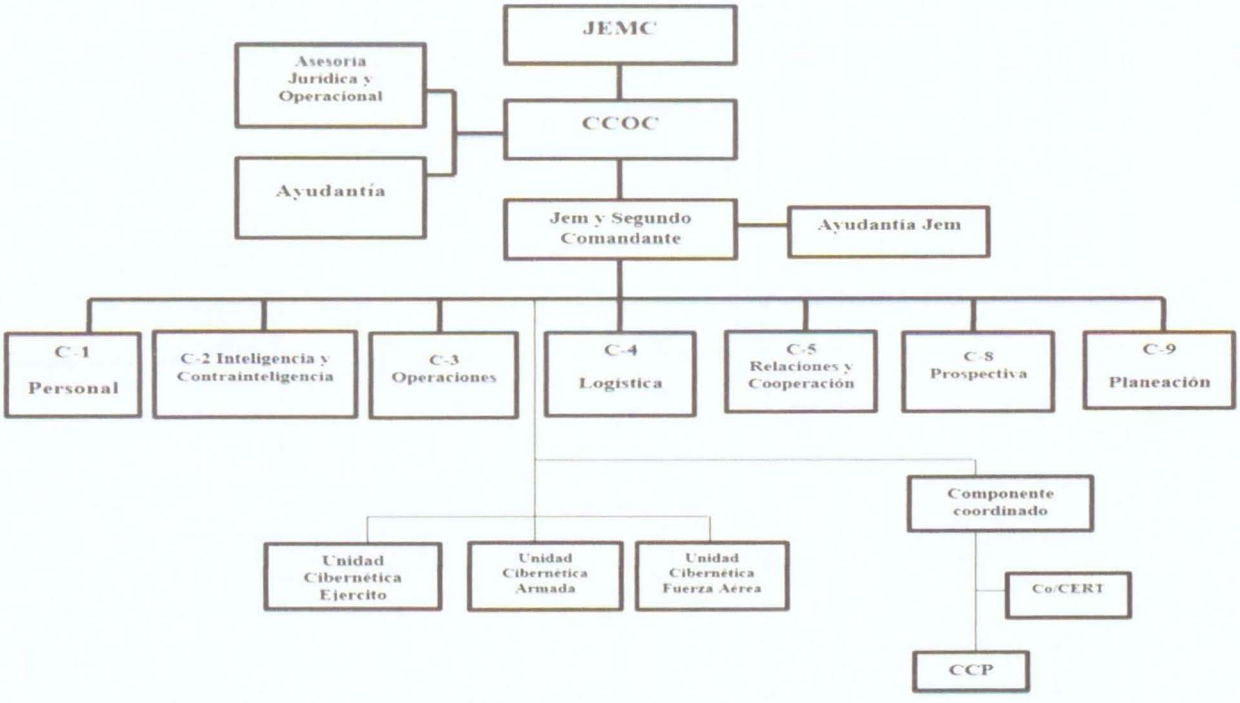
Figura No. 27 Estructura de la Unidad cibernética



Fuente: Comando Conjunto Cibernético (CCOC).

3.4.14. Organización Comando Conjunto Cibernético.

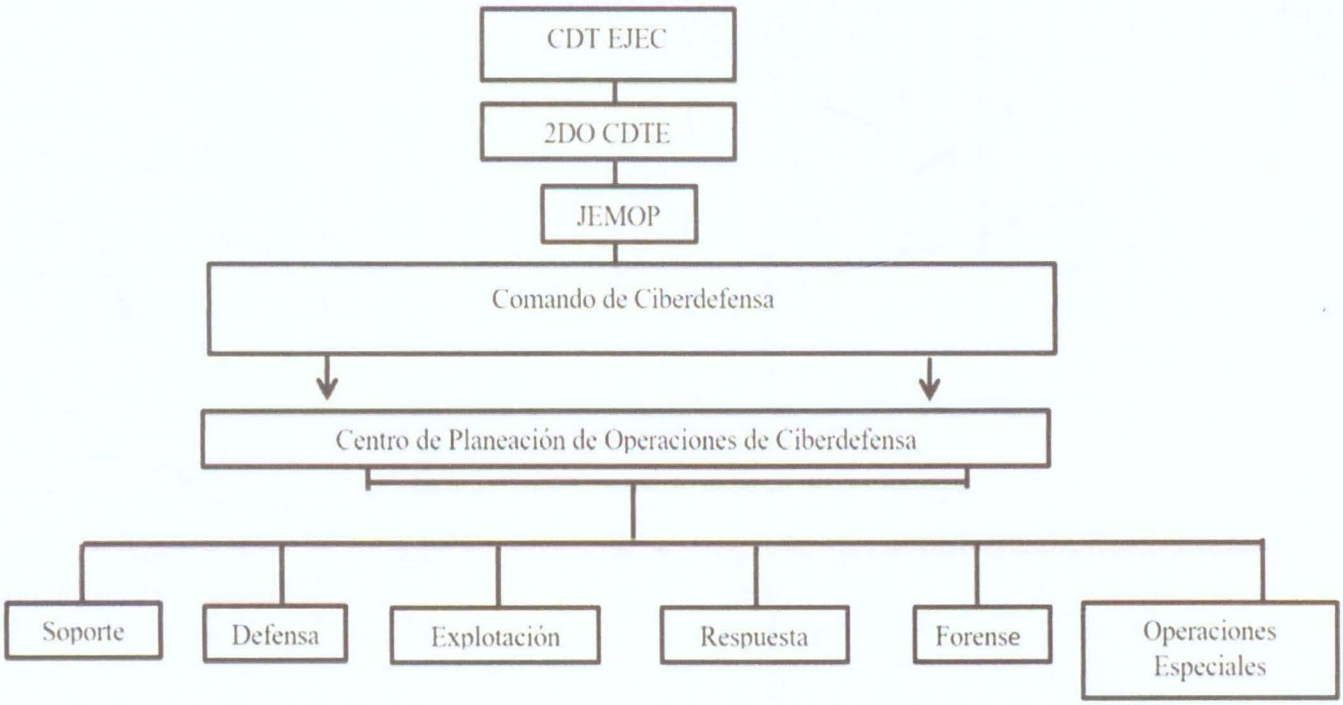
Figura No. 28 Estructura del Comando Conjunto Cibernético



Fuente: Comando Conjunto Cibernético (CCOC)

3.4.15. Recomendación de la creación Brigada de Cibernetica para el Ejército Nacional de Colombia

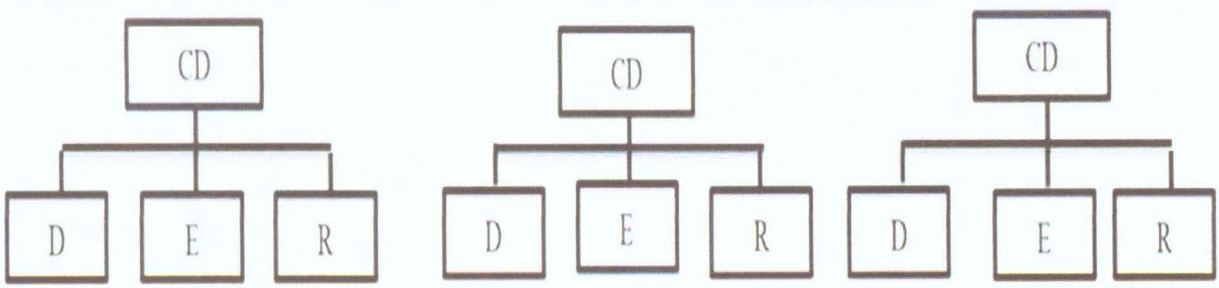
Figura No. 29 Creación Brigada de Cibernetica para el Ejército Nacional de Colombia



Fuente: Elaboración propia del autor.

3.4.16. Batallones de Ciberdefensa de Despliegue.

Figura No. 30 Estructura de Batallones de Ciberdefensa de Despliegue



Fuente: Elaboración propia del autor

3.4.17. Brigada Cibernética del Ejercito Nacional de Colombia. En las líneas anteriores tratamos parcialmente este tema cuando hablamos de la jerarquía de comando y toma de decisiones de Ciberdefensa. Profundizaremos por ser una de las innovaciones junto con la conformación de una especialidad en el ejército como arma de Ciberdefensa.

El comandante del Ejército Nacional de Colombia toma una estrategia defensiva de ciberdefensa donde debe disponer de los medios que sean necesarios para potenciar la capacidad de ciberdefensa; en razón a que un ataque cibernético se considera como un riesgo a la integridad de las tropas comprometidas en el desarrollo de operaciones militares y una agresión de la defensa y seguridad de la nación.

Por tal razón se planea el diseño de una organización que permita la articulación de los roles y funciones de las armas que poseen la capacidad de ciberdefensa, con la finalidad de poder emplear esta capacidad estratégica en forma integrada, articulada y sincronizada facilitando la protección del dominio cibernético. Permitiendo una superioridad en el ciberespacio mediante operaciones de ciberdefensa para defender la infraestructura critica del ejército y de la nación.

Esta unidad debe tener los analistas y planeadores de todas las operaciones de Ciberdefensa, con las herramientas adecuadas para cada efecto requerido, en apoyo de una operación militar o en defensa de la integridad digital del ejército, la infraestructura crítica nacional, la seguridad nacional, así como realizar operaciones multidimensionales en defensa explotación respuesta soporte forense y operaciones especiales, con un mando unificado y control centralizado. También tiene una lista de unidad de despliegue estratégico en apoyo a las divisiones y comandos del ejército. Cuenta con el siguiente personal:

01. Brigadier General – como comandante
02. Coroneles - uno de inteligencia y uno de comunicaciones, especialistas en ciberdefensa.
02. Tenientes coroneles con la misma especialidad
01. Asesor jurídico operacional con especialización en derecho digital

Es un estado mayor de planeación encargado de planear la operación de ciberdefensa y los efectos a emplear y minimizar el daño operacional, el error militar y el daño colateral que no debe existir. Esta nueva organización de la unidad de Ciberdefensa del Ejército Nacional de

Colombia será el paso inicial de una fusión de dos armas de inteligencia y comunicaciones dando paso a un cuerpo de ciberdefensa y un arma de apoyo de combate cibernética; con un centro de planeación y ejecución de operaciones de ciberdefensa la cual tendrá una articulación, sincronización con Comando y control unificado interoperable modular multidimensión y positivamente para hacer frente a las amenazas en el ciberespacio con una unidad modelo efectivo, eficiente y eficaz.

3.4.18. Objetivos. Brigada Cibernética del Ejercito Nacional de Colombia tendrá los siguientes objetivos:

- Comando, control y toma de decisiones centralizado.
- Fusión de capacidades de ciberdefensa mediante la unión de las dos armas de inteligencia y comunicaciones, mientras se unifica una sola especialidad y una sola arma de apoyo de combate o un cuerpo de ciberdefensa.
- Planeamiento de operaciones centralizado.
- Sinergia de capacidades.
- Tener técnicas, tácticas y procedimientos estandarizados.
- Doctrina de Ciberdefensa.
- Unidades de movilidad en apoyo a las divisiones y comandos.
- No hacer dobles esfuerzos.
- Tener una estrategia de Ciberdefensa para el ejército.

- Unificar las escuelas de capacitación con una sola doctrina operacional de Ciberdefensa.
- Tener una unidad de ciberdefensa del ejercito con todas sus capacidades lista para el ciberespacio con capacidades unificadas.

3.4.19. Financiación. La financiación del presente proyecto se garantiza hasta el año 2030 con recursos de DNP. Ejército Nacional hace cinco años la capacidad de ciberdefensa fue de carácter prioritario. Por esta razón se matriculo en la Dirección Nacional de Planeación (DNP) un proyecto de Ciberdefensa que permitiera desarrollar y sostener las unidades de Ciberdefensa.

Este proyecto se basa en la doctrina, entrenamiento, infraestructura y desarrollo de capacidades permanentes. Cuenta con una hoja de ruta de actividades por año y un tiempo de duración hasta el año 2030. De la misma forma y en apoyo del desarrollo de la capacidad de ciberdefensa el Ejército Nacional de Colombia mediante las armas de comunicaciones y de inteligencia destina presupuestos internos de sus armas para financiar la capacidad cibernética. De lo anterior expuesto se puede evidenciar que Ejercito Nacional de Colombia tiene una estrategia para el desarrollo de esta capacidad de cuerdo a la política del gobierno nacional y el sector defensa.

Por otra parte, hay que buscar otras formas de financiar la ciberdefensa, la capacitación del personal, así como las herramientas. El estar preparado depende en gran parte de los presupuestos que el gobierno nacional financie para tener unidades de Ciberdefensa y Ciberseguridad que permitan proteger los intereses de la nación.

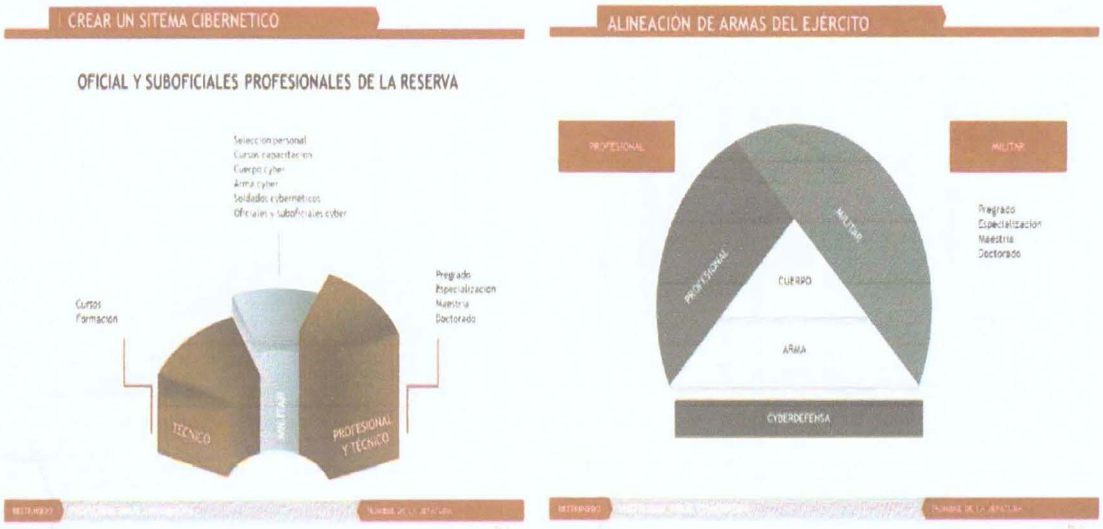
3.4.20 Conformación de de Unidades Especializadas.

Es indispensable tener personal que integren esta nueva especialidad, los relevos generacionales y la experiencia son indispensables para poder tener una capacidad cibernética permanente. Por esta razón se plantea formar soldados cibernéticos. Como se menciona anteriormente se toma de las armas de comunicaciones de inteligencia y de todo lo demás armas que cumplan con el perfil el proceso y el proceso de selección. Pero este proceso se realiza entre el personal de oficiales suboficiales y soldados con él atenuante que son susceptibles después de ser entrenados qué

cualquier empresa los quiera contratar perdiendo el personal la capa altos de capacitación y entrenamiento.

Por esta razón se plantea una opción qué es hacer cursos para oficiales profesionales de reserva, pero también crear esta condición para suboficiales profesionales de reserva. Este personal recibiría instrucción militar de formación puede ser contratado por la institución y seguir en su empleo normal. Pero la gran ganancia es que son profesionales y técnicos muy especializados los cuales llegan formados en estas especialidades generando gastos muy bajos para la institución y que como ya mencioné se puede contratar por horas mensuales o permanentes. Así quedaría completo el personal profesional. Cómo se presenta en la gráfica creación sistema Cibernético y alineación de armas del ejército (Ver figura 31).

Figura 31. Sistema Cibernetico y Alineación de Armas del Ejercito.



Al análisis de la Gráfica de capacidades de TIC y cibernética mediante la forma C-5 la cual explicare de la siguiente forma. C-5 está compuesto por la concentración de capacidades de comando, control, comunicaciones. computadores y ciberdefensa,lo que permite concentrar y fusionar todos estas capacidades articulándolas en defender los sistemas de telecomunicaciones, más la capacidad cibernética. Hay unos componentes adicionales el de comandar y controlar los cuales hablaremos así. El comandar permite la toma de decisiones en tiempo real sin tener qué escalonar a otras instancias perdiendo activos y colocando en peligro las infraestructuras críticas.

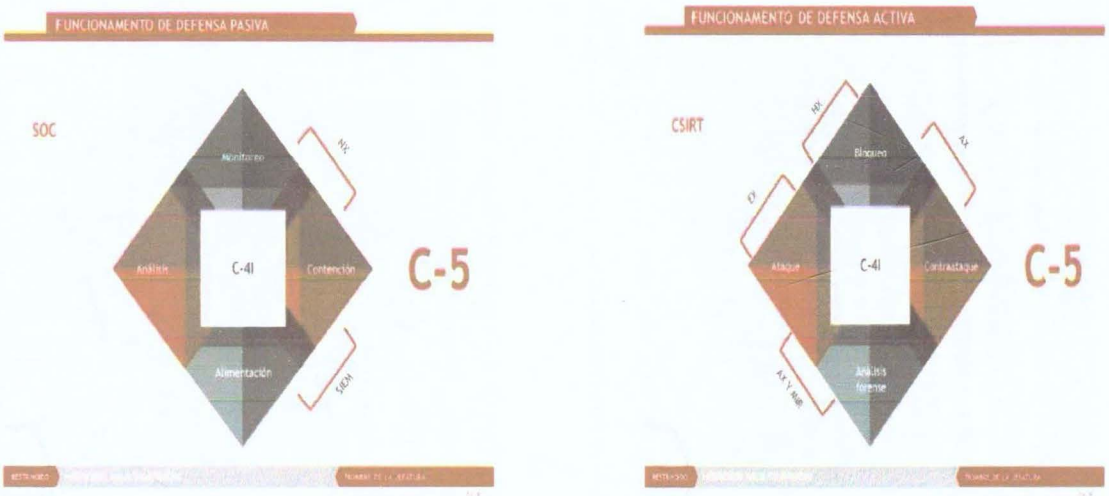
Las comunicaciones y computadores nos permiten tener la función de las telecomunicaciones facilitando minimizar los riesgos mediante controles y una política establecida para la protección centro de datos y redes de Comunicaciones más seguros y con una sola cadena de Mando y decisión. La capacidad cibernética o ciberdefensa es la última que se articulada con la finalidad que esta capacidad permita asegurar las otras cuatro capacidades C-4 qué nos permite operar las telecomunicaciones, Es lo que da vida a los sistemas cibernéticos mediante la adquisición de herramientas de Ciberdefensa cómo son los SOC unidades de defensa.

Pero también da el paso a la defensa activa combinando las capacidades de respuesta que CSIRT que permite tener integrado la capacidad de defensa y de respuesta ante eventos cibernéticos. Por esto se conforma en un C-5 que militar o empresarialmente permite hacer sinergia para evitar ataques cibernéticos a infraestructura crítica. (ver figura 32).

Figura 32. Productos innovadores.

GAOCC esta organización concentra y desarrolla las capacidades C-5 así como hacen la integración de operación de seguridad de telecomunicaciones y ciberdefensa mediante la operación de los activos de Comunicaciones e informática. Adicionalmente el SOC y el CSIRT. Todo esto con un mando uniformado con capacidad de tomar decisiones sobre la infraestructura crítica asignada (ver figura 33).

Figura 33. Gráficos explicativos C-5 Para Defensa Pasiva y Defensa Activa.



3.4.21 Herramientas cibernéticas.

En la pirámide siguiente se muestran diferentes herramientas lo más importante no es comprar de todo, es tener una conciencia con que se cuenta en el mercado, para qué se usa cada cosa, pero analizando cómo fueron elaboradas está tecnologías cuales permite realizar en defensa y en respuesta. Porque con este análisis se puede terminar las principales amenazas presentes, pero también poder determinar las amenazas que no están definidas hoy. Las que seguramente serán los ataques del futuro. Esto permitirá poder seleccionar cuáles son los principales riesgos de la infraestructura crítica y así efectuar los controles mediante el uso de política de seguridad y adquirir las herramientas necesarias.

En la parte de seguridad y defensa cibernética este mismo análisis permite hacer una prospectiva de cómo serán los nuevos ataques cibernéticos desde la creatividad de un atacante, las fallas de seguridad de software y Hardware y la debilidad de la ingeniería social para de esa manera poder estar mejor preparado y potenciar los centros de investigación de (I + D + i) investigación desarrollo e Innovación de Ciberdefensa (Ver figuras 34).

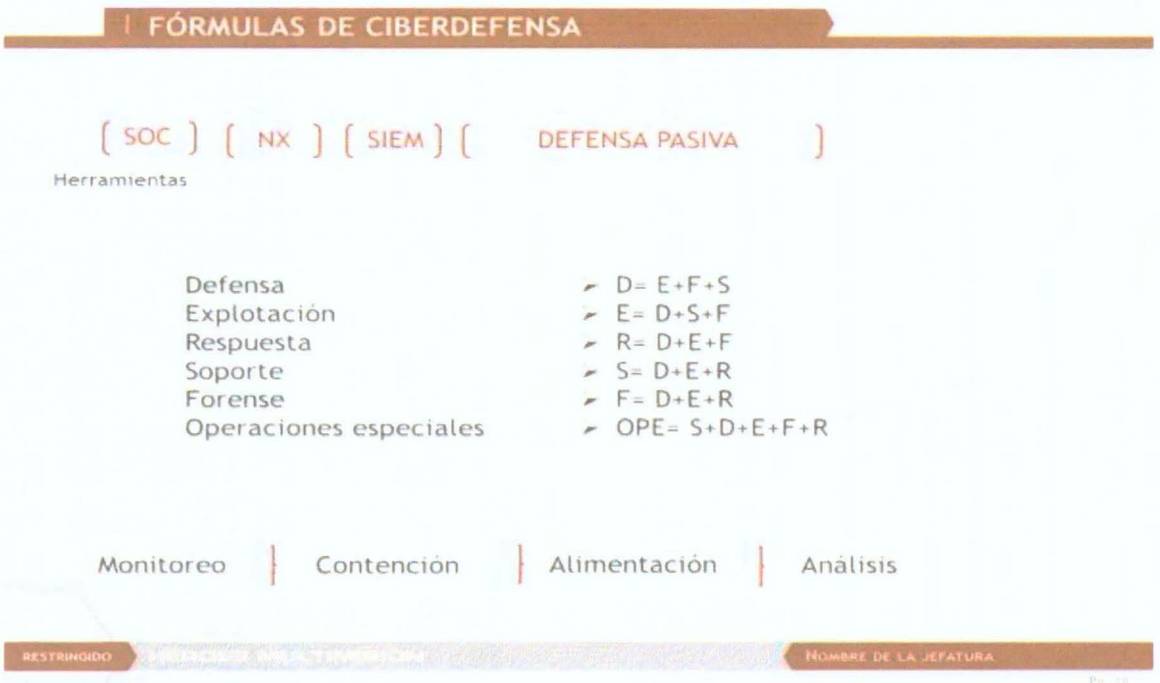
Figura 34. Herramientas de ciberdefensa recomendadas

3.4.22 Formula cibernéticas.

Con este breve explica se hace referencia de cómo desde la visión de este documento se articulan capacidades del SOC y CSIRT, mediante Tácticas, Técnicas y Procedimientos que permitan realizar protocolos de defensa pasiva y en defensa activa. Para defender y responder efectivamente ante ataques cibernéticos que comprometen la infraestructura crítica.

Mediante la combinación de tablas dinámicas realizada TTP, en defensa, explotación, respuesta soporte, forense y operaciones especiales, con la finalidad de tener claro la forma de actuar ante cada clase de operación cibernética. el personal sabrá cómo actuar en el planeamiento y ejecución de operaciones ciberneticas. Y usar a cada técnica táctica y procedimiento en forma clara y automática entrenando al personal en el desarrollo de capacidades (ver figura 35 y 36).

Figura 35. Fórmulas de ciberdefensa.



A continuación, procederemos a explicar brevemente una de estas fórmulas: *Operaciones Especiales: $OPE=S+D+E+F+R$.*

Soporte: personal de control, gestión, supervisión y mantenimiento de las herramientas cibernéticas, durante toda la operación. Garantizando los servicios.

Defensa: personal y herramientas de soc permanentes y funcional con análisis expertos en monitoreo y contención.

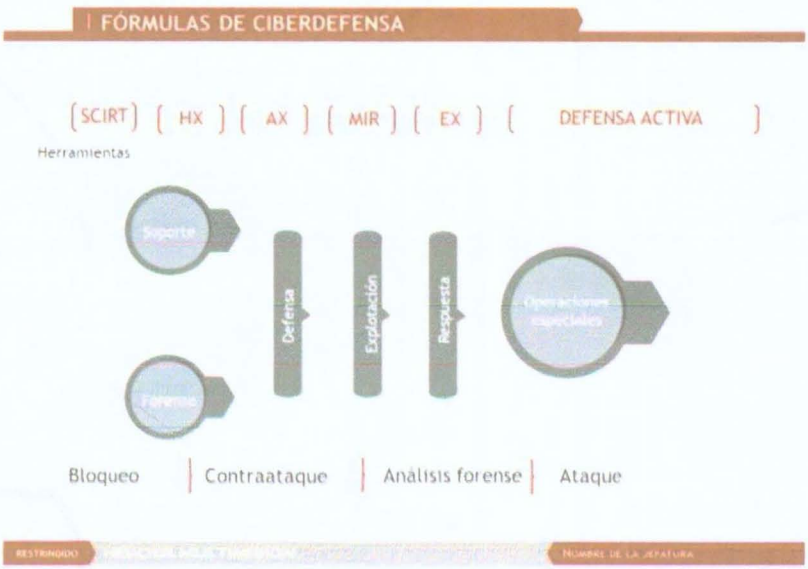
***Explotación*:** personal experto en recolección de información y análisis de inteligencia cibernética.

Forense: personal especializado en defensa y respuesta mediante análisis de software y Hardware y fabricación de herramientas en defensa activa y pasiva garantice la seguridad y la

defensa de las infraestructuras críticas exporta en i + d + i Cibernético.

Respuesta: fusión de todas las técnicas anteriores con la finalidad de realizar, análisis forense, bloqueo, contra ataque y ataque.

Figura 36. Fórmulas de ciberdefensa.



3.4.23 Planeación de operaciones cibernéticas.

Se desarrolla un procedimiento de comando Cibernético mediante el uso de plantillas de la operación a realizar, donde toda parte de la intención comandante de quien emite la orden de hacer la operación. Qué significa este concepto la intención del comandante y el efecto deseado requerido en defensa y en respuesta en operaciones de SOC y de CSIRT usando TTP de defensa, explotación, respuesta, soporte, forense y operaciones especiales cibernética. Usando las fórmulas o cuadro dinámico de posibilidades explicado anteriormente.

El Paso siguiente es la planificación de la operación cibernética donde se recibe la misión, se identifica la intención de del Comandante Director o Jefe. Se terminara el efecto requerido y se generan cómo, mínimo dos cursos o posibilidad acción a seguir para la operación cibernética.

Para consolidar los cursos de acción y el análisis de la misión tomo como base la gráfica de operaciones militares cibernéticas, donde hago un análisis detallado de las variables de las cual se comprobaron sólo unos análisis del enemigo. Como es blanco. Amenaza, organización, software malicioso etc. Determinado que me ataca para poder defenderme.

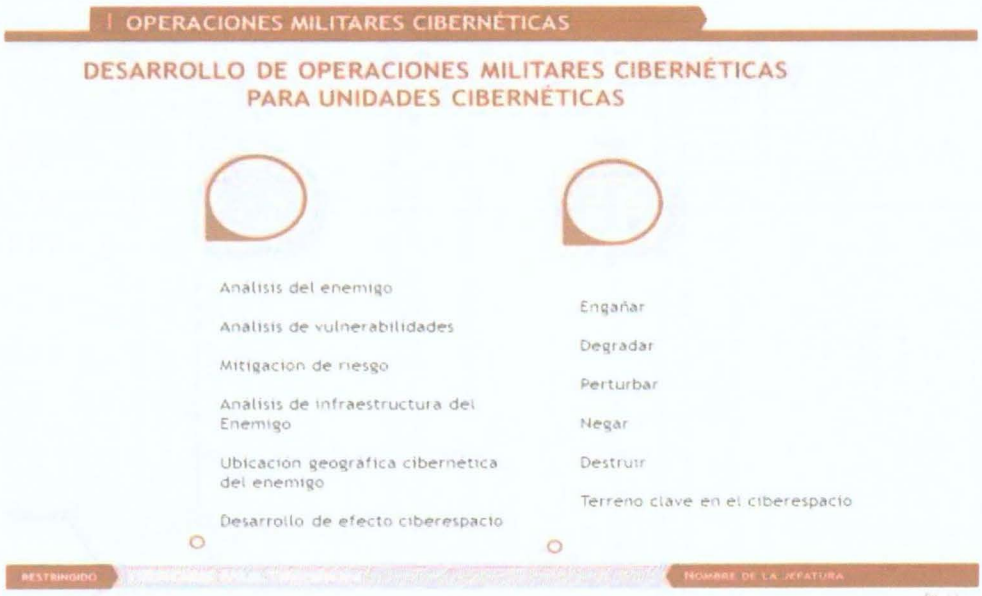
Seguimos haciendo un análisis de las vulnerabilidades propias y de la amenaza, con la finalidad de determinar la política y controles propios. Así como una estrategia y taticas mediante TTP y operaciones cibernéticas a seguir. También a análisis de infraestructura propia y del atacante para conocer cómo se comporta al atacar.

Determinó todo el terreno clave cibernético qué es el campo de operación o tablero de juego o como lo quieras llamar. El cual debe tener Comando y control (C-2) para poder plantear un efecto cibernético requerido y desarrollo de vectores de defensa y respuesta que permitan estar protegido de la intención de quien me ataca y de cómo debo responder

3.4.24 Operaciones Militares Cibernéticas

A continuación la gráfica 37 describe los principales aspectos se deben tener en cuenta para el desarrollo de las operaciones.

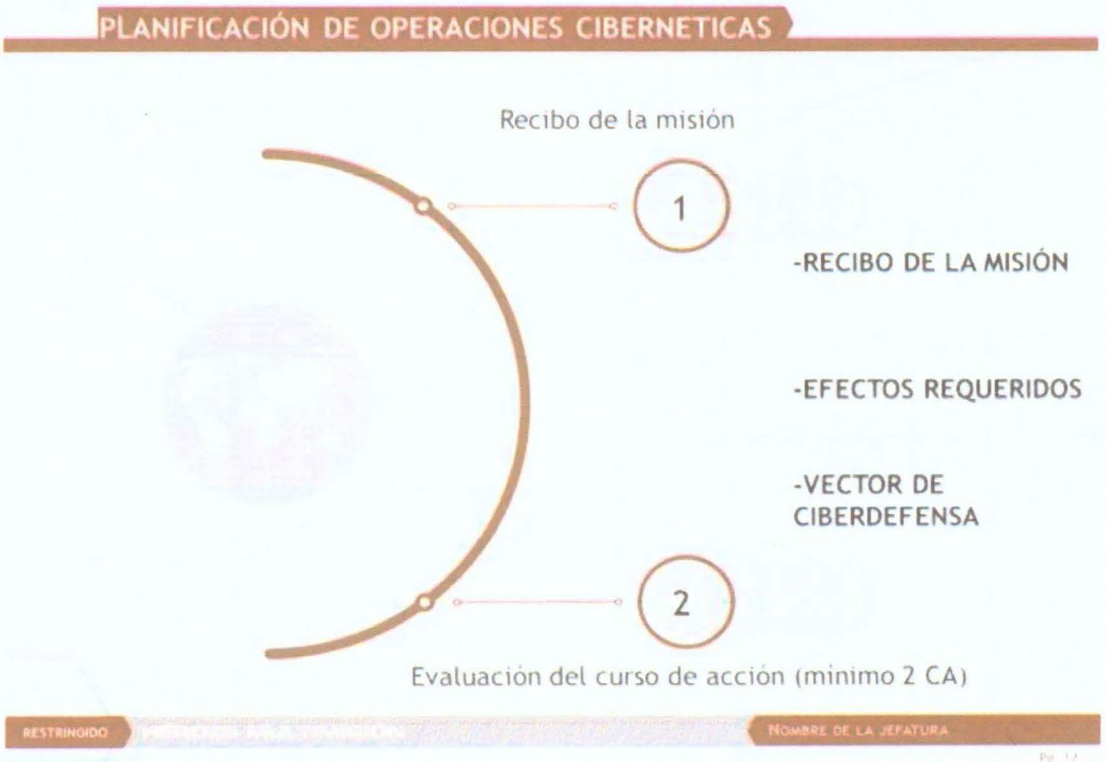
Grafica 37. Desarrollo de las operaciones cibernéticas.



3.4.24.1 Planificación de Operaciones Cibernéticas

A continuación la gráfica 38 describe los aspectos más relevantes, durante la planificación estratégica de las operaciones.

Grafica 38. Planificación de las operaciones cibernéticas.



IV. CONCLUSIONES

Todos los países americanos deben apoyar el concepto de seguridad multidimensional trabajando en la lucha contra amenazas de tipo militar externo, políticas, económicas, medio ambiente y seguridad humana. Este concepto permite incluir la lucha contra las amenazas que se presenta en el ciberespacio mediante el uso de internet.

Las crecientes amenazas cibernéticas contra la seguridad de un país obligan a desarrollar una estrategia de ciberseguridad y ciberdefensa, la cual permita el uso del ciberespacio en forma segura. Los países deben pensar en tener una Brigada cibernética, organizada y entrenada y con capacidades de realizar operaciones militares en el ciberespacio. Esta estrategia permitiría ampliar la seguridad de las americas fortaleciendo la seguridad multidimensinal.

Después de países como Estados Unidos y Brasil, Colombia quiere posicionarse regionalmente en ciberseguridad y ciberdefensa mediante las capacidades que brinda una Brigada Cibernética, que le permita realizar operaciones militares en el ciberespacio, con personal entrenado y apoyando otras unidades cibernéticas de la región fortaleciendo el concepto de seguridad multidimensional.

Esta Brigada de Ciberdefensa fortalecerá la seguridad y defensa nacional teniendo como objetivo fundamental la protección de la tierra y sus ciudades por eso es de vital relevancia proteger las infraestructuras criticas digital de los países en este nuevo campo de combate cibernético.

Donde es imprescindible importancia las alianzas continentales y regionales estableciendo políticas y estrategias en ciberseguridad y Ciberdefensa permitiendo estar preparados ante estas nuevas amenazas globales de ciberguerras y ciberconflictos que ya estamos viviendo. Donde tener una capacidad real disuasiva es fundamental mediante unos ejércitos cibernéticos, que permiten realizar operaciones militares cibernéticas apoyando la seguridad y defensa de los intereses nacionales.

Se requiere con urgencia una unificación de la operación ciberneticas de del Ejército Nacional de Colombia. La capacidad de ciberdefensa está separada y no hay comando de control unificado que articule la capacidad de defensa, explotación y respuesta que permita interoperar la unidad de ciberdefensa y ciberinteligencia.

Es urgente tener una capacidad real con organización e infraestructura que permita realizar operaciones de ciberseguridad y ciberdefensa, como también desarrollar el centro de planeación de operaciones Ciberneticas con la cual se planeara todas las operaciones que realice de la Brigada Cibernetica para hacer frente a una amenazas en el ciberespacio.

No es aconsejable que una sola unidad de Ciberdefensa de fuerzas militares responda por toda la infraestructura critica del país y realice operaciones en el ciberespacio, por lo tanto, se requiere que cada fuerza tenga su unidad, tipo Brigada con personal que conforme un cuerpo o especialidad cibernética y responda por las operaciones cibernéticas de acuerdo con al rol de fuerza, (tierra, mar, aire) y apoye al comando conjunto cibernético de las fuerzas militares. El desarrollo de las Tecnologías de Información y Comunicación ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo a la vez han generado nuevos riesgos y amenazas cibernéticas. Por esta razón, es importante que el Ejército Nacional de Colombia tenga una Brigada de ciberdefensa la cual hace frente a los ciberataques que permita proteger las infraestructuras críticas de la nación.

Al atacar infraestructuras críticas no solo las unidades militares o las organizaciones estatales se ponen amenazas también las instituciones privadas se ven afectadas tales como: el banco, el servicio público y el transporte. Esto significa que la seguridad y defensa del ciberespacio tiene implicaciones tanto civiles como económicas esto se convierte en un objetivo estratégico de seguridad multidimensional, por lo tanto, los hombres y mujeres que tienen esa responsabilidad deben estar preparados para asumir el compromiso de la defensa de un país. Se tiene que tener claro que sin dispar una sola bala un ataque cibernético sería un caos para cualquier país experimentar este tipo de agresión, genera impactos negativos tanto en la infraestructura crítica como en lo económico. Por esta razón, es necesario crear para el Ejército Nacional de Colombia una Brigada de ciberdefensa que evite cualquier tipo de amenaza cibernética.

Referencias

ACIS. (2015). *La Infraestructura Crítica Está en Riesgo.* Recuperado de http://www.acis.org.co/portal/content/la-infraestructura-cr%C3%ADtica-est%C3%A1-en-riesgo

Barrio, M. (2015). *Ciberdelitos: amenazas criminales del ciberespacio.* (1ª. ed.). Madrid, España: Editorial Reus. Recuperado de https://books.google.com.co/books?id=hrxUDwAAQBAJ&printsec=frontcover&dq=ciberdefensa&hl=es-419&sa=X&ved=0ahUKEwj8kajD6PvaAhVBtVMKHY-lA-w4ChDoAQhMMAg#v=onepage&q&f=false

Belt Soluciones de Seguridad Global. (s. f.). *El cibercomando militar de Estados Unidos.* Recuperado de http://www.belt.es/expertos/HOME2_experto.asp?id=5424

Berghel, H. (2015). El Code Red: Un software malicioso que no conoce límites. *Revista de comunicación. 44*(12), 15-19.

Boto, C. (2010). *Centro de operaciones de seguridad.* Recuperado de http://www.revistadintel.es/Revista/Numeros/Numero4/Seguridad/Industria/boto.pdf

Camacho, J. D. (2016). Evolución de la Ciberdefensa y la seguridad de la información en Colombia. *Trabajo de grado para optar al título de Especialista en la Administración de la seguridad.* Universidad Militar Nueva Granada. Bogotá D. C. Recuperado de http://repository.unimilitar.edu.co/bitstream/10654/14382/3/CamachoGarciaJuanDiego2016.pdf

Candela, L. (2014). Ciberdefensa: una visión desde la UNASUR. *Revista SEDICI, 5*(5), 1-24. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/44716/Documento_completo.pdf?sequence=1

Chen, Q. & Bridges, R. A. (2017). Análisis de comportamiento automatizado de malware Un caso de estudio de WannaCry Ransomware. *Revista de Criptografía y seguridad, 23*(5), 30-44.

COICERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2013). *Acerca de nosotros*. Recuperado de http://www.colcert.gov.co/?q=acerca-de

Comando General Fuerzas Militares de Colombia. (2014). *Políticas de seguridad de la información para el sector defensa.* Recuperado de http://www.cgfm.mil.co/documents/10197/265179/Directiva+_2014_18.pdf/485e4e48-07f8-497a-972a-af57881fb9ce

CSIRT-CCIT - Centro de Información de Seguridad Informática en Colombia. (2015). *Quienes Somos*. Recuperado de http://www.csirt-ccit.org.co/nosotros.html

Cuadra, F. (2016). La genealogía del malware. *Revista seguridad de la red.* 4(7), 17-20.

Dialogo Revista Militar Digital - Foro de las Américas. (2016). *Colombia asume el desafío cibernético.* Recuperado de https://dialogo-americas.com/es/articles/colombia-asume-el-desafio-cibernetico

Documento CONPES 3701. (14, julio, 2011). *Lineamientos de política para ciberseguridad y Ciberdefensa.* Recuperado de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Documento CONPES 3854. (11, abril, 2016). *Política nacional de seguridad digital*. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Ejército Nacional, Patria, Honor, Lealtad (2016). *Quienes somos.* Recuperado de http://www.ejercito.mil.co/?idcategoria=362169

Fiscarra, F. (2017). Los virus informáticos. *Revista Centro Internacional de Estudios Superiores de Comunicación para América Latina, 2*(2), 62- 69.

Flores, E. J., Asanza, M. I. & Berrones, M. (2014). Ciberdelincuencia un mal que afecta a la sociedad actual. *Revista contribuciones a la ciencia sociales, 2*(2), 1- 14. Recuperado de http://www.egov.ufsc.br/portal/sites/default/files/ciberdelincuencia_un_mal_que_afecta_a_la_sociedad_actual.pdf

Fuentes, L. F. (2008). Malware, una amenaza de internet. *Revista Digital Universitaria, 9*(4), 3-9. Recuperado de http://www.ru.tic.unam.mx:8080/bitstream/handle/123456789/1368/art22_2008.pdf?sequence=1&isAllowed=y

García, M. A. (2016). *Malware en Android: Descubrimiento, reversión y análisis forense.* (4ª. ed.). México: OX Word.

Giles, J. (2009). Conficker: el enemigo dentro. *Revista seguridad de la red, 202*(271), 36-39.

Gobierno de España. (2013). *Estrategia de Ciberseguridad Nacional.* Recuperado de https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Gobierno de España. (2015). *Mando Conjunto de Ciberdefensa.* Recuperado de http://www.defensa.gob.es/ministerio/organigrama/emad/mccd/

Gómez, H. (2017). Ciberguerra ¿dudáis? *Revista de Marina, 959*(35), 34-39. Recuperado de https://revistamarina.cl/revistas/2017/4/hgomeza.pdf

González, L. E. & Vázquez, R. A. (2015). Clasificación de Malware mediante Redes Neuronales Artificiales. *Revista del Centro de Investigación. Universidad La Salle, 11*(44), 69-102. Recuperado de http://www.redalyc.org/pdf/342/34242142004.pdf

Huerta, A. (2015). *Primeros pasos en protección de infraestructuras críticas.* Recuperado de https://www.securityartwork.es/2015/09/04/primeros-pasos-en-proteccion-de-infraestructuras-criticas/

Iglesias, A. (2016). *¿Cómo se protegen las infraestructuras críticas en España?* Recuperado de http://www.ticbeat.com/seguridad/como-se-protegen-las-infraestructuras-criticas-en-espana/

Joyanes, L. (2010). Introducción: estado del arte de la ciberseguridad. *Revista el mundo. 1*(29), 13-46. Recuperado de http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf

Kenney, M. (2015). Ciberterrorismo en un mundo Stuxnet. *Revista Orbis, 59*(1), 111-128.

López, J. (2013). *Capacidades Esenciales Para Una Ciberdefensa Nacional.* Recuperado de http://studylib.es/doc/5980237/capacidades-esenciales-para-una-ciberdefensa-nacional.

Mansfield, S. (2017). Ransomware: la forma más popular de ataque. *Revista Fraude informático y seguridad, 2017*(10), 15-20.

Martínez, L. M. (2014). *Virtualidad, ciberespacio y comunidades virtuales.* (1ª. ed.). México: Red Durango de Investigadores Educativos. Recuperado de http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Ministerio de Defensa Nacional. (2009). *Ciberseguridad y Ciberdefensa: Una primera aproximación.* Recuperado de: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

Newmeyer, K. (2015). *Ciberespacio, ciberseguridad y ciberguerra.* Recuperado de http://virtual.esup.edu.pe/jspui/bitstream/ESUP/113/1/pp.76-95.pdf

Pastor, O., Pérez, J. A., Arnáiz, D. & Taboso, P. (2009). *Seguridad Nacional y Ciberdefensa.* 1ª. ed. Bogotá D.C.: Cuadernos Catedra. Recuperado de http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

Peralta, O. H. (2015). Ciberseguridad: nuevo enfoque de las fuerzas militares de Colombia. *Trabajo de grado para optar al título de Especialista en la Administración de la seguridad.* Universidad Militar Nueva Granada. Bogotá D. C. Recuperado de http://repository.unimilitar.edu.co/bitstream/10654/7884/1/ensayo%20final%20EAS-2015%20UMNG%20OSCAR%20PERALTA.pdf

Pérez, J. R. (2018). *Diversos tipos y formas de virus informáticos. Formas de protegerse de estas amenazas.* (5ª. ed.). Colombia: Computer Science. Recuperado de https://www.grin.com/document/388017

Peter, k. (2014). ILOVEYOU: Virus, paranoia y el entorno de riesgo. *Revista la revisión sociológica, 48*(52), 1-14.

Poveda, M. A. & Torrente, B. (2016). Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista. *Revistas Científicas de América Latina, el Caribe, España y Portugal, 32*(8), 509 - 518. Recuperado de http://www.redalyc.org/pdf/310/31048481030.pdf

Sáinz, R. M. (2017). *Ciberseguridad, la protección de la información en un mundo digital.* (3ª. ed.). Barcelona, España: Editorial Ariel, S.A.

Sánchez, G. (2013). El ciberespionaje. *Revista nueva época, 12*(3), 115-124. Recuperado de http://www.academia.edu/7414397/El_ciberespionaje

Stel, E. (2014). *Seguridad y Defensa del Ciberespacio.* (1ª. ed.). Buenos Aires: Editorial Dunken. Recuperado de https://books.google.com.co/books?id=H1lhAwAAQBAJ&pg=PA131&dq=ciberdefensa&hl

=es-419&sa=X&ved=0ahUKEwj8kajD6PvaAhVBtVMKHY-lA-w4ChDoAQglMAA#v=onepage&q=ciberdefensa&f=false

Suárez, A. (2015). *El quinto elemento: Espionaje, ciberguerra y terrorismo.* (1ª. ed.). España: Editorial Deusto. Recuperado de https://books.google.com.co/books?id=1n16CgAAQBAJ&printsec=frontcover&dq=ciberdefensa&hl=es-419&sa=X&ved=0ahUKEwjtiZOo9_vaAhXHt1kKHRbpDMc4FBDoAQhQMAk#v=onepage&q=ciberdefensa&f=false

Vargas, E. M. (2014). Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional? *Trabajo de Grado para optar al título de Especialista en Alta Gerencia de la Defensa Nacional.* Universidad Militar Nueva Granada. Facultad de Relaciones Internacionales, Estrategia y Seguridad. Bogotá D.C. Recuperado de http://repository.unimilitar.edu.co/bitstream/10654/12259/1/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf

Vélez, C. (2015). Virus informáticos. *Revista Cápsulas de Tecnologías de la Información. 107*(1), 30-40.

Walt, D. (2013). *Definitive Guide Protección contra amenazas de próxima generación: Ganando la guerra a la nueva variedad de ciberataques.* (2ª. ed.). Colombia: CyberEdge Press. Recuperado de https://www.fireeye.com/content/dam/fireeye-www/regional/mx_ES/solutions/pdfs/eb-definitive-guide-next-gen-threat-protection.pdf

Wikipedia. (s. f). *Cibercomando de Estados Unidos.* Recuperado de https://es.wikipedia.org/wiki/Cibercomando_de_Estados_Unidos

Zuccardi, G. & Gutiérrez, J. D. (2006). *Informática forense.* Recuperado de: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf