Medidas de acción necesarias, para optimizar la ciberdefensa en la Armada Nacional de Colombia

Javier Fernando Posada Parra
Andrés Alberto Mateus Rojas

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

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

2016

MEDIDAS DE ACCIÓN NECESARIAS, PARA OPTIMIZAR LA CIBERDEFENSA EN LA ARMADA NACIONAL DE COLOMBIA

Capitán de Fragata JAVIER FERNANDO POSADA PARRA

Curso de Estado Mayor año 2.013

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA
BOGOTÁ D.C.
2016

MEDIDAS DE ACCIÓN NECESARIAS, PARA OPTIMIZAR LA CIBERDEFENSA EN LA ARMADA NACIONAL DE COLOMBIA

Capitán de Fragata JAVIER FERNANDO POSADA PARRA

TRABAJO DE GRADO PRESENTADO PARA
OPTAR EL TÍTULO DE
"MAGISTER EN SEGURIDAD Y DEFENSA NACIONAL"

Director del Proyecto
MSC ANDRES ALBERTO MATEUS ROJAS

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA
BOGOTÁ D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

Ciudad y fecha

AGRADECIMIENTOS

El presente trabajo, corresponde a la voluntad y entrega académica realizada durante el primer semestre del año en curso, en este, fue de vital importancia el apoyo incondicional de mi esposa e hijos, quienes evidenciaron permanentemente, el esfuerzo, la dedicación y el compromiso necesarios para recolectar, analizar y presentar los resultados de esta investigación acerca de la ciberdefensa en la Armada Nacional de Colombia. Que representa vital importancia para la institución y se manifiesta en el personal que conforma la Armada Nacional de Colombia, en su seguridad y la garantía de poder disfrutar los beneficios del uso de los medios informáticos de manera segura.

De la misma forma, iluminado por la gracia de Dios, tuve la fortuna de tener una guía y dirección continuada por parte de mi director de proyecto, quien con su exigencia, trazó una ruta de optimismo con metas claras y definidas, liderando un planeamiento organizado, que contribuyó a labrar el camino seguro, que me permitió alcanzar el éxito.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

El presente estudio de investigación formativa proporciona medidas de acción que contribuyen al fortalecimiento de la ciberseguridad, que sirven a la vez para abordar una estrategia de ciberdefensa en la Armada Nacional de Colombia como herramienta importante para la seguridad de la información institucional.

La Utilidad del proyecto es proporcionar una investigación que muestre áreas de oportunidad de mejora en los aspectos del control y la seguridad para la ciberdefensa en la Armada Nacional de Colombia, que estén sustentadas por un proceso sistemático, continuo y ordenado, que avale su viabilidad y factibilidad, basado en la experiencia vivida en la Armada Española para que su aplicación beneficie directamente a la institución que hace uso de las mismas.

La tesis que el presente trabajo quiere demostrar es que se requiere implementar unas medidas de acción para fortalecer la ciberseguridad en la Armada Nacional, por lo cual la investigación se centra en un enfoque cualitativo, de tipo exploratorio descriptivo; de carácter exploratorio, dado que buscó aproximaciones al conocimiento de las manifestaciones de la problemática en una comunidad específica y así mismo da a conocer un contexto, una situación y la identificación de una variable mediante una exploración inicial en un tiempo dado para generar nuevos abordajes posteriores en esta línea de investigación (ANGUERA, 1998).

El procedimiento consiste en medir o ubicar a un grupo de personas, objetos, situaciones, contextos, fenómenos en una variable o concepto y proporcionar su descripción, con el fin de aprovechar la información que estos tienen, gracias a la experiencia desarrollada en su ámbito de la informática y las redes en la Armada Nacional, partiendo del concepto concreto sobre la ciberdefensa y la ciberseguridad, para llegar a una descripción general y lograr comprobar hipótesis causales. Para ello se utilizó la entrevista abierta y personal, que es una técnica útil para indagar, comprender tal y como es conceptualizado e interpretado por los sujetos estudiados sin imponer categorías preconcebidas. Como afirma Patton (1980) (MONTERO, 1997), el objetivo

de la entrevista cualitativa es conocer la perspectiva y el marco de referencia a partir del cual las personas organizan su entorno y orientan su comportamiento.

La investigación, tomó 04 grupos poblacionales, a saber: En primer lugar a la Directora de Telemática de la Base Naval ARC "Bolívar", que se ha desempeñado en cargos de relevancia administrativa con respecto a la seguridad de la información, por lo cual tiene claridad de la necesidad, de plantear mejoras en lo concerniente a la optimización de la ciberseguridad. En segundo lugar, el universo está compuesto por el Subdirector de Telemática de la Base Naval ARC "Bolívar", el cual tiene experiencia en la problemática y necesidades informáticas de la Armada Nacional, en tercer lugar el jefe de la división de informática de la Armada Nacional, el cual tiene la experiencia y el conocimiento acerca de las necesidades para implementar unas medidas de ciberseguridad apropiadas en la Armada Nacional y en cuarto lugar un oficial del Departamento de Armas y Electrónica de BN1, el cual realizó una maestría en tecnologías de defensa en España y tiene el conocimiento acerca de los modelos de ciberseguridad y ciberdefensa implementados en la Armada Española.

De la misma forma, la investigación tiene un alcance descriptivo porque se recolectan datos sobre diversos aspectos, dimensiones o componentes del fenómeno de investigación, con el fin de llegar al resultado de la investigación. Es por ello que su diseño es no experimental, debido a que se analiza la realidad y se observa la situación actual de las medidas que se requieren para la Ciberdefensa y para la ciberseguridad, igualmente, no se manipulan, ni se modelan las variables. Debido a esto, la observación es transeccional correlacional-causal, debido a que se recolectaron datos actuales acerca de la ciberseguridad y la ciberdefensa. Correlacional, por cuanto se encarga de identificar la relación que hay entre los diferentes conceptos y las variables, con el fin de lograr entender el comportamiento de cada una de ellas. (Jiménez, 2011).

Por otra parte para la obtención de la información de este trabajo, se empleó el método de investigación documental; utilizando fuentes de información primarias, como las que contienen información original no abreviada ni traducida: tesis, libros, artículos de

revistas y manuscritos, las cuales proveerán un testimonio o evidencia directa sobre el tema de investigación ofreciendo un punto de vista en particular de cada organización. Asimismo, se emplean fuentes secundarias o derivadas, que contienen datos reelaborados o sintetizados como los resúmenes y obras de referencias (diccionarios o enciclopedias) y datos estadísticos con múltiples fuentes (Gonzalez, 2014), donde implican análisis, síntesis, interpretación de otros autores del tema de investigación. Por lo anterior, se tuvo acceso a diferentes autores a través de internet, como también el empleo de bibliotecas virtuales, tomando como base principal la plataforma blackboard.

La necesidad de establecer medidas de acción necesarias para optimizar la ciberseguridad en la Armada Nacional de Colombia y de adoptar una estrategia de ciberdefensa, se basa en la importancia de prevenir la sintomatología de los ciberataques presentada en diferentes países durante la última década. Dicha problemática es latente, por tener la Armada Nacional la responsabilidad de salvaguardar los mares, costas y ríos de todo el territorio colombiano, para lo cual, utiliza plataformas de información sensibles para el manejo y administración de las bases de datos de personal y de material, el mantenimiento de las unidades en tierra y a flote, los sistemas de información financiera, los sistemas electrónicos, los sistemas de navegación y los sistemas de armas de las unidades entre otros, los cuales contienen información reservada, secreta y ultra secreta.

Sin el ciberespacio, el manejo de la información de todos los sistemas anteriormente mencionados, las comunicaciones y la investigación institucionales, sería simplemente demasiada lenta y en ocasiones imposible, en especial las comunicaciones y el intercambio de información clasificada con otros países, mediante el flujo constante y seguro de los sistemas privados de redes (Brochet, 2010). Es por ello, que la importancia de este proyecto estriba en proporcionar propuestas encaminadas a preservar la confidencialidad, integridad y disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas del Sector Defensa, protegiendo adecuadamente la información de la Armada Nacional(Ministerio de Defensa Nacional, 2014).

Ahora bien, en cualquier análisis que se haga hoy día en el contexto de las Relaciones Internacionales en un mundo interdependiente, "el concepto de seguridad es un factor dominante"(Almirante (Ra) Alvaro Echandia Durán, 2011), pues los problemas políticos, económicos e internacionales contemporáneos, no son ajenos a la seguridad(Chin, 2013), la cual, siempre estará presente, considerando que la seguridad contemporánea está caracterizada por amenazas que trascienden la distinción clásica entre lo doméstico y lo externo, constituyéndose en retos internacionales que con frecuencia carecen de orígenes nacionales, proviniendo de actores no estatales y no gubernamentales, que se adaptan a la fluidez del actual sistema internacional y que frecuentemente interactúan entre sí (Garcia, 2013).

El estudio inicia de lo general a lo particular; el primer capítulo enmarca el contexto de la amenaza con los diferentes ataques cibernéticos que se han presentado en los últimos tiempos en diferentes países del mundo, posteriormente se define un marco legal a nivel internacional y nacional, que demuestra la necesidad de fortalecer algunos vacíos jurídicos. De la misma forma, se evidencia que existen vulnerabilidades en la protección de los sistemas de seguridad informática, debido a la facilidad para acceder a los mismos, convirtiéndose en una amenaza que obliga a implementar medidas de acción que contribuyan al fortalecimiento para la ciberseguridad. En el segundo capítulo se presentan las medidas utilizadas por la Armada Española para la protección de la ciberseguridad y la ciberdefensa, de las cuales, algunas se pueden aplicar en la Armada Nacional para incrementar la protección de la seguridad informática.

Seguidamente en el tercer capítulo, se analiza cuales medidas de acción de la experiencia vivida en la Armada Española, se considera necesario podrían aplicarse en la Armada Nacional para contribuir al fortalecimiento de la ciberseguridad, que permitan definir unos criterios para establecer una estrategia de ciberdefensa en la Armada Nacional de Colombia.

Posteriormente en el cuarto capítulo, se va a presentar una propuesta con las medidas y acciones más apropiadas que se deben tener en cuenta para fortalecer la ciberseguridad

en la Armada Nacional, que contribuyan a adoptar una estrategia de ciberdefensa institucional.

En síntesis y teniendo en cuenta que la Armada Nacional tiene la responsabilidad de salvaguardar dos océanos, que "aproximadamente el 50% del territorio nacional es oceánico, con lo cual posee una inmensa riqueza de recursos que incluye la producción de oxígeno, recursos pesqueros, líneas de comunicación marítima, energía renovable y no renovable entre otros"(Comisión Colombiana del oceano, 2007), se hace necesario fortalecer las herramientas y mecanismos que contribuyen a la protección de la información, mediante el desarrollo de una investigación que permita identificar como lo hacen en otro Estado y analizar cuales procedimientos son los más apropiados de implementar en nuestra institución para el mejoramiento de la ciberseguridad a nivel Armada Nacional, debido a que son un procedimiento viable y factible, teniendo en cuenta que en la institución se cuenta con recursos, medios y voluntad del alto mando, que le permiten adoptar los mecanismos que hoy día se ponen en práctica en otros países, como España.

CAPITULO I

1.1. LA AMENAZA:

La amenaza para cualquier nación se basa en la relativa facilidad con la que se pueden producir "artefactos" que pongan en riesgo la seguridad nacional, por lo que ya no solo basta con contar con armas de fuego, explosivos y sistemas de control avanzados para proteger la integridad de un país (GIL, 2009).

Esa relativa facilidad con la que se producen armas lógicas pone en igualdad de condición a cualquier enemigo con la nación (GIL, 2009), es decir, antes para enfrentarse a un estado era necesario contar con suficientes hombres y material bélico para enfrentar a las fuerzas de seguridad; esto además de costoso es muy complicado de organizar sin ser detectado por las agencias de inteligencia al servicio del gobierno; Ahora bien, así como en el entorno militar en todos sus ámbitos terrestre, marítimo y/o aéreo, la prioridad es el personal, los medios y todo lo material, pues en el ciberespacio el factor más importante es la información, ya que esta se convierte en el valor de mayor importancia estratégica y es aquella a la que se debe proteger para evitar que la vulneren (Niño, 2013).

Sin embargo, en el ciberespacio la situación es diferente ya que para producir un "arma lógica" básicamente se necesitan una serie de conocimientos sobre el funcionamiento de las redes y unos equipos de fácil acceso, esto sumado a la facilidad con la que se pueden reunir verdaderos ejércitos cibernéticos, lo cual hace que la tarea de proteger el "quinto dominio" no sea nada fácil (GIL, 2009). A este ambiente del ciberespacio, se le denomina el quinto dominio de batalla, el cual es hoy una realidad en el mundo; existen varios países que vienen desarrollando estrategias para explotarlo y protegerlo de explotaciones por parte del enemigo; un caso palpable es el de Estados Unidos, país que en la primera década del siglo XXI creó un nuevo mando militar para llevar a cabo un nuevo tipo de guerra de alta tecnología, de forma similar lo hicieron Rusia y China, además de otras muchas naciones; estas organizaciones militares y de inteligencia se están encargando de preparar el campo de batalla ciberespacial con artilugios

denominados "bombas lógicas" y "puertas traseras", colocando explosivos virtuales en otros países en tiempos de paz (Monroe, Operaciones en el Ciberespacio, 2010).

La información es el factor más importante del ciberespacio (López, 2007), por ello, hay grupos de personas que se dedican a investigar y a experimentar acerca de cómo vulnerar las redes informáticas ajenas, con el fin de obtener información o sabotear sistemas informáticos con fines lucrativos o extorsivos. Esta modalidad, se conoce como la ciberguerra o guerra informática y corresponde a todas las acciones que se realizan a fin de alterar la información y los sistemas de información del adversario; tales operaciones abarcan prácticamente toda medida cuyo objetivo sea: descubrir, alterar, destruir, interrumpir o transferir datos almacenados, procesados o transmitidos por un ordenador (López, 2007).

Entre las amenazas más conocidas, se encuentra: el cibercrimen, el ciberespionaje, los ciberataques, el uso de malware que compromete los sistemas de supervisión y de adquisición de datos (SCADA), los fraudes, los ataques dirigidos, el secuestro de computadoras, el hacktivismo, el robo de información pública y privada y de identidad (especialmente en el sector financiero), el terrorismo, la ciberguerra y el espionaje militar (Niño, 2013).

Dichas acciones se pueden evidenciar durante tiempos pacíficos o de crisis, sin embargo la ventaja estratégica la tendrá quien tenga los sistemas informáticos protegidos y con herramientas actualizadas continuamente, que sirvan para contrarrestar cualquier intención de ataque de esta índole (Diaz, 2014). Es por ello, que los ataques a la infraestructura crítica se han convertido en una importante preocupación para los gobiernos y proveedores privados de todo el mundo "ya sean ataques cometidos por criminales cibernéticos que buscan tener ganancias financieras o por hackers como actos políticos que buscan socavar la credibilidad de los gobiernos y las compañías" (Micro, 2.015). Es así, que se evidencia un aumento de ataques a los sistemas de cómputo, debido a que los ataques cibernéticos contra la infraestructura son cada vez más sofisticados.

De la misma forma, hoy día los escenarios de amenaza cambian constantemente, para lo cual se hace necesario implementar contramedidas, a fin de evitar que se presente el robo de identidades para fines criminales y de bases de datos para el espionaje de una nación o como el gusano Stuxnet para sabotaje (Andress, 2011). Hace una década, existieron casos de jóvenes atacando sistemas solo por diversión para ellos, luego fueron ataques criminales de identidades; ahora, aparecen más casos por las redes sociales, de amenazas y difusión de información ideológica difusa.

Son muchas las características de una guerra o un ataque cibernético, entre las cuales podemos mencionar:

La complejidad, la asimetría, los objetivos limitados, la corta duración, la desaparición del daño físico para los soldados, un mayor espacio de combate y una menor densidad de tropas, la lucha intensa por la superioridad de la información, la reacción rápida e igual de devastadora que una guerra convencional (Medero, 2012). Sin embargo, la más relevante es la asimetría, ya que la ciberguerra permite que los pequeños puedan amenazar y retar a los más grandes, con tan solo el uso de un computador portátil.

Colombia es un país que atraviesa una situación particular teniendo en cuenta los diferentes grupos armados organizados, a los que el Estado se ve enfrentado y sobre los cuales, la Armada Nacional tiene responsabilidad de hacer frente. Estos focos de amenaza son los siguientes:

Organización Narcoterrorista autodenominada "fuerzas armadas revolucionarias de Colombia". Grupo narcoterrorista, que inicialmente se constituye como un grupo guerrillero que surge después de una larga guerra entre, dos partidos políticos tradicionales en Colombia, liberales y conservadores, la cual se desarrolló entre los años de 1948 y 1953, periodo conocido como "época de la violencia", recrudecida tras el asesinato de Jorge Eliécer Gaitán (R. A. Clarke y R. K. Knake, 2011).

Esta organización actualmente se encuentra en unos diálogos de paz con el gobierno, con el fin de alcanzar unos objetivos para el beneficio de la población. Sus actividades para el sostenimiento, azotan gran parte de los rincones del país y basan su economía en el tráfico de drogas, extorsión, secuestro y la minería ilegal para mantener su accionar contra el Estado; es un grupo que ha venido evolucionando con el tiempo adquiriendo las tecnologías de la información y las comunicaciones necesarias para estar a la vanguardia del desarrollo tecnológico militar con el que cuenta la Fuerza Pública de Colombia, por lo cual sería una de las principales amenazas a hacer frente dentro del quinto dominio.

Organización narcoterrorista autodenominada "ejército de liberación nacional".

Surge como una repercusión nacional de la revolución cubana, el núcleo inicial estuvo conformado por 16 jóvenes que empezaron a delinquir en 1962; en 1965 lanzan su primer ataque contra el puesto de policía de la población de Simacota (Población del Departamento de Santander al nororiente del país), presentándose con el nombre de ejército de liberación nacional (ELN) (Ramón, 2002).

Hoy en día el ELN es el segundo grupo narcoterrorista más grande del país después de las FARC, tanto en el número de hombres como en el número de acciones perpetradas. Al igual que las FARC, las finanzas del ELN giran en torno a la extorsión, a la alianza con el narcotráfico y al secuestro. Pese a tener tan sólo la mitad de hombres que las FARC, el ELN es al parecer responsable de la misma cantidad de secuestros y de actos de sabotaje. Asimismo, las acciones del ELN se han extendido tanto en las ciudades como en el campo (Ramón, 2002), por lo anterior este sería otro de los principales focos de amenaza a tener en cuenta dentro del ciberespacio en Colombia.

Bandas Criminales

Las bandas criminales se definen como "...organizaciones criminales (macro - delincuenciales) significativamente armadas, que desarrollan actividades tanto de control de grandes negocios ilícitos como de depredación subsidiara de los mismos, y que con frecuencia emplean la violencia como mecanismo de disciplinamiento interno,

de delimitación de áreas de influencia específicas y de coacción e intimidación unilateral sobre terceros a fin de mantener las condiciones de operación requeridas por sus actividades" (F. Sánchez, 2003).

Este concepto responde a una dinámica particular, relacionada directamente con los sucesos posteriores a la desmovilización de los grupos de autodefensas ilegales en el gobierno del ex presidente Álvaro Uribe Vélez, donde reductos de estos grupos se reorganizaron para continuar con su accionar delictivo bajo un esquema netamente delictivo basado principalmente en el narcotráfico (J. Suárez Vanegas, 2012). Estos grupos al igual que los anteriores sustentan sus actividades delictivas en el uso de armas y tecnologías para la información y las comunicaciones, por lo que también es un adversario importante dentro del ciberespacio.

Delincuencia Común

Son todos aquellos pequeños grupos o pandillas dedicadas al microtráfico, el robo a mano armada, secuestros, extorsiones, homicidios, etc. cuyos fines son exclusivamente económicos y los cuales en muchas ocasiones (Velez, 2004), y gracias al avance tecnológico, implementan nuevas formas de delincuencia basadas en el uso de tecnologías de la información, por lo cual también son un enemigo a considerar dentro del "quinto dominio".

1.2. ANTECEDENTES HISTÓRICOS:

Históricamente, el uso de las redes informáticas se ha puesto en práctica ante la necesidad de enviar información para comunicarse entre un punto y otro. Sin embargo, desde la década de 1930 se desarrollaron máquinas con capacidad de descifrar los códigos claves que utilizaba el enemigo y de esa forma poder conocer las intenciones del mismo. Hoy día, a la era post industrial en la cual la capacidad de utilizar la información se tornó decisiva, se le denomina desde ahora edad de la información (Wiener, 1948).

Un método de conectar computadoras, se basaba en una computadora central, que consistía en permitir a sus terminales conectarse a través de largas líneas alquiladas. Este método se usaba en los años cincuenta por el Proyecto RAND (Research and Development de las Fuerzas Armadas Norteamericanas) (Fabra, 2010). Durante los años sesenta varios grupos de investigación interdisciplinarios, trabajaron en la conmutación de paquetes de datos y se creó el proyecto ARPANET (Advanced Research Project Agency Net) por parte del Gobierno estadounidense. Se trataba de una red en la que los ordenadores conectados a ella, disponían de diversas rutas por las que alternar las comunicaciones, con el fin de continuar funcionando, aunque alguno de ellos fuese destruido como consecuencia de algún ataque (Moraga, 2006).

A partir de 1995, se produce el gran boom de la internet comercial, lo que causó que a partir del año 2.000 se tuviesen más de 300 millones de usuarios conectados a internet (Moraga, 2006). Este medio de conexión global, es denominado ciberespacio y se le conoce como quinto dominio de la guerra junto a la tierra, mar, aire y espacio (Aguilar, 2010), el cual, permite a los usuarios esconder sus identidades, y brinda la facilidad de realizar ataques desde un lugar del globo a otro sin ser detectado; asimismo, dejar sin electricidad un sector de una ciudad, bloquear las comunicaciones o el transporte a toda una ciudad o penetrar los servidores de grandes redes informáticas industriales o estatales.

Hace unos años, China fue acusada de espionaje corporativo contra Google y otras compañías, en una operación conocida comúnmente como Aurora. De la misma forma, la comunidad de inteligencia fue acusada de utilizar el gusano Stuxnet para causar daño al programa nuclear iraní.

En una temporada las compañías wikileaks y anonimous, fueron acusadas por el robo de identidades y sabotear el acceso a las plataformas virtuales (Andress, 2011). Hoy día las cosas han cambiado, por cuanto ya no tienen dicho acceso y si el control de acceso falla, todas las cosas fallan, al igual, el robo de identidad es tan común que ya no es de interés periodístico.

¿Cuantas personas en los Estados Unidos han sido víctimas de robo de identidad? Muchos de los expertos dicen que todas las personas han sido víctimas del robo de identidad. Hay tantos datos robados, que los criminales aún no saben cómo usarlos (Andress, 2011). Los grupos criminales están contratando expertos de la informática para llevar a cabo sus estafas cibernéticas y obtener grandes resultados. Los temas de ciberguerra están haciendo parte de las discusiones del orden nacional. La ciberseguridad ya es un evento que no solo puede impactarnos a nivel personal como usuarios de internet, sino también como escenarios de amenazas permanentes en el orden de la defensa nacional.

A continuación se presentan algunos de los casos más típicos de ataques cibernéticos:

1.2.1. ROBO DE INFORMACIÓN SENSIBLE

Se conoce un caso del año 1988, donde 5 hackers tomaron información por la red del Pentágono, NASA, Laboratorio Nacional de los Álamos, CERN, ESA, Thomson, diversas empresas de armamento de Europa Occidental y compañías alemanas involucradas en investigaciones nucleares"(Díaz, 2014). De la misma forma, un informe del Congreso de Estados Unidos expone los indicios que hacen sospechar que desde China se tuvo acceso a dos satélites gestionados por la Administración Nacional de Aeronáutica de Estados Unidos (NASA) (Corredera, 2012).

1.2.2. ACCIDENTES AEREOS

En el año 1.999 un avión de la Fuerza Aérea Norteamericana accidentalmente bombardeo la embajada de China en Belgrado (Spade, 2.012), momento en el cual, un grupo de hackers chinos aprovechó para desdibujar la imagen favorable del gobierno norteamericano haciendo publicaciones en diferentes sitios web del ciberespacio. Esta situación se repitió nuevamente en mayo de 2.001, cuando una aeronave tipo P3 Orion de la marina norteamericana colisionó con un avión F8 de combate del grupo de liberación del Ejército y la Armada de China (Spade, 2.012), pero los medios cibernéticos lo presentaron como una situación intencional de los norteamericanos.

De igual forma, las guerras cibernéticas de los hacker acompañaron las intervenciones de la OTAN en Kosovo, la incursión a Lebanon por parte de Israel en el 2.006 y el conflicto ruso en Chechenia (Spade, 2.012), evidenciando que ya se consideran el quinto elemento por proteger contra las amenazas internacionales de otros países.

1.2.3. ESTONIA – 2007

Estonia posee un amplio uso de la banda ancha, lo cual lo convirtió el 27 de abril en un blanco perfecto para un ciberataque. Fue por ello, que después de ese 27 de abril, los nodos de internet en Estonia se bloquearon por completo ante la cantidad de solicitudes de conexión. Es decir, había sido víctima de un ataque distribuido de denegación de servicio o DDoS (por sus siglas en inglés), los habitantes no podían utilizar sus bancos en línea, leer sus periódicos en internet o acceder a los servicios electrónicos del gobierno (Spade, 2.012).

En febrero de 2007, en Estonia el Legislativo aprobó una "ley de estructuras prohibidas" que ordenaba derribar todo emblema de la ocupación soviética, que incluía un gigante soldado de bronce que se erigía en Tallin como recuerdo de los sacrificios que Rusia había hecho para liberarlos durante la segunda guerra mundial (Díaz, 2014). Ante esta situación Moscú protestó señalando que mover el soldado de bronce sería una ignominia para los soviéticos que habían muerto heroicamente en la segunda guerra mundial; toda esta serie de eventos generaron enfrentamientos al interior de Estonia que estallaron el 27 de abril del mismo año en lo que hoy se conoce como "la noche de bronce" (Diaz, 2014); fue entonces cuando el conflicto saltó al ciberespacio.

1.2.4. BOMBARDEO DE ISRAEL A IRAN EL 6 DE SEPTIEMBRE DE 2007

Este bombardeo que realizó Israel es quizás la primera vez que se utiliza un arma "cibernética" para apoyar el desarrollo de una operación militar; el 06 de septiembre de 2.007 aviones Israelíes penetraron territorio de Irán y lograron bombardear instalaciones que serían utilizadas para el desarrollo de armas nucleares, la hipótesis más fuerte apunta a que en la misión, fue utilizado un UAV que iba delante del resto de aviones israelíes cargado con un sistema de ciberataque similar al norteamericano "Suter", el

cual, no es más que un sistema diseñado para atacar sistemas de redes de información del enemigo(Díaz, 2014), operación a la que denominaron "huerto".

1.2.5. CONFLICTO ENTRE GEORGIA Y RUSIA – AGOSTO DE 2008

En este año Georgia y Rusia se vieron enfrentados por un territorio que históricamente había pertenecido a Georgia, y por el cual se desataron una serie de operaciones militares que enfrentaron a ambas naciones; sin embargo, de forma paralela a dichas operaciones, ciberguerreros rusos entraron en acción, su objetivo en esta ocasión era impedir que los georgianos supieran qué estaba pasando, y para ello, lanzaron ataques DDoS contra las páginas web de los medios de comunicación locales y los organismos de gobierno; asimismo, bloquearon el acceso de Georgia a las webs de la CNN y la BBC(Monroe, Ejercito de los Estados Unidos de Norteamerica. Operaciones en el ciberespacio, 2014).

Entre tanto, los rusos bombardeaban Georgia y tomaban un trozo de su territorio que no estaba en disputa; sin embargo antes de que la guerra hubiera estallado en el mundo real, ya había dado inicio en el mundo virtual, el ciberespacio, con los ataques a las webs del gobierno georgiano. En la fase inicial, los agresores realizaron ataques DDOS básicos contra las páginas web de los organismos gubernamentales y hackearon el servidor que alojaba la web de la presidencia para desfigurarla con fotografías que comparaban al presidente Mijaíl Saakashvili con Adolf Hitler (Diaz, 2014).

Ante esta situación, los georgianos intentaron defender su ciberespacio y buscar soluciones alternas para frustrar el ataque DDoS, sin embargo los rusos contrarrestaron cada uno de sus movimientos, Georgia intentó bloquear el tráfico procedente de Rusia a lo que los rusos redirigieron sus ataques para que los paquetes parecieran proceder de China. Aunque el controlador maestro de la botnets usadas en los ataques estaba en Moscú, los hackers empezaron a emplear también servidores canadienses, turcos y estonios para dirigir a sus botnets (Monroe, Ejercito de los Estados Unidos de Norteamerica. Operaciones en el ciberespacio, 2014)

Georgia trasladó la página web de su presidente a un servidor de Blogspot, un servicio de la compañía Google, en California; los rusos respondieron entonces creando páginas del presidente falsas y redirigiendo el tráfico hacia ellas. La banca georgiana apagó sus servidores con la esperanza de salir airosa de los ataques; incapaces de llegar a los bancos georgianos, los rusos hicieron que sus botnets bombardearan con tráfico la comunidad bancaria internacional fingiendo que el ciberataque provenía de Georgia, estos ataques desencadenaron una respuesta automatizada en la mayoría de los bancos extranjeros, que cortaron sus conexiones con el sector bancario georgiano (Diaz, 2014).

Sin acceso a los sistemas de liquidación europeos, las operaciones bancarias quedaron paralizadas en Georgia, los sistemas de las tarjetas de crédito también se vinieron abajo, y pronto los siguió el sistema de telefonía móvil.

1.2.6. ATAQUE INFORMÁTICO CONTRA INSTALACIONES NUCLEARES

Cymerman (2010) en la Vanguardia, informa que Irán sufrió el 27 de septiembre de 2010, el ataque cibernético más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet. Los expertos consultados afirman que el 60% de los ordenadores iraníes se podrían haber visto afectados, igual que el 20% en Indonesia y el 8% en India (Diaz, 2014). El virus Stuxnet se convierte en agente durmiente y se puede accionar a distancia en el momento que su creador lo desee sin que el usuario sea consciente.

Dada su complejidad sin precedentes es imposible que haya sido creado por un hacker en solitario. Todo apunta a un equipo de profesionales que han dispuesto de medios y dinero suficiente y al menos seis meses de tiempo para prepararlo (Acosta, El econosmista, 2010). Los expertos consideran que el Stuxnet es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas como centrales eléctricas y nucleares, represas e industrias químicas. «La complejidad del programa es tal que los especialistas en seguridad informática que lo han examinado están convencidos de que no puede ser obra de un mero pirata informático. La mayoría

opina que hay un Estado detrás y que es el primer ejemplo de guerra cibernética» (Acosta, 2010).

Este tipo de troyano no utiliza Internet para propagarse, sino que lo hace a través de lápices de memoria de tipo USB. Primero, el virus se oculta mediante un rootkit2 a nivel de kemel3 firmando con certificados robados a los fabricantes de hardware JMcron y Realtek, lo que implica también que previamente tuvo que realizarse un ataque a estas empresas para substraer dicho material criptográfico (Medero G. s., 2012).

1.2.7. ATAQUE INFORMÁTICO CONTRA LA PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA

Este ataque ocurrió durante el primer semestre de 2011, "cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República de Colombia, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas"(Planeación, 2011).

1.2.8. ATAQUE A UNA PLANTA DE ACERO ALEMANA.

A finales de 2014, un ataque lanzado contra una planta de acero alemana provocó daños físicos, de acuerdo con un reporte de la Oficina Federal para la Seguridad de la Información de Alemania, debido a que los atacantes utilizaron correos electrónicos con spear-phishing e ingeniería social inteligente, logrando penetrar a la red de producción y sistemas de control de la planta (Stel, 2014).

1.3. CONTEXTO LEGAL:

Hoy día, en el entorno socio económico mundial, el desarrollo del ciberespacio ha aumentado las interacciones comerciales, sociales, gubernamentales y delictivas, por lo cual han aumentado las ciber-amenazas y los países han dedicado parte de sus esfuerzos a desarrollar una estrategia legal que pueda ser efectiva (estratégicos, 2010), para contrarrestarlas.

Cada día el ciberespacio le brinda a las organizaciones delictivas, unas capacidades para hacer daño, que les garantiza causar la repercusión mediática que tienen los incidentes informáticos, especialmente cuando se combinan con acontecimientos de gran relevancia cuya seguridad física haría muy difícil actuar contra ellos directamente (Corredera, 2012).

Países como los Estados Unidos de Norteamérica, tienen leyes muy estrictas en cuanto al uso inapropiado de las redes informáticas y han llegado al punto de que rastrean e identifican desde el lugar donde estén cometiendo un delito informático. El Gobierno de los Estados Unidos de Norteamérica, creó un proyecto de ley diseñado para el intercambio de información con las empresas más influyentes en el ámbito de la tecnología y las comunicaciones, con el objeto de identificar amenazas en el ciberespacio y optimizar la seguridad de los sistemas (Leithauser, 2013).

Asimismo, en otros países se han implementado convenios como el CICTE que permiten trabajar de manera conjunta entre países de diferentes regiones del mundo, buscando minimizar al máximo los ataques ciber-terroristas, tratando de contrarrestar las técnicas que utilizan estos grupos, con el objetivo de capturar a los ciber-delincuentes y sancionar todo este tipo de delitos (Tahajian, 2013). Sin embargo, existen vacíos jurídicos que blinden las vulnerabilidades de la guerra informática y que garanticen que la comisión de un delito informático, sea penalizado apropiadamente.

En España se cuenta con la Ley Orgánica 15/1999 de 13 de diciembre de protección de datos de carácter personal. El real decreto 1720/2007, del 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal. Ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI-CE), la ley 59/2003 de 19 de diciembre de 2.003 de la firma electrónica. El Real decreto 1/1996, del 12 de abril, por la cual se aprueba el texto de la propiedad intelectual (Jimenez, 2015).

En Colombia en enero de 2.009, el congreso aprobó la ley 1273 por medio de la cual se modifica el Código Penal, debido a que se creó un nuevo bien jurídico tutelado –denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Ley 1273 , 2009), cuyo Capítulo I relaciona como atentados contra la confidencialidad el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño Informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales.

Asimismo, el 18 de agosto de 1.999, se reglamentó el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales mediante la Ley 527 de 1999 - COMERCIO ELECTRÓNICO. Más adelante, el 24 de julio del año 2.000 se declaró la ley 599 de 2.000, que multa a quien se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo. Luego, el 08 de julio de 2.005 se dictaron disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

En el código penal Colombiano, Ley 599 de 2000, en el capítulo VII "De la Violación a la Intimidad, Reserva e Interceptación de Comunicaciones" se tipifican delitos que bien pueden llegar a verse relacionados con tecnologías de la Información y las Comunicaciones, sin embargo no hay una específica precisa para delitos de esta naturaleza; por lo que para tener una idea de los diferentes tipos de delitos informáticos que existen se tomará como referencia el "Convenio sobre la Ciberdelincuencia", realizado por el Consejo de Europa el 23 de Noviembre de 2001. En dicho documento se dividen los delitos informáticos en cuatro grupos, como se muestra a continuación:

a. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de los anteriores delitos.

b. Delitos informáticos.

- Falsificación informática mediante la introducción, alteración, borrada o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

c. Delitos relacionados con el contenido.

- Producción, oferta, difusión, transmisión, adquisición o tenencia, en sistemas o soportes informáticos, de contenidos de pornografía infantil.

d. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

El interés colombiano por regular y reglamentar los delitos informáticos, se ven reflejados en casos como la detención y condena del hacker Andrés Sepúlveda, condenado en el mes de abril del año 2.015, por los delitos de concierto para delinquir, espionaje, violación de datos personales y uso de software malicioso durante la campaña del ex candidato presidencial Oscar Iván Zuluaga (Pelaez, 2015). Con este hecho de la justicia, se evidencia que en Colombia se sanciona la comisión de este tipo de delitos.

Por otra parte, en el ámbito mundial, la mayoría de los ataques informáticos se han recogido bajo denominación de la categoría de "Ciber-crimen", es decir corresponde a los delitos cometidos por medio de ordenadores a través de internet, tales como: la pornografía infantil, el robo de información personal o violación de las leyes de

asociación, difamaciones, etcétera (Casabona, 2014), lo cual coincide con todo aquello que en Colombia son considerados como delitos informáticos.

Ahora bien, ante la importancia que para el gobierno Nacional de Colombia, reviste implementar políticas para los tópicos de ciberseguridad y ciberdefensa, se adoptó una política cuyas bases se encuentran consignadas en el documento CONPES 3701, donde se traza como objetivo central el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético. Allí, se definen tres objetivos específicos: 1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; 2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y 3) Fortalecer el cuerpo normativo y de cumplimiento en la materia (Planeación, 2011).

1.4. CIBERSEGURIDAD EN LA ARMADA NACIONAL

La Armada Nacional es la institución de Colombia, que contribuye a la defensa de la Nación a través del empleo efectivo de un poder naval flexible en los espacios marítimo, fluvial y terrestre bajo su responsabilidad, con el propósito de cumplir la función constitucional y participar en el desarrollo del poder marítimo y a la protección de los intereses de los colombianos (Durán, 2011). Protege la vida humana en el mar, garantiza la libre navegación, la adecuada señalización marítima en sus aguas jurisdiccionales, hace cumplir la normatividad internacional del mar, las convenciones de la OMI, entre otras, con la eficiente utilización de sus medios en coordinación con las entidades encargadas del control marítimo nacional (Dirección General Marítima, Comisión Nacional del Océano).

De la misma forma, cuenta con los sistemas tecnológicos y la capacitación profesional para compartir información de inteligencia con las agencias internacionales y nacionales, con el fin de negar a las bandas narcotraficantes el uso del mar para actividades ilícitas, debido a que un alto porcentaje de todo el tráfico de narcóticos se da

por vía marítima a bordo de buques portacontenedores, lanchas rápidas ("Go-Fast"), lanchas de transporte u otros artefactos semisumergibles, "con un promedio de más de un evento por día, con la capacidad de colocar entre una y una y media toneladas de cocaína en el mercado internacional" (Colombia, 2007).

Adicionalmente, la Armada Nacional "participa en operaciones combinadas de interdicción marítima y de entrenamiento en cumplimiento de convenios internacionales que Colombia ha suscrito con varios países del mundo" (Duran, 2011), tales como: Operaciones Unitas, Operación Antártida (investigación científica en el polo sur), Operaciones DESI (entrenamiento Submarinos Diesel) y Operación Atalanta (OTAN-Cuerno de África). Estas operaciones internacionales, favorecen la imagen institucional en escenarios de gran importancia marítima mundial, donde las unidades navales de superficie y submarinas de la Armada evidencian las capacidades tecnológicas actuales con que se cuentan, para ser parte de operaciones multinacionales en contra de las amenazas en el mar.

Teniendo en cuenta los diferentes roles anteriormente mencionados, se hace necesario que la Armada Nacional fortalezca sus capacidades en el nuevo campo de batalla, denominado el quinto dominio "el ciberespacio"(Meyerrose, 2010), donde cada día se tiene mayor cantidad de información sensible y estratégica de nuestras capacidades funcionales, procesada a través del uso de herramientas informáticas para el mantenimiento, la educación, la gestión del talento humano y las comunicaciones operacionales, entre otras. Ahora bien, a pesar de que se han implementado una serie de controles en lo concerniente al uso de las redes informáticas, aún no se cuenta con una estrategia sólida que garantice la apropiada protección de las plataformas de información de la institución.

Por ello, desde el año 2.011 el Departamento Nacional de Planeación con el trabajo conjunto del Ministerio de Defensa, Ministerio del Interior y Ministerio de Relaciones Exteriores entre otros, escribieron los lineamientos de política para ciberseguridad y ciberdefensa Nacional, orientados a desarrollar una estrategia nacional que contrarreste

el incremento de las amenazas informáticas que afectan significativamente al país (Planeación, 2011). Es de esa manera, que la Armada Nacional ha derivado sus directrices institucionales en ciberseguridad, enmarcado en dichos lineamientos, en los antecedentes nacionales e internacionales, así como de la normatividad del país en torno al tema.

Más aún, cuando las noticias de ciberataques a ciudadanos, organizaciones, empresas y, hasta, instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diferentes índoles se han vuelto habituales en los diferentes medios de comunicación no sólo escritos, sino radio, televisión y, naturalmente, los medios electrónicos de Internet (estratégicos, 2010). Al igual, en las operaciones militares, los ataques cibernéticos también se han convertido en una amenaza, más aun sabiendo que con el uso de estos se pueden afectar los sistemas de control del enemigo y viceversa.

Tanto así, que "los países ya están haciendo uso de las ciber operaciones para atacarse entre sí, al punto que estas se convirtieron en la ventaja para colocar en desventaja al adversario en el contexto ciber electromagnético" (Lucious Morton, Ejercito de los Estados Unidos de Norteamerica, 2010), obligando a las Fuerzas Militares a tener planteada una estrategia de ciberdefensa, para estar alerta y proteger los sistemas informáticos en todo momento. "La expansión del ciber-espionaje ha elevado el riesgo de interrupción de infraestructuras como estaciones eléctricas y servicios financieros. La amenaza es real y creíble" (Lobban).

La Armada Nacional desde el año 2.014, implementó la unidad cibernética, dependencia que actualmente funciona bajo el control de la Jefatura de Inteligencia Naval para realizar tareas de análisis y recolección de información a través del ciberespacio en coordinación con el Comando Conjunto Cibernético de las Fuerzas Militares (Ruiz, 2015), con el fin de optimizar el desarrollo de las operaciones de Inteligencia. Asimismo, desde allí se realizan tareas de seguridad informática, tales como:

1.4.1. Establecer las directrices institucionales de seguridad informática encaminadas a proteger los activos informáticos de cada una de las dependencias de la Armada Nacional (Ruiz, 2015),

1.4.2. Plantear tácticas de ciberseguridad con el objetivo de concientizar a todo el personal a dar un uso apropiado del ciberespacio (Ruiz, 2015).

1.4.3. Mantener clasificados los activos de información acuerdo los requerimientos de confidencialidad, integridad y disponibilidad (Ruiz, 2015).

1.4.4. Realizar periódicamente los niveles de riesgo, para determinar las amenazas vigentes y confirmar requerimientos de confidencialidad de las redes institucionales.

1.4.5. Supervisar continuamente que nadie tenga acceso físico sin autorización a la redes de información de la Armada Nacional (Ruiz, 2015).

Como parte de la Estrategia de la Unidad Cibernética de la Armada Nacional, se tiene proyectado adquirir capacidades en infraestructura, herramientas tecnológicas y aplicaciones virtuales de seguridad informática entre otras, que permitan ejercer un adecuado control del ciberespacio institucional (Medina, 2015). De la misma forma, se tiene planeado capacitar oficiales y suboficiales que adquieran los conocimientos y la experiencia en ciberdefensa y ciberseguridad, para que neutralicen el entorno de amenazas cibernéticas e implementen constantemente sistemas de protección virtual (Medina, 2015). Que se mantengan actualizados en los últimos desarrollos e inventivas del ámbito cibernético para que tengan la capacidad de contrarrestar cualquier intento de vulnerabilidad de los activos informáticos de la institución.

Sin embargo, el presupuesto es limitado para ampliar sus capacidades en material y personal, debido a que no se cuenta con suficientes recursos económicos para fortalecer estas necesidades. En lo concerniente a la educación, se hace necesario mantener un personal altamente calificado a la altura de los países más desarrollados en ciberdefensa, con el fin de que se puedan dedicar al monitoreo y la supervisión de las redes informáticas en el más alto nivel de los desarrolladores de software y uso de las redes virtuales del ciberespacio. A su vez se hace necesario, que todos los miembros de la

Armada Nacional adopten una cultura de la seguridad informática, enmarcada en la protección de la información institucional, desde el uso apropiado de la documentación, hasta el uso seguro de los medios informáticos tales como; teléfonos inteligentes, tablets, laptops, pc´s, memorias usb y todo tipo de dispositivos móviles en los que no está autorizado el almacenamiento de información clasificada.

CAPITULO II

2.1 MECANISMOS QUE UTILIZA LA ARMADA ESPAÑOLA PARA OPTIMIZAR LA CIBERSEGURIDAD Y LA CIBERDEFENSA

Para asegurar una adecuada protección del ciberespacio, en la Armada Española se ejerce un efectivo control mediante el uso de la defensa en profundidad (término militar que se utiliza para denotar el uso de varias líneas de defensa consecutivas) (Secretaría General Técnica, Ministerio de Defensa, 2012), dividiendo el ciberespacio en tres grandes sectores sobre los cuales se ubicarán las diferentes barreras de protección, así: 1) Sector del ciberespacio utilizado por la red cibernética naval. 2) Sector del ciberespacio utilizado por las infraestructuras críticas. 3) Sector del ciberespacio utilizado por la población en general.

Este concepto se puede complementar con lo contenido en el documento del NIST SP800-53: Recommended Security Controls for Federal Information Systems and Organizations, el cual define la defensa en profundidad como una estrategia de la seguridad de la información que contempla las actividades operativas cotidianas, la tecnología y las personas, de cara a establecer un conjunto de barreras o controles implementados en múltiples capas de una organización (Pacheco, 2012).

Para la ejecución de esta defensa se cuenta con un centro de comando y control de ciberseguridad y ciberdefensa, donde se cuenta con la capacidad de asegurar y salvaguardar la prestación de los servicios proporcionados por los sistemas de información y Comunicaciones en la fase de operación de los sistemas en producción, en respuesta a posibles inminentes acciones maliciosas originadas en el ciberespacio (Higuera, 2013). Allí se protegen 03 escenarios así:

1. Red Cibernética Naval: Hace referencia básicamente a la red informática de la Armada Española, la cual está formada por todos los equipos interconectados en la Institución a través de los cuales se intercambia información operativa o administrativa y se comparten recursos entre dependencias según los requerimientos (Higuera, 2013).

2. Redes Utilizadas por Infraestructuras Críticas: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación (M. J. West-Brown, 2003). Teniendo en cuenta lo anterior, estas apoyan de forma directa o indirecta al desarrollo de la misión institucional; estas son, por ejemplo, las entidades prestadoras de servicios públicos, contratistas que presten servicios indispensables para la Institución, red bancaria, etc.
3. Redes de Sistemas Informáticos dentro del área de Responsabilidad: Son todas aquellas redes, públicas o privadas, que se encuentran dentro del área de responsabilidad operacional asignada a la Institución, las cuales son protegidas por la misma.

De la misma forma, cuentan con una "Doctrina de Ciberseguridad", que contiene lineamientos, órdenes e instrucciones para todo el personal de usuarios y administradores de la red cibernética, que conlleva a la utilización de las tecnologías de la información y las comunicaciones de forma segura entre todos los puntos y nodos de la red de sistemas informáticos institucionales, donde se establecen procedimientos que permiten adelantar estudios sobre el comportamiento de los focos de amenaza en el ciberespacio y canales de comunicación seguros (Secretaría General Técnica, Ministerio de Defensa, 2012) entre las Fuerzas Armadas (Ejército Nacional, Armada Nacional y Fuerza Aérea).

Con una doctrina orientada hacia un escenario de combate cibernético (Monroe, Ejercito de los Estados Unidos de Norteamerica. Operaciones en el ciberespacio, 2014), con los procedimientos a seguir cuando la amenaza está causando daños a las redes de interés, tales como: procedimientos para la recopilación de información en el ciberespacio que conduzca al desarrollo de actividades de inteligencia cibernética.

La Armada Española protege las redes institucionales y las utilizadas por infraestructuras propias, utilizando los procedimientos y tecnologías necesarias para

contrarrestar y neutralizar cualquier amenaza detectada antes que puedan llegar a ocasionar algún tipo de daño dentro de las redes de interés institucional, las cuales se dividen en las siguientes capacidades:

1. **Capacidad de Defensa**: con el objetivo de prevenir, detectar, reaccionar y recuperarse frente a ataques, intrusiones, interrupciones o cualquier tipo de acción hostil que pueda comprometer la información que transita dentro de la red cibernética naval, las redes utilizadas por las infraestructuras críticas y las redes que se encuentren dentro del área de responsabilidad de la Armada Española (Díaz, 2015).
2. **Capacidad de Inteligencia**: con el objetivo de recopilar, analizar y procesar toda la información relacionada con las tecnologías y sistemas utilizados por los adversarios (diaz, 2015).
3. **Capacidad de Respuesta**: con el objetivo de desplegar medidas y acciones que se deban tomar frente a amenazas y ataques que se presenten dentro de las redes de interés institucional o cualquier sector del ciberespacio donde se requiera la acción de la Armada Española (Higuera, 2013).

Para el cumplimiento de los objetivos de las **capacidades de defensa** las subdividen en cuatro grupos:

1) Valoración dinámica del riesgo: Previene ataques contra la red cibernética naval, realizando evaluaciones periódicas, con el fin de analizar la evolución de la amenaza y poder proponer mejoras en la estrategia de ciberdefensa, para lo cual tienen las siguientes capacidades:
   a. Capacidad para mantener actualizada la situación del estado del sistema y análisis de vulnerabilidades: Cuenta con un mapa de la red cibernética naval donde se tienen inventariados todos los dispositivos que se encuentran interconectados dentro de la misma (Higuera, 2013).
   b. Capacidad para gestionar los riesgos presentes en la red cibernética naval: se cuenta con una matriz de riesgo que permite evaluar de forma constante los riesgos presentes en la red cibernética naval (Higuera, 2013).

c. Capacidad para evaluar la amenaza: Cuentan con un laboratorio de ciberseguridad donde se realiza un estudio a fondo de las tecnologías y sistemas utilizados para atacar redes informáticas (Higuera, 2013).
d. Capacidad para establecer escenarios de entrenamiento: Cuentan con aulas de simulación para entrenar los posibles escenarios de amenaza o de riesgo inminente, donde se pone a prueba la reacción del personal encargado de monitorizar la red cibernética naval (diaz, 2015).
e. Capacidad para mantener actualizado el hardware y software: Tienen un programa de renovación periódica de los equipos consistente en la instalación de mayores capacidades de memoria, de almacenamiento, de procesamiento, etc (diaz, 2015).

2) Detección y análisis de ataques cibernéticos y actividades maliciosas: tiene el objetivo de medir el nivel de daño que se haya causado contra la red institucional, al tiempo que permite tomar medidas para mitigar el riesgo. Para lo cual se tienen las siguientes capacidades:
   a. Capacidad de monitorizar la red cibernética naval: cuentan con un sistema de monitoreo que alerta en el momento oportuno sobre la presencia de actividades maliciosas, permitiendo identificar falsos positivos y falsos negativos en tiempo corto, que permite tomar las medidas necesarias en el momento oportuno (diaz, 2015).
   b. Capacidad para almacenar y procesar la información recopilada por los sensores sobre actividades maliciosas o ataques contra la red cibernética naval: Cuentan con la capacidad de almacenar y procesar la información recopilada por los sensores de monitorización, en coordinación con el personal destinado a evaluar la amenaza (diaz, 2015).
   c. Capacidad de evaluación de entidades: Cuentan con los recursos necesarios que permitan recopilar datos con el suficiente detalle, como para caracterizar eventos en curso y poder clasificarlos como maliciosos o no y a su vez asignarles atributos (diaz, 2015).
   d. Capacidad para emitir una evaluación de la situación: cuentan con los medios que permiten emitir una valoración sobre un evento de seguridad que se presente,

con el fin de poder tomar las medidas necesarias de forma eficiente, en el momento oportuno (diaz, 2015).

3) Toma de decisiones en tiempo oportuno: tiene el objetivo de reaccionar ante una situación de riesgo que se evidencie en contra de la red cibernética naval. Para lo cual tienen las siguientes capacidades:
   a. Capacidad para identificar opciones: Es el primer paso, ante un ataque o cualquier situación que ponga en riesgo la seguridad y la integridad de la red cibernética naval, porque permite identificar las vías de acción disponibles que permiten neutralizar el riesgo (diaz, 2015).
   b. Capacidad para comunicar y controlar los cursos de acción determinados: permite la coordinación entre varios sectores de la red cibernética naval, para coordinar todas las acciones que se determinen necesarias para responder ante un ataque o actividad maliciosa (diaz, 2015).
4) Recuperación frente a ciberataques: con el objetivo de recuperarse de un ataque mediante la restauración del sistema y la información a su estado original y a sus propiedades de seguridad. Para lo cual tienen las siguientes capacidades:
   a. Capacidad para valorar los daños: Identifica en el menor tiempo posible los daños ocasionados en la red cibernética naval por causa de un ataque, una vez este ha sido confirmado y detenido; a su vez, cuentan con la capacidad de identificar los sistemas afectados y determinar cada uno de los sistemas que se vieron afectados por el ataque y delimita los sectores de la red comprometidos. Verifica la integridad de la información, identifica la información comprometida y verifica la disponibilidad de los servicios (diaz, 2015).
   b. Capacidad para restaurar la integridad del sistema: Cuentan con los medios y recursos necesarios para devolver la red cibernética naval a un estado de seguridad no comprometido. Para ello utiliza las siguientes técnicas: Virtualización, implantación de arquitecturas de alta disponibilidad en sistemas y dispositivos de red, almacenamiento y restauración de imágenes de máquinas guardadas como copia de seguridad cuya integridad haya sido verificada, reinstalación completa de los mismos como última medida (diaz, 2015).

c. Capacidad para restaurar la integridad de la información: Cuentan con los procedimientos y los medios necesarios para restaurar la información almacenada o procesada, por el sistema, a un estado anterior de nivel de seguridad no comprometido, de forma que se pueda verificar su integridad y confidencialidad (diaz, 2015).

d. Capacidad para realizar trazabilidad de la información comprometida: Cuentan con un registro de toda la información, cuya confidencialidad haya sido comprometida, para poder informar convenientemente a todas las partes interesadas (diaz, 2015).

En cuanto a las actividades de inteligencia, recopilan, distribuyen e intercambian información sobre las tecnologías utilizadas por los atacantes en el ciberespacio (Secretaría General Técnica, Ministerio de Defensa, 2012); asimismo realizan análisis de la información recolectada y con base en esto establecen el panorama que permite al mando mantener actualizado el estado de conciencia situacional sobre el ciberespacio, en lo referente al sector utilizado por las infraestructuras críticas, lo cual para cumplir con los objetivos de las **capacidades de Inteligencia** lo subdividen en tres niveles:

1) **Obtención de Información**:

Proceso desarrollado con el fin de alcanzar el primer nivel de conciencia situacional, la percepción, para ello obtienen la mayor cantidad de datos relacionados con actividades maliciosas y ataques detectados en el ciberespacio (Inteligencia, 2010). Esta recolección de información la realizan básicamente, a través de dos métodos:

a. **Obtención de información de fuentes abiertas:** Reúnen la mayor cantidad posible sobre las tecnologías de la información y comunicaciones utilizadas en ataques y actividades maliciosas, llevadas a cabo en el ciberespacio, a través de fuentes abiertas tales como páginas web, redes sociales, medios de comunicación, google hacking, documentos públicos (Inteligencia, 2010), etc.

b. **Sistemas de Decepción:** Consiste en la instalación de sistemas de decepción que sean llamativos para el atacante, pero que no pongan en riesgo ni la red cibernética

naval ni las utilizadas por las infraestructuras críticas, estos sistemas también se pueden constituir de cierta forma en un medio de defensa ya que ralentizan el ataque de manera significativa, permitiendo reconfigurar la red para resistir mejor el ataque; sin embargo su principal objetivo será el de permitir el estudio y caracterización de las acciones y consecuencias de un ataque (Inteligencia, 2010).

2) **Análisis de Malware**

Este grupo de capacidades está orientado a alcanzar el segundo nivel del estado de conciencia situacional, la comprensión, para ello con base a la información recopilada anteriormente, se deben asignar los recursos necesarios que permitan analizar y comprender el funcionamiento de todo tipo de malware, con el fin de llegar a establecer el nivel de daño que estos podrían ocasionar en el ciberespacio, conocer su estructura, funcionamiento e interacción (diaz, 2015).

El grado de complejidad de las técnicas y el nivel de conocimientos necesarios para analizar malware es proporcional al nivel de sofisticación del mismo; estas se conocen como técnicas de análisis y reingeniería del malware, las cuales pretenden facilitar la adquisición de conocimiento sobre el mismo de una manera sistemática y metodológica (diaz, 2015), a continuación se relacionan algunas capacidades:

a. **Capacidad para clasificar malware:** Según Panda Security en el año 2010 se identificaron aproximadamente 60 millones diferentes de ejemplares de malware; el excesivo incremento de este tipo de software hace necesario que se haga una clasificación para identificar rápidamente el tipo de amenaza al que se puede ver enfrentado; existen diferentes formas de hacerlo, como ejemplo, se detallan en la figura 1 ("árbol de clasificación" de malware) los tipos de malware en los que se basa el motor antivirus de la firma Kaspersky (madrid, 2011).

b. **Capacidad para analizar Código:** Para investigar acerca de los códigos maliciosos cuentan con mecanismos que permiten estudiar la manera en que opera el malware, uno de éstos consiste en la realización de un análisis bajo ambiente controlado que permite generar información para mitigar el impacto, alertando a los involucrados (Endsley, 1995). Para analizar este código utilizan dos técnicas:

i. **Análisis de comportamiento:** También conocido como análisis dinámico, su objetivo es el de investigar la actividad del malware en el sistema comprometido. El comportamiento se puede observar y analizar a través de un ambiente controlado, ya sea virtual, o bien por medio de una red donde este limitado el tráfico con el propósito de evitar la propagación e infección hacia otros equipos de la organización (Endsley, 1995). En este punto, se monitorea la actividad de los procesos maliciosos que ejecuta el malware, los puertos que abre, su actividad en la red (es decir si se comunica a un servidor remoto o a algún dominio), el tipo de protocolo que utiliza para comunicarse con él (HTTP, IRC) y la manera en que se activa en el sistema comprometido (que puede ser mediante la activación de un servicio o iniciándolo directamente desde los archivos de inicio). Para este proceso, resulta más sencillo utilizar equipos virtuales, pues permiten regresar al escenario original de manera más sencilla, aunque algunos binarios maliciosos ya son capaces de detectar este tipo de ambientes para evitar su ejecución y de esta forma dificultar su análisis (Endsley, 1995).

ii. **Estudio del código:** También conocida como análisis estático, esta técnica requiere la aplicación de técnicas como la ingeniería inversa y depuradores para desensamblar el código, debido a que la mayoría de las ocasiones se parte de un archivo binario y no se cuenta con el código fuente (Francés). Es necesario tener un conocimiento técnico avanzado para interpretar el código desensamblado (Endsley, 1995).

3) Intercambio de Información de Ciberdefensa

Este grupo de capacidades lo tienen orientado para alcanzar el tercer nivel del estado de conciencia situacional, la proyección, y su objetivo es el de compartir información o datos de ciberdefensa y colaborar intercambiando conocimiento entre las personas y organismos expertos en las diferentes áreas de la ciberdefensa. Para ello disponen de enlaces seguros y protocolos comunes e interoperables, con el fin de mantener canales de comunicación que permitan el tránsito de información sobre amenazas en el ciberespacio entre los equipos CERT/CSIRT de la administración, las

organizaciones privadas y las empresas encargadas de la gestión de infraestructuras críticas.

Lo anterior permite establecer protocolos de coordinación para responder de forma conjunta contra los ciberataques que se detecten, distribuye rápidamente información sobre nuevas amenazas y toma las medidas que obstaculicen al accionar de los posibles adversarios en la red. Para cumplir con los objetivos propuestos para este grupo cuentan con las siguientes capacidades:

a. **Capacidad para compartir información de ciberdefensa de forma eficiente:** Esta capacidad está orientada a contar con los recursos y protocolos necesarios para distribuir en el momento oportuno la información, recopilada de diferentes fuentes así como la de incidentes en curso, entre las agencias y organizaciones con las que se establezcan previamente acuerdos de colaboración (Francés).
b. **Capacidad para garantizar la capacidad de la información de ciberdefensa:** Esta capacidad está orientada a gestionar la confiabilidad de la información de ciberdefensa recibida, dado que esta puede provenir de diferentes fuentes, incluyendo desde fuentes abiertas en Internet a informes de la comunidad de inteligencia (Técnica, 2012).
c. **Capacidad para recolectar y explotar el histórico de datos:** Registran información en almacenes de datos de corta y larga duración, con el fin de que estos puedan ser útiles en futuras acciones; este histórico de datos puede incluir tráfico de red, información captada por sensores, etc (Técnica, 2012).

Por último, existen tienen las **capacidades de respuesta**, las cuales están encaminadas a demarcar las medidas y acciones a tomar ante amenazas o ataques; esto quiere decir que con estas capacidades buscan no solamente proteger las redes de interés Institucional sino desplegar técnicas en el ciberespacio que permitan neutralizar el accionar de los adversarios. Para cumplir con el objetivo propuesto desarrollan y fortalecen las siguientes capacidades:

1) **Capacidad para mitigar Ciberataques**

Este grupo de capacidades conlleva a contar con los recursos y protocolos necesarios que permitan, de forma eficiente, realizar cambios de configuración de los sistemas TIC, gestión de los componentes criptográficos, autenticación, manipulación de los flujos de tráfico y el registro y mantenimiento de la cadena de pruebas para el propósito de juicios posteriores (E. Fojón Chamorro, 2012), para cumplir con los objetivos planteados cuentan con las siguientes capacidades:

a. **Configuración de aplicaciones TIC:** Consiste en permitir a los operadores configurar los componentes de los sistemas TIC, incluyendo la infraestructura de red, servicios de los sistemas de información, seguridad, etc., al objeto de poder contrarrestar un incidente o realizar un proceso de reacción ante el mismo. Para ello disponen de aplicaciones de configuración de los sistemas fuera de banda como una red LAN aparte y protegida por firewall, para evitar que sea comprometida (Técnica, 2012).

b. **Denegación de permisos de acceso:** Capacidad de retirar los privilegios específicos a una entidad o usuario basándose en su identidad autenticada. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, localización de la entidad solicitante, prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. Los privilegios pueden ser: filtrado de direcciones IP, asignación de direcciones, de rutas, de parámetros de calidad de servicio, de ancho de banda y algoritmos cifrado. Esta capacidad les exigió la implantación de sistemas AAA, los cuales se basan en protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Técnica, 2012).

c. **Reconfiguración de la topología de los sistemas:** Capacidad para modificar la estructura topológica de los sistemas TIC, incluyendo sus servicios, software y hardware, interconexiones, etc., así como la configuración de cualquiera de sus módulos o componentes. A su vez se compone de:

i. **Reubicación de los servicios de información:** Capacidad para mover servicios y su información asociada a infraestructuras TIC alternativas en ubicaciones diferentes (Técnica, 2012).

ii. **Aislamiento de sistemas:** Capacidad de separar y aislar ciertas partes de un Sistema TIC con el propósito de limitar y amortiguar los daños e impacto producido por un ciberataque, y preservar la integridad, confidencialidad de la información y la disponibilidad operativa del sistema. Se basa en el principio de "El mínimo privilegio" que implica la asignación a cada usuario o proceso un nivel de privilegios, de modo que únicamente pueda acceder a los datos que debe gestionar y a nada más (Técnica, 2012).

iii. **Bloqueo de componentes y servicios:** Para el desarrollo de esta capacidad establecen los grados de relevancia de los sectores de la red cibernética naval y el de las infraestructuras críticas; el objetivo es determinar los mínimos sectores de la red cibernética naval, con los cuales se podrían mantener las operaciones navales. Lo anterior teniendo en cuenta que en caso de un ataque sería necesario detener componentes o servicios de un sistema, como máquinas de proceso, puertos o interfaces de red, como medida eficaz para mitigar los efectos producidos (Técnica, 2012). En todo caso, el comando operacional del sistema valida y sopesa este tipo de actuaciones, pues puede impactar negativamente en la operación.

iv. **Control del flujo de tráfico**: Capacidad para realizar el encaminamiento de las comunicaciones de un sistema por otros enlaces, lo que significa que disponen de redundancia de comunicaciones terrestre y satelitales, limitan a un cierto ancho de banda, o modifican el retraso de un flujo de datos, con el fin de detener o mitigar un ataque (Diaz, 2015).

v. **Coordinación de la respuesta externa:** Capacidad de coordinación con los proveedores de servicio nacional o internacional, y otros organismos e instituciones afines, con el fin de detener o mitigar los ataques que se detecten.

d. **Defensa Activa:** Cuentan con la capacidad de utilizar técnicas de ataque con el único propósito de detener o mitigar un ataque en curso. Tienen como objetivo retomar el control sobre los recursos propios o sofocar ataques neutralizando la fuente de los mismos (Técnica, 2012).

Por otra parte, cuentan con lo siguiente:

i. Centro de comando y control cibernético:

Está dotado con equipos especializados cuya tecnología está diseñada para realizar un monitoreo continuo de las redes informáticas que controlan la infraestructura de los servicios estatales y públicos, para lo cual cuenta con grupos de personas especializadas en el manejo de las redes informáticas, sistemas de encriptación y des-encriptación virtual (Técnica, 2012).

ii. Definición de Infraestructuras Criticas:

Se cuenta con un registro de todas las infraestructuras críticas y su distribución en áreas de responsabilidad de la institución. Allí se tienen determinadas cuáles infraestructuras son críticas, tales como: Entidades gubernamentales, Empresas prestadoras de servicios públicos, Entidades del sector salud, Redes eléctricas, Redes de Comunicaciones, industrias del Sector farmacéutico, Industrias de petróleo, Industrias de gas, empresas del Sector financiero, Oleoductos, Empresas de transporte y Fábricas de artículos de primera necesidad (Corporation, 2015).

iii. Auditorias de seguridad a las redes cibernéticas:

Antes de lanzar cualquier tipo de estrategia hacia el exterior de la red cibernética, que conduzca a la neutralización de las amenazas en el ciberespacio, realizan una auditoría del estado de seguridad de la misma que permita incrementar los niveles de seguridad para evitar futuros daños en el desarrollo de operaciones contra los adversarios (Corporation, 2015).

CAPITULO III

3.1 MECANISMOS APLICABLES A LA ARMADA NACIONAL

Al comparar las acciones que ejercen en ciberdefensa y ciberseguridad en la Armada Española y las que ejerce la Armada Nacional de Colombia, entendemos que son acciones desde la perspectiva y el ámbito de la Defensa Nacional, teniendo en cuenta que el ciberespacio permite alcanzar miles de blancos, casi en cualquier lugar del mundo (Monroe, Operaciones en el ciberespacio, plan de capacidades 2.016-2.028, 2010), y su mal uso puede afectar los intereses nacionales de la Nación. Por ello en el ámbito de su responsabilidad, la Armada Española vela por el control del ciberespacio de acuerdo con los instrumentos jurídicos internacionales y la legislación nacional, a fin de detectar una intención de amenaza cibernética y minimizar un posible daño.

Para realizar un análisis y verificar cuales medidas son las más aplicables para optimizar en la Armada Nacional de Colombia, se realizó una recolección de información en forma cualitativa, a partir de la investigación documental e investigación electrónica en bases de datos y a través del mecanismo de la entrevista a expertos que permitieron obtener información y evidencia de una muestra de la población.

Asimismo, se realizó una tabla comparativa de las medidas aplicadas por la Armada Española y las que se utilizan actualmente en la Armada Nacional de Colombia (Tabla 2: Comparativo de medidas aplicadas por la Armada Española y la Armada Nacional de Colombia.), donde se identificaron cuales medidas no se tienen implementadas en la Armada Nacional de Colombia y se clasificaron como variables principales. Posteriormente se empleó la modelación de las variables seleccionadas a través del uso del software (Mic-Mac), con el fin de identificar por prioridad las variables de mayor influencia que corresponden a las medidas de acción necesarias para optimizar la ciberdefensa y la ciberseguridad en la Armada Nacional de Colombia, con base en las medidas que se utilizan en la Armada Española.

Las variables seleccionadas para identificar las medidas de acción necesarias para optimizar la ciberdefensa y la ciberseguridad en la Armada Nacional de Colombia, fueron:

3.1.1. Establecer la Ciberdefensa como un objetivo estratégico de la Armada Nacional.

3.1.2. Fortalecer las capacidades actuales de control del ciberespacio en la Armada Nacional.

3.1.3. Implementar nuevas capacidades en ciberdefensa de la Armada Nacional, para el control del ciberespacio.

3.1.4. Elaborar la Doctrina de ciberdefensa y ciberseguridad de la Armada Nacional.

3.1.5. Continuar Fomentando en los miembros de la Armada Nacional la cultura de la ciberseguridad.

3.1.6. Crear el Centro de comando y control cibernético de la Armada Nacional.

Con base en las variables obtenidas en los resultados de las encuestas, se corrió un modelo de prospectiva basado en el software MICMAC, el cual nos arrojó un resultado de las variables con más influencia para optimizar la ciberdefensa y la ciberseguridad en Colombia. A estas variables de mayor impacto seleccionadas, se les dio una prioridad y una puntuación acorde a la importancia que reviste como mecanismo de acción para optimizar la ciberdefensa y la ciberseguridad en la Armada Nacional, con base en las respuestas de las encuestas.

Es así, que en la figura 2 del software MIC-MAC "influencia directa de las variables", se observa que "el establecer la ciberdefensa como un objetivo estratégico de la Armada Nacional" (diaz, 2015), es el punto de convergencia de las otras variables y del que se derivan las variables con la influencia más fuerte. Esto refleja la necesidad de que a partir de que se considere a la ciberdefensa como un objetivo estratégico, se van a poder enfocar mayores esfuerzos institucionales en lo concerniente a recursos, personal, etc.

Ahora bien, la variable "elaboración de una doctrina de ciberdefensa en la Armada Nacional" (diaz, 2015), es de fuerte influencia, y su importancia radica en la necesidad de que exista un patrón de procedimientos para cada tipo de evento que se presente o en caso de cualquier amenaza cibernética. También es una variable de fuerte influencia la

cultura institucional, teniendo en cuenta que a pesar de existir políticas institucionales provenientes de la jefatura de Inteligencia Naval (CARLOS, 2015), los miembros de la institución aún no hemos adoptado todas las medidas de seguridad preventivas para minimizar las amenazas cibernéticas.

En la misma figura 2, la línea azul, significa que la variable de implementación de capacidades es relativamente fuerte, debido a que permite minimizar los riesgos ante posibles amenazas. Sin embargo, requiere una inversión importante de recursos en tecnologías para que el sistema de defensa funcione apropiadamente, con el objetivo de prevenir, detectar, reaccionar y recuperarse frente a ataques, intrusiones, interrupciones o cualquier tipo de acción hostil que pueda comprometer la información que transita dentro de la red cibernética naval (diaz, 2015).

Adquirir la capacidad de Inteligencia que utiliza la Armada Española, va a permitir recopilar, analizar y procesar toda la información relacionada con las tecnologías y sistemas utilizados por los adversarios (diaz, 2015), asimismo adquirir unas capacidades de respuesta, con el objetivo de desplegar medidas y acciones que se deban tomar frente a amenazas y ataques que se presenten dentro de las redes de interés institucional o cualquier sector del ciberespacio (Higuera, 2013), donde se requiera la acción de la Armada Nacional.

En el caso del control del ciberespacio (figura 2), se observa que tiene influencia directa con la ciberseguridad, con la ciberdefensa y con la cultura de la seguridad informática. En cuanto a la protección del ciberespacio, se observa que tiene una influencia directa con la conciencia de la seguridad informática y con la necesidad de implementar mayor cantidad de medidas para proteger el ciberespacio. De la misma forma, se observa que el ciberespacio tiene una influencia directa con los medios tecnológicos, el control del ciberespacio, la conciencia de seguridad informática, la doctrina de ciberdefensa y la implementación del centro de comando y control cibernético de la Armada Nacional.

Ahora bien, el control del ciberespacio es una medida de protección que facilita el trabajo de seguridad cibernética, más aun teniendo en cuenta la documentación existente

en lo referente a la seguridad nacional, por lo cual podemos entender con mayor claridad su relevancia en el ambiente de las relaciones internacionales; esta se manifiesta como un proceso continuo e incesante, la cual, es la condición política, económica, militar y social que garantiza el desarrollo y la estabilidad de un Estado. Permite "el equilibrio necesario para asegurar, mediante la aplicación del poder nacional, la obtención y el mantenimiento de los objetivos nacionales, previniendo y actuando ante cualquier amenaza interna o externa que ponga en peligro los intereses de la sociedad" (Martinez, 2011).

Es por ello, que la ciberseguridad y la ciberdefensa se consideran vitales para la seguridad de las comunicaciones, de la información y de la infraestructura de un estado, debido a que mantienen un control preventivo a las amenazas existentes en el ámbito del quinto dominio (el ciberespacio). En el caso de la Armada Nacional, el plan estratégico de ciberdefensa y las acciones en ciberseguridad, favorecen la protección de las plataformas con bases de datos de personal, mantenimiento de las unidades, contratación y gestión de calidad entre otras.

Para que la Armada Nacional ejerza un adecuado control del ciberespacio propio de su misión institucional, se requiere como primera medida: 1. Adquirir ese conjunto de sistemas y capacidades que se complementen entre sí, tal como las que utiliza la Armada Española, entre las que se destacan la capacidad para mitigar ciberataques, la cual conlleva a contar con los recursos y protocolos necesarios que permitan de forma eficiente, realizar cambios de configuración de los sistemas TIC, gestión de los componentes criptográficos, autenticación, manipulación de los flujos de tráfico y el registro y mantenimiento de la cadena de pruebas para el propósito de juicios posteriores (E. Fojón Chamorro, 2012), teniendo en cuenta que son indispensables para garantizar un respaldo de monitoreo ininterrumpido.

b. Como segundo medida, adquirir la capacidad para configurar aplicaciones TIC, con el fin de permitir a los operadores configurar los componentes de los sistemas TIC, incluyendo la infraestructura de red, servicios de los sistemas de información y

seguridad, con el objeto de poder contrarrestar un incidente o realizar un proceso de reacción ante el mismo. De igual manera, que permita a los operadores denegar permisos de acceso y que el operador tenga los privilegios para filtrado de direcciones IP, asignación de direcciones, de rutas, de parámetros de calidad de servicio, de ancho de banda y algoritmos cifrado, cuyos protocolos realicen tres funciones: Autenticación, Autorización y Contabilización (Técnica, 2012).

c. Como tercera medida, adquirir la capacidad para modificar la estructura topológica de los sistemas TIC, incluyendo sus servicios, software y hardware y sus interconexiones, así como la configuración de cualquiera de sus módulos o componentes, con la capacidad de separar y aislar ciertas partes de un sistema TIC con el propósito de limitar y amortiguar los daños e impacto producido por un ciberataque, y preservar la integridad, confidencialidad de la información y la disponibilidad operativa del sistema (Técnica, 2012).

d. Como Cuarta medida, adquirir la capacidad de comunicaciones satelitales, limitar en coordinación con los proveedores de servicio nacional e internacional a un cierto ancho de banda las comunicaciones terrestres, con el fin de detener o mitigar un ataque (Diaz, 2015).

e. Como quinta medida fortalecer la unidad cibernética naval, dependencia que funciona en la Jefatura de Inteligencia Naval (CARLOS, 2015), donde se realizan tareas de ciberseguridad, pero que requiere estar dotado con equipos especializados cuya tecnología está diseñada para realizar un monitoreo continuo de las redes informáticas que controlan la infraestructura de los servicios estatales y públicos, por otra parte, requiere de mayor cantidad de personal capacitado y especializado en el manejo de las redes informáticas, sistemas de encriptación y des-encriptación virtual (Técnica, 2012).

Es así, que en la Armada Española se cuenta con un centro de Comando y Control Cibernético con todas las capacidades tecnológicas y de personal, para garantizar un monitoreo adecuado del ciberespacio y facilitar la neutralización de posibles amenazas a fin de evitar un posible ataque cibernético o infiltración de algunas de las redes

informáticas. En la Armada Nacional, se cuenta con la unidad cibernética naval, dependencia que funciona en la Jefatura de Inteligencia Naval (Medina, 2015), donde se realizan algunas tareas de ciberseguridad limitadas, que favorecen el desarrollo de las operaciones de inteligencia institucionales, pero que poseen debilidad tanto de personal como de tecnología para desarrollar operaciones de control del ciberespacio.

La proyección que esta unidad cibernética requiere, es la de poder contar con capacidad para: compartir información de ciberdefensa de forma eficiente con centros de comando y control cibernético de otros países, garantizar la información de ciberdefensa, recolectar y explotar la información histórica de datos, mitigar ciberataques, configuración de aplicaciones TIC, denegación de permisos de acceso y control de ciberdefensa que abarque:

- Las infraestructuras críticas del país: administraciones, organismos e instituciones y empresas públicas o privadas consideradas como infraestructuras críticas del país.
- Las Fuerzas Militares.
- Los Cuerpos y Fuerzas de Seguridad del Estado (Secretaría General Técnica, Ministerio de Defensa, 2012).

f. Como sexta medida, se hace necesario realizar una doctrina de ciberdefensa para la Armada Nacional, donde se establezcan políticas amplias de ciberseguridad para la Armada Nacional, además donde se relacionen los procedimientos y directrices que guíen el uso apropiado de los medios informáticos que permitan a los encargados de tripular un centro de comando y control cibernético de la Armada Nacional, poner en práctica las técnicas de control y neutralización de posibles ataques cibernéticos. Asimismo, debe establecer unos principios fundamentales para regir la ciberdefensa, enmarcada en normas y leyes nacionales e internacionales.

CAPITULO IV

4.1 RECOMENDACIONES

4.1.1 Adquirir en la Armada Nacional de Colombia, los equipos informáticos apropiados para la implementación de las diferentes capacidades de defensa, tales como: la valoración dinámica del riesgo, gestión de los posibles riesgos y amenazas presentes en la red cibernética naval, capacidad de mantener actualizado el hardware y software, recuperación frente a ciberataques, capacidad para restaurar la integridad de los sistemas, de la misma forma unas capacidades de Inteligencia para clasificar malware, análisis de Códigos, intercambio de información de ciberdefensa con diferentes agencias y unas capacidades de respuesta para mitigar ciberataques, configuración de aplicaciones TIC, denegación de permisos de acceso, reubicación de los servicios de información, bloqueo de componentes y servicios y una defensa activa que en la Armada Española funcionan para ejercer medidas de control efectivas, con el fin de prevenir, contrarrestar y atacar posibles amenazas de intrusión a nuestras plataformas y redes institucionales. Por otra parte adquirir equipos informáticos para realizar diseños de configuraciones especializadas de manejo automático de las TIC, con códigos de encriptación sofisticada.

4.1.2 Implementar en la Armada Nacional de Colombia, un centro de comando y control cibernético, que integre los diferentes tipos de capacidades para la ciberdefensa que se utilizan en la Armada Española, donde personal especializado se mantenga identificando posibles amenazas en el ciberespacio que puedan afectar los sistemas y plataformas informáticas de la institución, a su vez que contrarresten posibles daños informáticos. Dichos expertos en ciberdefensa y ciberseguridad deben contar con un departamento de investigación, donde puedan diseñar y realizar simulación de ataques informáticos que complementen la protección de los sistemas de control.

4.1.3 Implementar la doctrina para la ciberdefensa y la ciberseguridad de la Armada Nacional con el fin de brindar lineamientos, instrucciones y enseñanzas al personal destinado a cumplir con el que se requiere se defina como un objetivo estratégico institucional. Es decir para el personal que se capacite para desempeñarse en el centro de comando y control cibernético de la Armada Nacional. Por otra parte una doctrina para

todos los miembros de la institución, que garantice el uso eficiente de los sistemas y minimice las amenazas a las que se exponen los sistemas en el ciberespacio.

4.1.4 Continuar fomentando con campañas y boletines la cultura institucional de la seguridad informática y la ciberseguridad en todos los miembros de la Armada Nacional, con el fin de crear hábitos informáticos para garantizar la protección y clasificación segura de la información que cada uno a su nivel tiene bajo su responsabilidad. Todo esto encaminado a minimizar la fuga de información e intrusión a nuestros archivos de información por desconocimiento o por omisión.

4.2 PROPUESTA DE INTERVENCION

Con el objetivo de minimizar las posibles amenazas que se evidencian en el ciberespacio y proteger la información sensible de las plataformas informáticas que la Armada Nacional de Colombia utiliza actualmente para el funcionamiento y control de personal, abastecimiento y dotación del personal y las unidades, mantenimiento de las unidades e instalaciones marítimas, fluviales y terrestres, control financiero, herramientas de planeación, etc, se hace necesario optimizar las medidas de acción de la ciberdefensa y la ciberseguridad en la Armada Nacional de Colombia, para lo cual se proponen las siguientes:

4.2.1. Poner en ejecución una estrategia de ciberdefensa basada en la misión y los roles que desarrolla la institución, que garantice ejercer un efectivo control del ciberespacio en la red cibernética naval (SILOG, SIATH, ZEUS, Portal Armada Nacional), donde se plantee una visión institucional enfocada a minimizar o evitar cualquier amenaza o intrusión a las redes de la Armada Nacional, sostenible en el tiempo, liderada por una jefatura institucional de cibernética, donde se planteen todas las tareas y hoja de ruta en lo concerniente a ciberdefensa y ciberseguridad para las próximas décadas. Dicha estrategia debe abarcar unas líneas de acción que contemplen la actualización constante de tecnología, capacitación de personal, políticas de protección de los sistemas, cultura informática institucional y alianzas con agencias internacionales dedicadas a esta misión, para garantizar se minimicen los posibles riesgos y amenazas mundiales.

De la misma forma, se debe plantear a la ciberdefensa al interior de la Armada nacional, como un objetivo estratégico institucional, para garantizar la dinámica operacional y de funcionamiento, con las capacidades y el conocimiento para contrarrestar la evolución acelerada tecnológica de las amenazas cibernéticas desde cualquier latitud del planeta.

4.2.2. La Armada Nacional debe crear un centro de comando y control cibernético que integre las capacidades y los sistemas disponibles de la institución, donde se tenga un control del ciberespacio en que trabajan las diferentes plataformas para la operación institucional, con las capacidades para detectar y contrarrestar una amenaza cibernética. Asimismo, donde se tenga la capacidad de enlace para compartir información y se pueda interactuar coordinadamente con otras agencias internacionales y con las diferentes entidades del Estado. Este Centro de Comando y control Cibernético debe contar con un departamento de investigación, donde permanentemente se estén identificando y actualizando las últimas técnicas y tendencias en el ámbito cibernético, con el fin de que los especialistas diseñen sistemas para proteger a la institución y a todos sus sistemas de un posible ataque cibernético o mejor aún que permita recuperar las capacidades de los sistemas en el menor tiempo posible.

4.2.3. El uso de las TIC's en el desarrollo de operaciones militares ha hecho que la cantidad de información que transita por las redes se incremente de manera exponencial y de esta misma forma ha facilitado el crecimiento de las amenazas; por lo que los gobiernos se han visto en la obligación de diseñar e implementar estrategias que conlleven al uso seguro de este tipo de tecnologías. Por ello, la Armada Nacional, debe elaborar su doctrina de ciberseguridad con medidas que abarquen todos los procedimientos requisito para contribuir a la protección de la red cibernética naval. Los procedimientos contenidos en la doctrina de ciberdefensa, deben ser obligatorios para todos los integrantes de la institución, encaminados a dar el uso apropiado al quinto dominio, en especial durante el planeamiento operacional y el desarrollo de tareas de campo. De esta forma, se canalizan lo conductos para el trámite de la información buscando minimizar fuga de información operacional y restringida.

4.2.4. Se requiere fortalecer las herramientas jurídicas para sancionar los delitos

informáticos, o mejor aún se hace necesario enmarcar como delito informático a toda acción que se considere violatoria de la seguridad informática, es decir acceder a plataformas y sistemas que son de carácter restringido institucional, al igual que los medios de uso personal. Esta debilidad se debe fortalecer desde el campo del Gobierno Nacional, ya que aunque en nuestro país se han tomado medidas penales con la comisión de este tipo de delitos, aún existen vacíos jurídicos para sancionar este tipo de faltas, para las cuales se hace necesario diseñar y establecer en la ley la solución a este problema.

BIBLIOGRAFÍA

Ley 1273 (Congreso de Colombia 05 de enero de 2009).

Acosta, N. (20 de 01 de 2010). *El economista*. Recuperado el 15 de 03 de 2015, de http://eleconomista.com.mx/tecnociencia/2010/01/20/operación-aurora-ciberataque-as-sofisticado-historia.

Aguilar, L. J. (2010). *Ciberseguridad, retos y amenazas.* Madrid: Imprenta Ministerio de defensa.

Almirante (Ra) Alvaro Echandia Durán. (2011). Planeamiento de la Fuerza 2030. *Plan de Desarrollo Armada Nacional*. bogota, Cundinamarca, Colombia.

Andress, J. (2011). *Ciberguerra, técnicas, tácticas y herramientas para profesionales de la seguridad.* Waltham: Elsevier.

ANGUERA, M. A. (1998). Métodos de investigación en sicologia. En M. ANGUERA. Sintesis.

Brochet, N. d. (2010). Ciberdelincuentes tras control de firmas. *Portafolio*.

CARLOS, T. d. (17 de marzo de 2015). Trabajo de Grado para optar al titulo de magister en seguridad y defensa. (C. J. Parra, Entrevistador)

Casabona, C. M. (2014). *De los delitos informaticos al cibercrimen.* Universidad de salamanca.

CEE, E. (2007). *Tarjeta Informatíva Núm. 150 del 18/09/07.* México, D.F.

Chin, Y. (2013). Desarrollo de la teoria de las relaciones internacionales en China. *Relaciones internacionales*, 67-84.

Colombia, A. N. (2007). Cerrando espacios al futuro. *escenarios operacionales*.

Colombia, F. M. (2004.). *Manual de Inteligencia de Combate.* Bogotá D.C.

Comisión Colombiana del oceano. (12 de septiembre de 2007). Politica Nacional del Oceano y los espacios costeros. *Politica Nacional del Oceano y los espacios costeros*. Bogotá, Cundinamarca, Colombia.

Corporation, T. M. (2015). *Reporte de Seguridad Cibernética e infraestructura critica de las Américas.* washington: Trend Micro Corporation.

Corredera, J. R. (marzo de 2012). El Ciberespacio nuevo escenario de confrontación. Madrid, España.

Cruz Ballado, J. (2007). CEE EDOMAY. Control Naval de Tráfico Marítimo. *Control Naval de Tráfico Marítimo.* México, D.F.: CEE EDOMAY.

diaz, T. J. (18 de 04 de 2015). Magister en Tecnologias para la Defensa. (C. J. Parra, Entrevistador)

Durán, A. A. (2011). Plan de desarrollo Armada Nacional de Colombia. *Planeamiento de Fuerza 2.030*. Colombia.

E. Fojón Chamorro, J. R. (2012). La Ciberseguridad Nacional, un compromiso de todos. Madrid.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. human factors.

Estado Mayor Naval, Semar. (1969). *Control y Pritección del Tráfico Marítimo.* México, D.F.: Semar.

estratégicos, I. e. (diciembre de 2010). Ciberseguridad, retos y amenazas a la seguridad nacional en el espacio. Madrid, España.

Eyssautier de la Mora, M. (2007). *Metodología de la Investigación. Desarrollo de la Inteligencia.* México, D.F.: Thomson.

F. Sánchez, A. M. (2003). CONFLICTO, VIOLENCIA Y ACTIVIDAD CRIMINAL EN COLOMBIA: UN ANALISIS ESPACIAL. *Universidad de los Andes*.

Fabra, U. P. (24 de 04 de 2010). *universitat pompeu fabra.* Recuperado el 23 de agosto de 2014, de http://www.upf.edu/estiu/_pdf/1421t1.pdf

Francés, D. C. (s.f.). Recuperado el mayo 2014, de http://www.ssi.gov.fr

Garcia, J. I. (2013). Los conflictos armados en la estrategia de seguridad nacional. *UNISCI Discussion papers*.

GIL, D. C. (2009). La seguridad frente artefactos explosivos. En C. d. superiores. Madrid.

Gonzalez, A. G. (2014). La colaboración cientifica. *Revista Española de Documentacion cientifica*.

Higuera, J. B. (2013). Introducción a la Ciberdefensa. Madrid: Fundación In-Nova Castilla La Mancha.

Inteligencia, M. d. (2010). *Fuerzas Armadas Españolas.* Madrid.

J. Suárez Vanegas. (2012). BACRIM Bandas Crminales. *Observatorio de D.I.H.*

Jiménez, E. (2011). Rigor científico en las prácticas de investigación cualitativa. *Ciencia, docencia y tecnología*.

Jimenez, M. (30 de noviembre de 2015). el negocio de la ciberseguridad se dispara ante las nuevas amenazas. *Diario cinco días*.

Johnson, R. (2007). *Estadística Elemental* (2007 ed.). México, D.F.: Editorial Trillas S.A. de C.V.

Leithauser, T. (22 de abril de 2013). Que es CISPA y que protege? *New York Times*.

Lopez, C. (2007). La guerra informática. *Boletín del centro naval*, 2,3.

Lucious Morton, Ejercito de los Estados Unidos de Norteamerica. (22 de febrero de 2010). Plan de capacidades en las operaciones del ciberespacio.

M. J. West-Brown, D. S.-P. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Pittsburgh: Carnegie Mellon University.

M.J.West-Brown, D. r. (2003). libreta para respuesta de incidentes de seguridad informática. Pittsburg: Carnegie Mellon University.

madrid, U. c. (2011). Estrategia española de sguridad. *Departamento de estudios*.

Martinez, A. (2011). *Concepto sobre seguridad nacional.*

Medero, G. S. (2008). Ciberguerra y ciberterrorismo ¿realidad o ficción? una nueva forma de guerra asimetrica. *LAS FF.AA. EN LOS CONFLICTOS ASIMÉTRICOS Y EN LAS OPERACIONES DE ESTABILIZACIÓN.*

Medero, G. S. (noviembre de 2012). *la ciberguerra: los casos de stuxnet y anonymous.* Recuperado el 12 de julio de 2014, de www.stuxnet

Medero, G. s. (2012). Los casos cibernéticos: stuxnet y anonymous. *Nueva época*, 10.

Medina, C. d. (20 de 05 de 2015). Trabajo de grado. (C. d. Posada, Entrevistador)

México- USA- Cánada. (2005). *"Alianza para la Seguridad y Prosperidadde América del Norte".* Waco, Tx.: México, USA, Cánada.

Meyerrose. (2010). Gm of cyber integrated solutions. *In 4th annual Homeland Security.*

Micro, T. (2.015). *REPORTE DE SEGURIDAD CIBERNÉTICA E INFRAESTRUCTURA CRÍTICA DE LAS AMÉRICAS.*

Ministerio de Defensa Nacional. (19 de 06 de 2014). Politicas de seguridad de la información para el sector defensa. *Directiva Permanente*. Bogotá, Cundinamarca, Colombia: MINDEFENSA.

Monroe, F. (2010). Operaciones en el Ciberespacio. *Ejercito de los Estados Unidos de Norteamerica*.

Monroe, F. (2010). *Operaciones en el ciberespacio, plan de capacidades 2.016-2.028.* Estados Unidos de América.

Monroe, F. (2014). Ejercito de los Estados Unidos de Norteamerica. Operaciones en el ciberespacio. *PLan de capacidades 2016-2018*.

MONTERO, L. Y. (1997). *diseños de Investigación.* México: Mc Graw Hill.

Moraga, A. L. (2006). historia e internet: aproximación al futuro de la labor investigadora. *Universidad complutense de madrid*, 1.

Nájar, C. D. (2012). la Ciberguerra en el quinto dominio. *Fuerzas Militares*.

Niño, A. (2013). El quinto dominio de la guerra. *Estudios en seguridad y defensa*.

Notario, E. (16 de 05 de 2013). Grandes robos informaticos de la historia. *diario turing*.

Nye, K. (2013). *Ciberespacio para Ciberdefensa.*

OMI. (30 de abril de 2008). *http://www.imo.org.* Recuperado el 2008, de http://www.imo.org/TCD/mainframe.asp?topic_id=415:

Pacheco, H. J. (2012). Ethical Hacking 2.0. *Red Users*.

Pelaez, L. d. (2015). La defensa de zuluzga a luis alfonso hoyos. *semana*.

Planeación, D. N. (2011). *Documento Conpes 3701. Lineamientos de politica para ciberseguridad y ciberdefensa.* Bogota.

R. A. Clarke y R. K. Knake, A. (2011). Los nuevos campos de batalla. *Guerra en la red.*

Ramón, J. G. (2002). El orden de la guerra: las FARC-EP, entre la organización y la política. *Pontificia Universidad Javeriana.*

Ruiz, T. d. (18 de mayo de 2015). Entrevista trabajo de grado . (C. d. Parra, Entrevistador)

Saade, C. (7 de septiembre de 2002). *Renuncia México al TIAR por considerarlo "obsoleto".* Recuperado el 23 de febrero de 2008, de www.jornada.unam.mx:

Sampieri, R. H. (1998). *Metodología de la Investigación.* México, D.F.: McGraw-Hill.

Saynez, M. (2007). *Programa Sectorial de Marina 2007-2012.* México, D.F.: Semar.

SCT- Semar. (2007). *Lineamientos Generales del CUMAR.* México, D.F.: Acuerdo de Colaboración SCT-SEMAR del 3 de agosto de 2007.

Secretaría General Técnica, Ministerio de Defensa. (12 de 05 de 2012). El Ciberespacio.

Nuevo escenario de confrontación. *El Ciberespacio. Nuevo escenario de confrontación.* Madrid, Madrid, España: Centro Superior de Estudios de la Defensa Nacional.

Spade, J. M. (2.012). *Ciberpotencia China y la seguridad Nacional de Estados Unidos.* pensilvania: us army war college.

Stel, E. (2014). *Seguridad y defensa del ciberespacio.* Buenos Aires: Dunken.

Tahajian, L. (18 de noviembre de 2013). Cispa is back. *University Wire [Carlsbad].*

Técnica, M. d. (2012). El ciberespacio, nuevo escenario de confrontación. *Centro Superior de Estudios de Defensa Nacional.* Madrid.

Velez, O. R. (2004). *Los caminos a la delincuencia: posibilidades para su prevención.* Bogota: Pontificia universidad javeriana.

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine.* Cambridge: Mit press.

Zorrilla Arena, S. (2005). *"Guia para elaborar la Tesis".* México, D.F.: Mcgraw-Hill.

ANEXOS

ANEXO 1

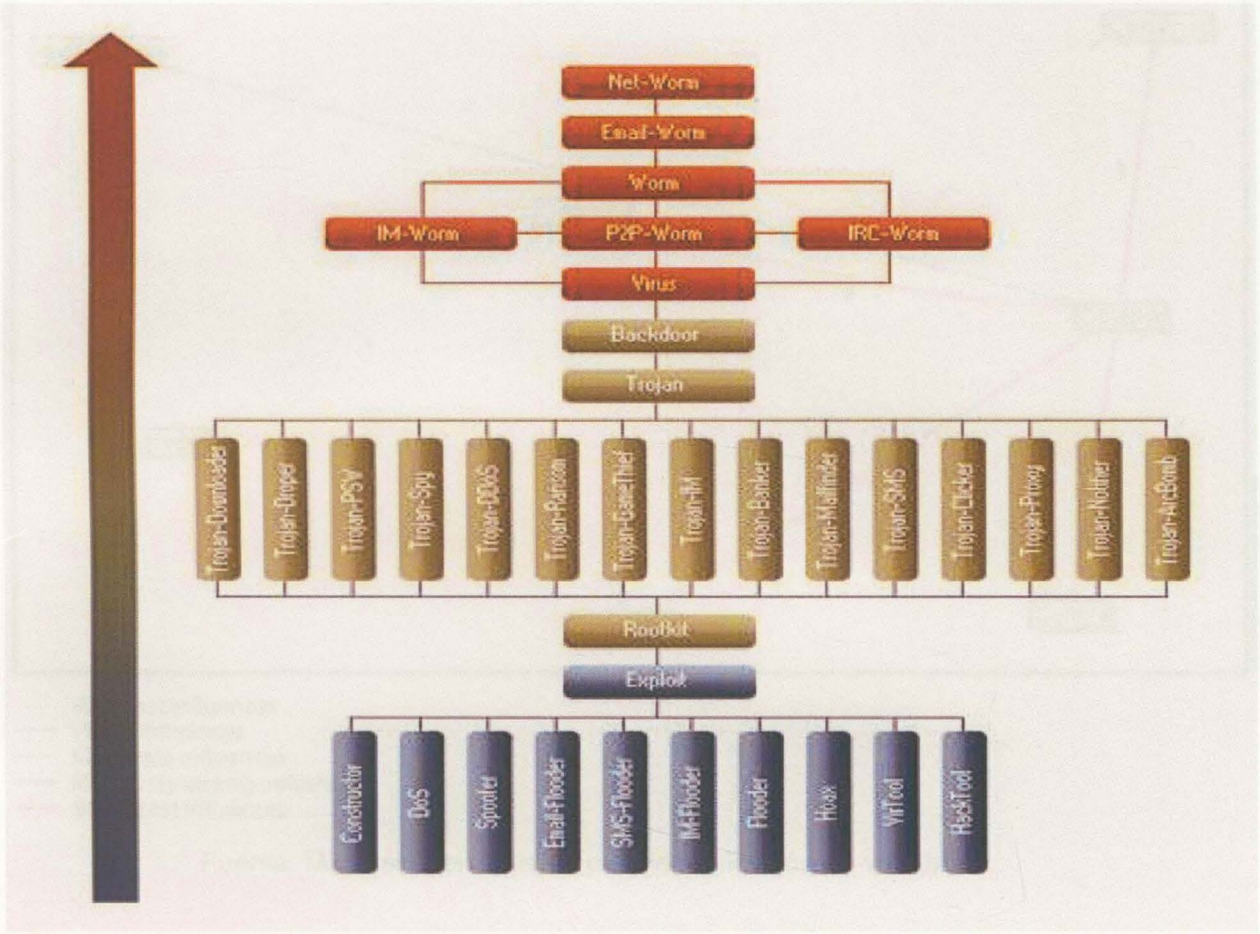
Tabla 1. Entrevistas de expertos seleccionados en el tema.

	Nombre del Profesional	*Especialidad*
1.	CN Gladys Medina	Directora de Telemática de la Base Naval ARC "Bolívar".
2.	TN Juan Laserna	Ingeniero de Sistemas – Subdirector Telemática de la Base Naval ARC "Bolívar".
3.	TN Julián Aponte Díaz	Oficial del Departamento de Armas y Electrónica Base Naval ARC "Bolívar".
4.	TF Héctor García	División de Informática de la Armada Nacional.

Fuente: Elaborado por los autores a partir del muestreo.

ANEXO 2

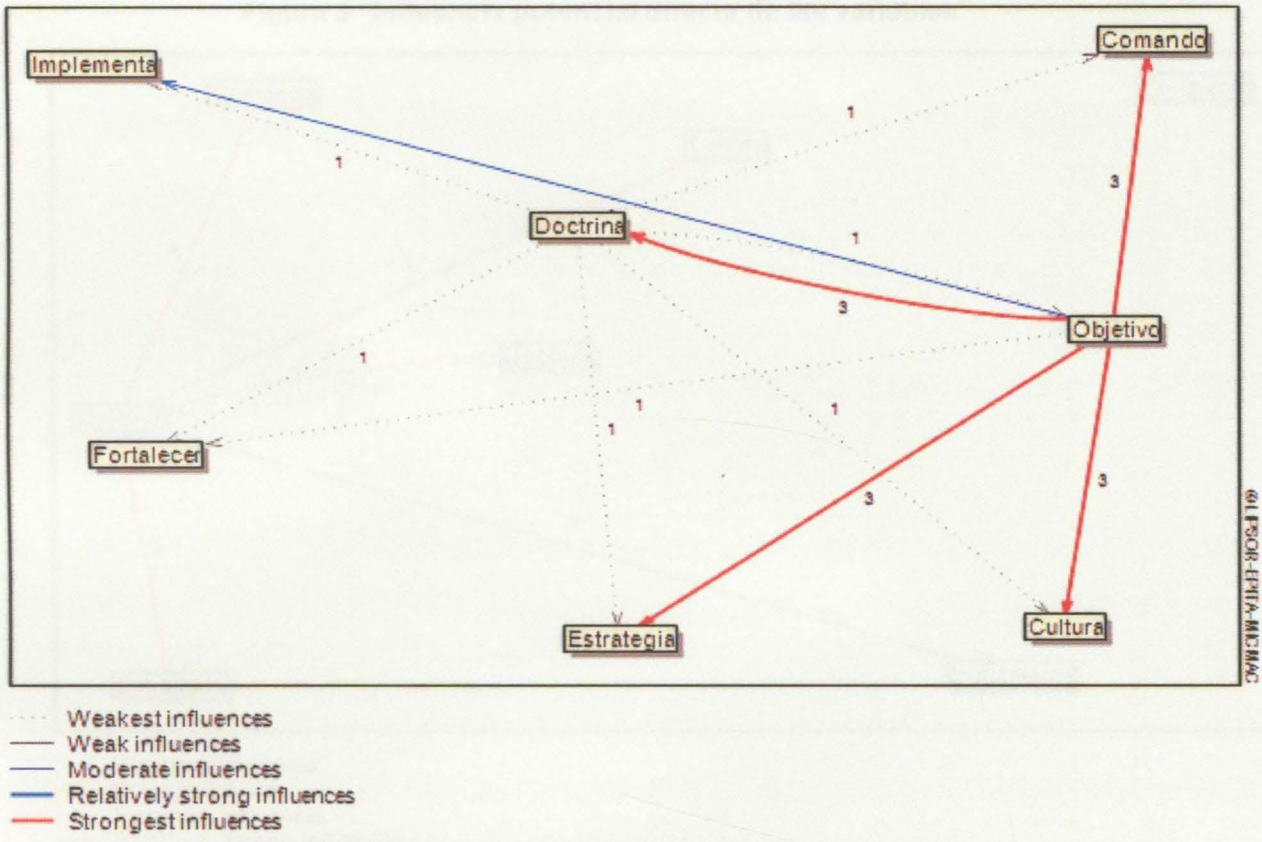
Figura 1. Árbol de clasificación de malware



"Árbol de clasificación de Malware". Tomada de http://www.kaspersky.es/internet-security-center/threats/malware-classifications.

ANEXO 3

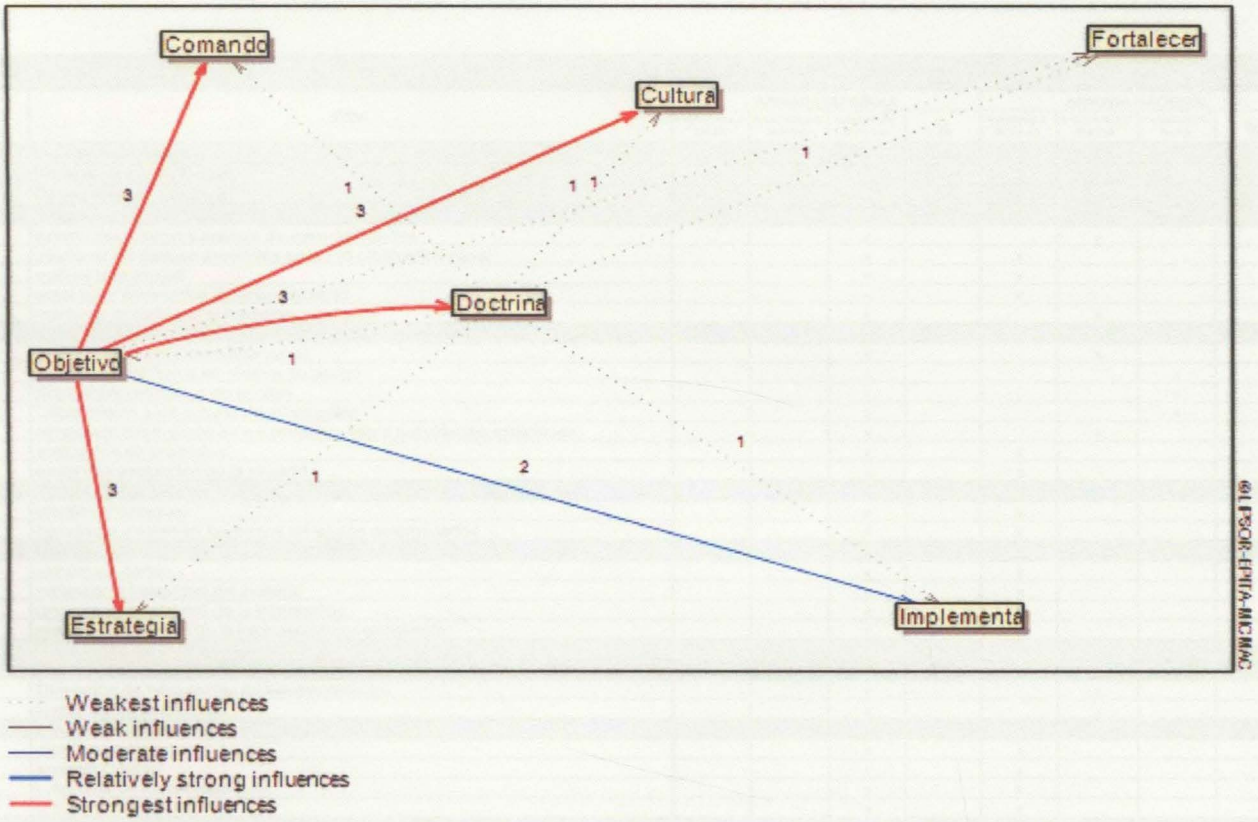
Figura 2 "Influencia directa de las variables"



Fuente: Mic Mac "herramienta para identificación de variables"

ANEXO 4

Figura 3 "Influencia potencial directa de las variables"



Fuente: Mic Mac "herramienta para identificación de variables"

ANEXO 5

Tabla 2: Comparativo de medidas aplicadas por la Armada Española y la Armada Nacional de Colombia.

TABLA COMPARATIVA DE MEDIDAS EN ARMADA ESPAÑOLA VS ARMADA NACIONAL DE COLOMBIA									
No.	ITEM	ARMADA ESPAÑOLA				ARMADA NACIONAL			
		PRIORIDAD BAJA	PRIORIDAD MEDIA	PRIORIDAD ALTA	%	PRIORIDAD BAJA	PRIORIDAD MEDIA	PRIORIDAD ALTA	%
1	**Objetivo estratégico**			x	100%		x		50%
2	**Fortalecer capacidades**			x	100%	x			20%
3	**Capacidad de defensa**				100%				40%
a	**Valoración dinámica del riesgo**				100%				70%
	estado del sistema y análisis de vulnerabilidades			x			x		
	gestionar los riesgos presentes en la red cibernética naval			x		x			
	evaluar la amenaza			x		x			
	establecer escenarios de entrenamiento			x		x			
	mantener actualizado el hardware y software			x			x		
b	**Detección y análisis de ataques cibernéticos y actividades maliciosas**				100%				50%
	monitorizar la red cibernética naval			x			x		
	Revisión periódica a los niveles de riesgo			x				x	
	Supervisión periódica de acceso			x				x	
	Clasificación a los activos de información			x				x	
	almacenar información de los sensores sobre actividades maliciosas			x			x		
	evaluación de entidades			x		x			
	emitir una evaluación de la situación			x		x			
c	**Toma de decisiones en tiempo oportuno**				100%				20%
	identificar opciones			x		x			
	comunicar y controlar los cursos de acción determinados			x		x			
d	**Recuperación frente a ciberataques**				100%				20%
	valorar los daños			x		x			
	restaurar la integridad del sistema			x		x			
	restaurar la integridad de la información			x		x			
	realizar trazabilidad de la información comprometida			x		x			
4	**Capacidad de Inteligencia**				100%				40%
a	**Obtención de Información**				100%				40%
	Obtención de Información de fuentes abiertas			x			x		
	Sistemas de Decepción			x			x		
b	**Análisis de Malware**								
	clasificar malware			x		x			
	analizar Código			x		x			
	i. Análisis de comportamiento			x		x			
	ii. Estudio del código			x		x			
c	**Intercambio de Información de Ciberdefensa**				100%				50%
	compartir información de ciberdefensa de forma eficiente			x			x		
	garantizar la capacidad de la información de ciberdefensa			x		x			
	recolectar y explotar el histórico de datos			x			x		
5	**Capacidad de respuesta**				100%				30%
a	**mitigar Ciberataques**				100%				30%
	a. Configuración de aplicaciones TIC			x			x		
	b. Denegación de permisos de acceso			x			x		
	c. Reconfiguración de la topología de los sistemas			x					
	i. Reubicación de los servicios de información			x		x			
	ii. Aislamiento de sistemas			x		x			
	iii. Bloqueo de componentes y servicios			x		x			
	iv. Control del flujo de tráfico			x		x			
	v. Coordinación de la respuesta externa			x		x			
	d. Defensa Activa			x			x		
	i. Centro de comando y control cibernético			x		x			
	Unidad cibernética naval			x				x	
	ii. Definición de Infraestructuras Criticas			x			x		
	iii. Auditorias de seguridad a las redes cibernéticas			x			x		
6	**Implementar nuevas capacidades**			x	100%		x		40%
7	**Estrategia de Ciberdefensa**			x	100%	x			20%
a	Cultura de Ciberseguridad			x		x			20%
b	Red cibernética naval			x			x		60%
c	Personal capacitado			x		x			20%
8	**Doctrina de Ciberdefensa y ciberseguridad**				100%				90%
	Impartir politicas y directrices institucionales			x				x	
	PORCENTAJE TOTAL	**100%**				**41%**			

ANEXO 6

Entrevista trabajo de grado Ciberdefensa y ciberseguridad.

Nombre y cargo del encuestado:

TN JULIAN DAVID APONTE DIAZ. Master en Tecnologías para la Defensa.

Orgánico del Departamento de Armas y Electrónica de la Base Naval ARC "Bolívar".

a. ¿Por qué es importante para la Armada Nacional de Colombia, garantizar la seguridad del ciberespacio en que opera la institución?
   RTA: Porque hoy en día nos encontramos en una era tecnológica, donde toda la información y los datos viajan a través del ciberespacio, aumentando la vulnerabilidad y fuga de información en el desarrollo de las tareas y operaciones propias de la institución.
   Pregunta complementaria:
   a. ¿Qué impacto estratégico tiene para la Armada Nacional,ejercer un mayor control en el ciberespacio?
      RTA: Optimizar las operaciones encaminadas a ejercer un adecuado control contra el narcotráfico, con el fin de continuar manteniendo la buena imagen institucional ante los colombianos, asimismo, favorecer el cumplimiento de la misión constitucional en la protección de los intereses de los colombianos.

b. ¿Qué acciones en ciberdefensa y cuales en ciberseguridad, considera usted que debería aplicar la Armada Nacional?
   RTA:
   La Armada Nacional debe contar una Jefatura de Ciberdefensa Naval con personal dedicado a implementar y garantizar que se cumplan con las últimas técnicas y se cuente con las mejores tecnologías en Cibernética para contar con las siguientes **Capacidades de defensa**:
   a. Capacidades que permitan realizar una valoración dinámica de los riesgos, para:
      i. Mantener actualizada la situación del estado del sistema y análisis de vulnerabilidades.
      ii. Gestionar los riesgos presentes en la red cibernética naval.
      iii. Evaluar la amenaza.
      iv. establecer escenarios de entrenamiento.
      v. Mantener actualizado el hardware y software.
   b. Capacidad de detección y análisis de ataques cibernéticos y actividades maliciosas, para:
      i. Monitorizar la red cibernética naval.

ii. Almacenar y procesar la información recopilada por los sensores sobre actividades maliciosas o ataques contra la red cibernética naval.
iii. Detectar y analizar actividades maliciosas dentro de la red cibernética naval.
iv. Emitir una evaluación de la situación.

c. Capacidad de toma de decisiones en tiempo oportuno, para:
   i. identificar opciones.
   ii. comunicar y controlar los cursos de acción determinados.

d. Capacidad de recuperación frente a ciberataques, para:
   i. Valorar los daños
   ii. Restaurar la integridad del sistema
   iii. Restaurar la integridad de la información
   iv. Realizar trazabilidad de la información comprometida

Capacidades de inteligencia:

1) Obtención de Información.
2) Análisis de Malware, para:
   i. Clasificar Malware.
   ii. Analizar código.
3) Intercambio de información de ciberdefensa, para:
   i. Compartir información de ciberdefensa de forma eficiente.
   ii. Garantizar la capacidad de la información de ciberdefensa.
   iii. Recolectar y explotar el histórico de datos.

Capacidades de Respuesta:

1) Capacidad para mitigar ciberataques, que permitan:
   i. Configuración de aplicaciones TIC.
   ii. Denegación de permisos de acceso.
   iii. Reconfiguración de la topología de los sistemas.
   iv. Coordinación de la respuesta externa.

c. ¿Cómo puede la Armada Nacional fortalecer su vinculación con la Comunidad cibernética Internacional, orientada al control del ciberespacio?

Implementando un comando Cibernético naval, que se encargue de administrar las capacidades de defensa, en cuanto al ciberespacio se refiere, de la Armada Nacional de la República de Colombia y cumpliendo los estándares exigidos por la comunidad internacional. De la misma forma, debe diseñarse un Laboratorio de Ciberseguridad y Ciberdefensa, destinado a liderar todas las investigaciones que se requieran para tener un estado de conciencia situacional actualizado en base al material recopilado de ataques o intentos de intrusión; así como todos aquellos proyectos que conlleven al desarrollo y mejoramiento de herramientas que puedan ser utilizadas en operaciones de ciberseguridad y de ciberdefensa.

d. ¿Considera necesaria la implementación de una Doctrina para el Control del Ciberespacio en la Armada Nacional de Colombia?

En la Armada Nacional se deben establecer y diseñar dos tipos de doctrina, una de ciberseguridad orientada abrindar lineamientos, instrucciones y enseñanzas al personal destinado a garantizar la seguridad de la red cibernética naval y de las utilizadas por las infraestructuras críticas y otra de ciberdefensa orientada hacia el personal encargado de detectar, identificar y neutralizar las amenazas que se encuentren presentes en el ciberespacio, dentro de las áreas de responsabilidad asignadas a la Institución.

Entrevista trabajo de grado Ciberdefensa y ciberseguridad.

Capitán de Navío GLADYS MEDINA

Jefe Departamento de Telemática Base Naval ARC "Bolívar"

a. ¿Por qué es importante para la Armada Nacional de Colombia, garantizar la seguridad del ciberespacio en que opera la institución?
RTA:
El ciberespacio es considerado como un nuevo escenario de conflicto que podría evolucionar a una ciberguerra.

Pregunta complementaria:
1) ¿Qué impacto estratégico tiene para la Armada Nacional, ejercer un mayor control en el ciberespacio?
RTA:
De protección, de estar alerta y principalmente de estar preparados, no solo como armada, si no integrados a la totalidad del sistema, ya que un ataque de un punto cercado (otra fuerza o infraestructura crítica) nos puede afectar.

b. ¿Qué acciones en ciberdefensa y cuales en ciberseguridad, considera usted que debería aplicar la Armada Nacional?
RTA:
Para un buen sistema de ciberdefensa y ciberseguridad, debe contar con el conocimiento de los ataques actuales, es la base para construir una defensa práctica y efectiva. Priorizar controles para reducción de riesgos y amenazas, monitoreos continuos y automatización de las defensas.

c. ¿Cómo puede la Armada Nacional fortalecer su vinculación con la Comunidad cibernética Internacional, orientada al control del ciberespacio?
RTA:
Como Armada debemos trabajar unidos en una política centralizada no aislada a través del CSIRT Colombiano. Lo obliga generar una Ley de ciberseguridad y defensa con los lineamientos del conpes 3701, genera una estrategia nacional, la definición de infraestructuras críticas y la estrategia militar de ciberdefensa.

d. ¿Considera necesaria la implementación de una Doctrina para el Control del Ciberespacio en la Armada Nacional de Colombia?
RTA:
Claro, después de lograr los anteriores puntos toca generar una doctrina militar en ciberseguridad y unas operaciones en el ciberespacio, continuar en el C4ISR y una formación académica adecuada con estos temas.

Entrevista trabajo de grado Ciberdefensa y ciberseguridad.

Teniente de Navío JUAN LASERNA

Subdirector Departamento de Telemática Base Naval ARC "Bolívar"

a. ¿Por qué es importante para la Armada Nacional de Colombia, garantizar la seguridad del ciberespacio en que opera la institución?
RTA:
Con el fin de proteger todo lo relacionado con las comunicaciones, por seguridad nacional.

Pregunta complementaria:

1. ¿Qué impacto estratégico tiene para la Armada Nacional, ejercer un mayor control en el ciberespacio?
RTA:
Si se ejerce un control del ciberespacio, la ARC puede tener gran participación, enfatizando su centro en el campo de ciberseguridad.

b. ¿Qué acciones en ciberdefensa y cuales en ciberseguridad, considera usted que debería aplicar la Armada Nacional?
RTA:
- *Ciberdefensa: Control aéreo, terrestre y marítimo, control en tiempo real.*
- *Ciberseguridad: Control de las acciones informáticas eticalhacking, penetración para mayor control.*

c. ¿Cómo puede la Armada Nacional fortalecer su vinculación con la Comunidad cibernética Internacional, orientada al control del ciberespacio?
RTA:
Alianzas con las potencias mundiales, desarrollando las mejores prácticas en pro de las CNT.

d. ¿Considera necesaria la implementación de una Doctrina para el Control del Ciberespacio en la Armada Nacional de Colombia?
RTA:
Se debe primero empezar por la cabeza, al definir al definir al nivel presidencial, ministerio, fuerzas, tarea que no es fácil, visto, no es algo que es estrictamente único de la ARC.

Entrevista trabajo de grado Ciberdefensa y ciberseguridad.

Teniente de Fragata GARCÍA RUIZ JUAN CARLOS

División de Informática Armada Nacional

a. ¿Por qué es importante para la Armada Nacional de Colombia, garantizar la seguridad del ciberespacio en que opera la institución?
RTA: Porque hoy en día nos encontramos en una era tecnológica, donde toda la información y los datos viajan a través del ciberespacio, aumentando la vulnerabilidad y fuga de información en el desarrollo de las tareas y operaciones propias de la institución.

Pregunta complementaria:
1) ¿Qué impacto estratégico tiene para la Armada Nacional,ejercer un mayor control en el ciberespacio?
RTA: Optimizar las operaciones encaminadas a ejercer un adecuado control contra el narcotráfico, con el fin de continuar manteniendo la buena imagen institucional ante los colombianos, asimismo, favorecer el cumplimiento de la misión constitucional en la protección de los intereses de los colombianos.

b. ¿En el caso dela Armada Nacional, qué limitaciones (de tipo jurídico, económico, político, de legislación internacional, etc.) considera usted impactan en la implementación de medidas de acción para la obtención de un efectivo control del ciberespacio? La Armada Nacional desde el año 2.014, implementó la unidad cibernética, dependencia que funciona en la Jefatura de Inteligencia Naval, donde se realizan tareas de ciberseguridad, sin embargo el presupuesto es limitado para ampliar sus capacidades en material y personal, debido a que no se cuenta ni en la institución ni en Colombia con jueces especializados en temas de ciberdefensa y/o de ciberseguridad, a pesar de que desde el nacimiento del conpes 3701 se ha marcado un derrotero para iniciar un largo camino de crecimiento y de fortalecimiento, esto aún va por la mitad.

c. ¿Considera usted que son adecuadas las medidas de control del ciberespacio que utiliza la Armada Nacional de Colombia?
No, son insuficientes.
Pregunta complementaria:
1) ¿Considera usted, Qué la Armada Nacional cuenta con los medios suficientes de ciberdefensa y las medidas de acción necesarias para ejercer un efectivo control del ciberespacio? No, estamos iniciando pero vamos por buen camino.

d. ¿Qué acciones en ciberdefensa y cuales en ciberseguridad, considera usted se deberían aplicar en el ciberespacio en que opera la Armada Nacional?
En ciberseguridad se cuentas con los equipos con el fin de proteger interna y externamente a nuestros usuarios, pero falta un poco más de personal, en

ciberdefensa se han adquirido herramientas y están en la fase de capacitación del personal para sacarle un mejor provecho a los mismos

e. ¿Cómo puede la Armada Nacional fortalecer su vinculación con la Comunidad cibernética Internacional, orientada al control del ciberespacio?
Por medio del comando conjunto Cibernético y cumpliendo los estándares exigidos por la comunidad internacional.

f. ¿Considera necesaria la implementación de una Doctrina para el Control del Ciberespacio en la Armada Nacional de Colombia?
Si claro esto nos blindaría para poder actuar con mayor confianza en el ciberespacio.

g. ¿Considera usted que la Armada Nacional de Colombia, debe contar con un comando de ciberseguridad y ciberdefensa?
Si y debería depender de la Jefatura de Operaciones Navales o del Segundo Comando de la Armada, en este momento depende de la Jefatura de Inteligencia Naval que tiene sus ventajas, debido a que las operaciones son reservadas y se rigen por la ley de inteligencia.