ANÁLISIS DE CAPACIDADES CIBERNÉTICAS DE LA ARMADA DE COLOMBIA. [1]

Capitán de Corbeta Diego Fernando Cruz Sáenz[2]

Escuela Superior de Guerra General "Rafael Reyes Prieto"

1. Resumen

En la actualidad las operaciones ciberespaciales juegan un papel importante en el desarrollo de las operaciones militares, ya que con su empleo tienen el propósito principal de lograr objetivos en o a través del ciberespacio. La Armada Nacional en el desarrollo de operaciones, no puede ser ajena a la actualización de sus sistemas para el uso adecuado de este medio, es por esto que se quiere abordar desde una perspectiva marítima y de control del mar en este este campo.

Así las cosas, el ciberespacio, como parte de un entorno virtual, depende de los dominios físicos del aire, la tierra, el mar y el espacio (CJCS, 2018). Teniendo en cuenta esto se puede abordar el entorno físico, desde el ámbito cibernético, y es aquí donde el campo de acción del ciberespacio la ciberseguridad y ciberdefensa entra~~n~~ a jugar un papel preponderante en las operaciones militares, enfocadas principalmente en el entorno marítimo.

[1] El presente capitulo de libro es presentado como opción de grado para optar al título de Magister en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de Investigación titulado "Análisis de capacidades cibernéticas de la Armada de Colombia.".

[2] Estudiante que optará por el título de Magister en Ciberseguridad y Ciberdefensa. Especialista en Política y Estrategia Marítima, Profesional en Oceanografia Fisica y Ciencias Navales de la Escuela Naval "Almirante Padilla", Colombia. Contacto:diegofdocruz@gmail.com

Se puede diferir que en el desarrollo de esta investigación se va a recopilar información de fuentes primarias y secundarias, buscando como el desarrollo de tecnologías han influenciado el desarrollo de las operaciones navales marítimas en Colombia; teniendo en cuenta lo anterior, podemos decir, que se da origen a un quinto dominio, donde la Armada Nacional debe incursionar para el uso adecuado de este campo, es por esto que se puede enmarcar dentro de un método cualitativo, así también, como descriptivo.

Teniendo en cuenta lo anterior, en Colombia las Fuerzas Militares requieren abordar el ciberespacio como un ámbito estratégico, operativo y táctico, para organizar, entrenar y equipar a sus hombres, con el fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permitan fortalecer las capacidades en el ciberespacio ~~de Ciberdefensa~~, para enfrentar las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país, así como causar daños masivos, debilitar la economía, y/o dañar la moral pública y la confianza (Realpe y Cano, 2020) .

Dentro del desarrollo de estas operaciones militares, la intención es abordar las capacidades de la Armada Nacional para focalizar los alcances de las operaciones, desde un ámbito de operaciones ciberespaciales en el espectro de todas las operaciones militares.

2. Introducción

En los últimos años el entorno cibernético ha permitido la globalización mundial, la interconexión, el internet de las cosas, la sistematización de la catalanidad ha creado una dependencia de la humanidad que ha evolucionado en una necesidad. La interacción a través del ciberespacio, si bien ha permitido que mejoren muchos procesos, de igual forma genera un aumento en las vulnerabilidades, poniendo en riesgo la defensa y seguridad de los Estados (Sampaio, 2001).

Así las cosas, el desarrollo de tecnologías, el volcamiento a la utilización de los medios cibernéticos, maximizados por la aparición del COVID 19, el cual apalanco exponencialmente el uso de los ambientes cibernéticos, causando en la población mundial la dependencia acentuada a las tecnologías y al uso de las mismas, aportando de manera significativa al desarrollo de las capacidades y la adaptación de los medios cibernéticos. Entonces, es preciso cuestionarse si realmente la población estaba lista para la utilización de forma segura de estos medios, centrado en un entorno local el Estado colombiano y sus campos de acción se encontraban listos para afrontar los desafíos propios de la pandemia.

Se puede observar en los efectos de la pandemia, donde el coronavirus también ha tenido un impacto negativo en términos de ciberseguridad en el país. Según las cifras más recientes del Centro Cibernético de la Policía Nacional, los delitos informáticos aumentaron un 59% en el primer semestre, respecto al mismo periodo del año pasado, debido a que la

pandemia impulsó en los colombianos el uso de las operaciones digitales (Revista Portafolio, 2020).

Los crímenes en el ciberespacio, como se ha demostrado han aumentado, producto del incremento de la utilización de este medio, es por esto que las estructuras críticas del Estado se ven vulneradas, desde las entidades financieras, sistema de salud, entes gubernamentales, en razon, a que estos ataques se pueden realizar por actores estatales o no estatales, lo que conlleva a el debilitamiento de la estructura estatal, creando nuevos campos que sean trasversales en la gobernanza del país.

Esto demuestra como los intereses de los Estados pueden verse amenazados por medio de la interacción en el ciberespacio; a través de este, se pueden llevar a cabo desde crímenes cibernéticos a la sociedad en general, hasta ataques cibernéticos a los Estados, los cuales se convierten en un medio o recurso que pueden ser empleados directamente por parte de actores estatales o no estatales (Gómez, 2017).

Teniendo en cuenta lo anterior, concentrémonos en el siguiente escrito, el dominio del mar, ya que el ciberespacio es transversal a todos los dominios del Estado, se recalcara la importancia de la Armada Nacional, en el desarrollo de tecnologías, en el control de este ciberespacio y en el uso para adquirir una ventaja en el uso del mismo, la implementación de diferentes recursos cibernéticos para incrementar la ciberseguridad y la ciberdefensa, así como el aporte para la protección de estructuras críticas para el Estado, esto teniendo en

cuenta la necesidad de estar a la vanguardia en el desarrollo e implementación de un campo que está en constante evolución.

Mirando el ciberespacio como un quinto dominio, el cual influye drásticamente en el dominio marítimo y por ende en el desarrollo de las operaciones de la Armada Nacional, en el desarrollo de esta investigación, se utilizaran métodos cualitativos, como también, descriptivos, donde se analizara de manera exploratoria el diagnostico general del estado en materia cibernética de la Armada Nacional y aportara una visión de la proyección de la misma a un futuro cercano, haciendo una aproximación al fin deseado en un entorno en constante evolución.

Entonces en ese mismo entorno, el cual está en constante evolución, llevo al desarrollo de normas que de alguna u otra forma alinearan a países aliados en el control del quinto dominio, dando origen al Manual de Tallin, el cual dicta una normativa aplicada con diferentes tratados, leyes o simplemente al Derecho consuetudinario, extrayendo todo lo que fuese aplicable a la ciberguerra, este manual sirvió como referencia para la creación del CONPES 3854 de 2016, donde se crea la política de seguridad digital, dándole relevancia a la protección de los intereses del Estado, plasmado en aquellas infraestructuras críticas que pueden llegar a vulnerar la integridad, el bienestar, la salud, la economía o los recursos naturales de un Estado y sus pobladores.

En el CONPES 3854/2016, se define la infraestructura critica cibernética nacional como: aquella soportada por las tecnologías de la información y las comunicaciones y por

las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública (p. 29). Como por ejemplo, en relación bienestar de los ciudadanos, se vería afectado el libre flujo de información, como, asimismo, la confidencialidad de la información y las comunicaciones, entre otros, consagrados en la Constitución de 1.991; con respecto al eficaz funcionamiento de organizaciones y con el objeto de que exista una eficaz prestación del servicio, y que no se vea afectado se deberá promover la seguridad digital tanto del estado como de los ciudadanos, en el mismo sentido, se debe aumentar la capacidad de resiliencia nacional frente a amenazas y eventos no deseados digitalmente, para lo cual se deberá también, solicitar la máxima colaboración entre las múltiples partes interesadas.

El Ministerio de Defensa Nacional en concordancia a la protección de las Infraestructuras Criticas estableció el Plan Nacional de Protección y Defensa de Infraestructura Crítica Cibernética (2017) donde crea directrices, de cumplimiento en todos los actores que involucran medios cibernéticos de vital importancia para el País, dándole relevancia a los conceptos de ciberseguridad y ciberdefensa, donde es pertinente aclararlos.

La ciberseguridad se define como el "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio" (Cárdenas , 2015, p. 1) y la

ciberdefensa se presenta, como el conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición (Cárdenas, 2015), estos dos conceptos, son la aproximación al fin deseado por parte del Ministerio de Defensa Nacional, para la vinculación de los actores del ciberespacio.

Por ende, la Armada Nacional, como estructura ~~miembro~~ del Ministerio de Defensa Nacional está en la obligación del cumplimiento de las directrices que este emana, vinculándose de manera permanente y de forma prioritaria en la protección de la Infraestructura Critica del Estado, desarrollando actividades de ciberinteligencia o ciberdusacion como parte fundamental del desarrollo de operaciones militares en pro a los intereses propios de la Nación.

En este capítulo, se busca de esta forma, encontrar esas capacidades propias de la Armada Nacional, comprometida, vinculada al desarrollo del Estado colombiano aportando de manera significativa en la evolución constante, soportando las necesidades de un mundo cambiante, pues dispone de una infraestructura naval de gran estrategia, por medio de la cual, puede llevar a cabo operaciones militares de defensa en pro de la nación, en la búsqueda, el rescate, en las ayudas humanitarias, en el control del espacio en mares y océanos colombianos, enfrentando el crimen transnacional a la delincuencia organizada en delitos como, la piratería el robo a embarcaciones en altamar, narcotráfico, contrabando, migración ilegal, pesca depredadora, etc.

La Armada Nacional, ha conseguido avances en materia de ciberseguridad, disponiendo del Centro de Operación de Seguridad (SOC) y de un Sistema de Información de Gestión de Eventos (SIEM), fortaleciendo de esta forma, su capacidad de respuesta ante los delitos o posibles amenazas de origen cibernético, poniendo a disposición, no solo su capacidad humana, sino también, la infraestructura, la organización, el material necesario, que le permiten establecer una defensa eficaz en favor del Estado.

3. Metodología

Se puede diferir que en el desarrollo de esta investigación se va a recopilar información de fuentes primarias y secundarias, buscando cómo el desarrollo de tecnologías han influenciado el desarrollo de las operaciones navales ~~marítimas~~ en Colombia, teniendo en cuenta lo anterior, podemos decir, que se da origen a un quinto dominio, donde la Armada Nacional debe incursionar para el uso adecuado de este campo, es por esto que se puede enmarar dentro de un método cualitativo así también como descriptivo.

> "el cual implica organizar los datos recogidos, transcribirlos cuando resulta necesario y codificarlos. La codificación tiene dos planos o niveles. Del primero, se generan unidades de significado y categorías. Del segundo, emergen temas y relaciones entre conceptos". (Hernández, R., Fernández, C., y Baptista, (2014).

Es asi como se define el ciberesapacio como un dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de tecnología de la información y datos residentes, incluidos Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados. (CJCS, 2018)

La Armada Nacional ejerce presencia y soberanía sobre el Mar Caribe y el Océano Pacífico, con el propósito de mantener la integridad territorial, el orden constitucional y contribuir al desarrollo del poder marítimo y a la protección de los intereses de la Nación. (Armada Nacional, s.f.).

De igual manera, la Armada nacional, cuenta con Fuerzas Navales y Batallones Fluviales, de esta forma: Bajo el mando operacional de las Fuerzas Navales del Caribe, en (540.876 km2) y del Pacífico en (339.500 Km2), esas dos Brigadas cubren 40.835 km2 de territorio, protegiendo ocho departamentos de la Costa Caribe y Pacífica. De la misma forma, la Brigada Fluvial, cumple la misión, con sus seis Batallones Fluviales y con el apoyo del componente naval, de ejercer el control fluvial de los principales ríos navegables del territorio colombiano.

A través de los puestos Fluviales, que son los que ejercen el control sobre los ríos más importantes de nuestro país, permitiendo que muchos colombianos puedan navegar con tranquilidad, controlando el uso de las aguas, del tráfico de narcóticos, de armamento, y de químicos.

Asi las cosas la ciberseguridad es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (CONPES 3854, 2016). Stevens (2018), señala que la ciberseguridad es “un medio no sólo de proteger y defender infraestructuras de información esenciales, pero también una forma de políticas internacionales a través de los medios tecnológicos de la información” (pág. 2)

En el compes la ciberdefensa se define como el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales (CONPES 3854, 2016)

Por otro lado se define como un ataque cibernético a las acciones organizada o premeditada realizada por uno o más actores con la finalidad de causar daño o problemas a un sistema a través del ciberespacio (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

Entonces las Amenazas cibernéticas es una situación potencial que pone en peligro la seguridad cibernética de la población, el territorio y la organización política del estado (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

En ese orden de ideas la Ciberguerra es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales (CONPES 3854, 2016)

En la actualidad el Ciberespionaje es el acto o practica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza

clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas. (CONPES 3854, 2016).

Uno de los crímenes actuales es el ciberlavado el cual esta definido como el uso del ciberespacio en cualquiera de sus formas, con la finalidad de dar apariencia de legalidad a bienes obtenidos ilícitamente u ocultad la ilegalidad de los mismos ante las autoridades (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

En ese entorno la explotación del ciberespacio son ese conjunto de acciones tomadas en el ciberespacio para obtener inteligencia, maniobrar, recopilar información o realizar otras acciones necesarias para prepararse para futuras operaciones militares. (CJCS, 2018)

Algo muy importante en la actualidad es el ciberterrorismo el cual se denomina de este modo el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado y desencadenando como consecuencia la violación de la voluntad de las personas (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

En el desarrollo actual de las Fuerzas Armadas se desarrollan ciberoperaciones que son operaciones militares desarrolladas en el ciberespacio, con objetivos iguales, a los que se producen en las dimensiones clásicas del área de operaciones: como las de adquirir ventaja, conservarla, situar al enemigo en desventaja y explotarla.

Para esto los estados utilizan la ciberinteligencia que es la aplicada al ciberespacio, consistente en recopilar, analizar e interpretar toda la la información, recopilada mediante técnicas complejas para de esta manera poder identificar, prevenir y mitigar posibles ciberataques.

Así también la ciberdisuasion que básicamente consiste en la prevención de cualquier agresión al ciberespacio de un adversario, bajo condiciones de amenaza que le sean demostradas, por tanto, "la disuasión consiste en la amenaza de recurrir a la fuerza, en proporción capaz de causar daños difícilmente asumibles, con el objeto de evitar un ataque" (Sodupe, 1991).

Para esto el ciberdominio teniendo en cuenta que entendemos como, "dominio", es el poder absoluto, que ejercen los Estados sobre ciertas áreas, tales como la tierra, el mar, el aire. Según, Gen Michael V. Hayden (2018), se pregunta, si efectivamente existe un "ciberdominio", por cuanto, estamos frente a un ambiente muy complejo de tangibilidad como sucede con el resto de los dominios considerados tradicionalmente por los países. Según la doctrina, el ciberdominio o ciberespacio, se puede considerar como un dominio aceptado, y concebido de esa manera, es así: tierra, mar, aire, espacio y ciberespacio. Pero se trata de un dominio particular, natural, creado por el hombre, y es lo que lo diferencia de los demás dominios.

1. REALIZAR UN DIAGNÓSTICO DE LAS CAPACIDADES CIBERNÉTICAS DE LA ARMADA DE COLOMBIA.

La revolución digital, conocida como la cuarta revolución industrial, por su auge a gran escala, ha generado un cambio en el sistema informático, lo que ha conllevado a que nazcan gran cantidad de amenazas cibernéticas, las cuales son múltiples y variadas, pues pueden en cuestión de segundos, cambiar los vectores operacionales, las cuales ponen no solo en riesgo la economía y la sociedad, sino la seguridad y defensa de un país, toda vez. que los organizadores de ataques, buscan, constantemente, mejorar sus técnicas, para lograr mejores y más fáciles objetivos, conllevando a escenarios más complejos, que ponen en riesgo la seguridad y defensa nacional, que debe ser afrontado de manera rápida y decidida por las fuerzas de la Ley.

El autor Schwab Klaus, ha manifestado que la revolución digital en su esencia, “No cambia lo que hacemos, sino que cambia lo que somos” Klaus S. (2018). Marcando una señal que se piense y se evolucione en el concepto de Defensa Nacional, al nuevo entorno operacional llamado ciberespacio, para examinar las vulnerabilidades y los retos que se deben asumir ante la nueva revolución digital.

Por tanto, la nueva confrontación bélica se da a través el ciberespacio, que, al ser combinado con los dominios de tierra, mar, aire y del espacio, construyen una capacidad y superioridad que debe primar en cualquier nación; por tanto, esta evolución y crecimiento tecnológico, toman cada vez menos tiempo y se pronostica que para este año 2022, según

estudio realizado por el Instituto Tecnológico de Massachusetts (MIT) [23] y las reflexiones de Klaus Schwab (2018), en su libro “La cuarta revolución industrial”, donde se pronostica, entre otras cosas, que “las innovaciones tecnológicas más importantes están a punto de generar un cambio trascendental en todo el mundo y esto es inevitable”. Como consecuencia de este artículo, se plantea a corto plazo una estrategia cibernética para nuestro país, para obtener de esta forma victorias tempranas, contando con estrategias preventivas.

Así las cosas, se debe plantear una serie de estrategias, en los diferentes niveles de la guerra, con el fin de generar a nivel de doctrina, utilizando la organización, el material, el personal y la infraestructura, necesarias que permitan establecer la situación actual, que deben utilizar las FF.MM de Colombia, frente a las amenazas que presenta el ciberespacio, y frente a las tecnologías variables, para que de esta forma, la Ciberdefensa Nacional en Colombia, pueda utilizar dichas estrategias, en un instrumento llamado la “Ventana de AREM” (amenazas y riesgos emergentes), planteándose como una operación estratégica y táctica de actuación de los organismos, para comprender los aspectos conocidos (que son las situaciones tradicionales que se presentan en la organización) y desconocidos (entendidos como los riesgos latentes, que se manifiestan en forma frecuente), de sus capacidades, en el contexto de aquellos riesgos y amenazas propias de su entorno.

Por tanto, la ventana de AREM, es una propuesta novedosa que busca motivar a las organizaciones, para pensar sobre aquello que conocen y desconocen, “una apuesta para detallar y profundizar la misión empresarial que los moviliza para crear las condiciones de

operación que les permita “caminar sobre las aguas” de la inestabilidad y no morir en el intento”.

En conclusión, la ventana de AREM, “es una forma de nunca subestimar las condiciones asimétricas de la inseguridad de la información, sino más bien, de pensar en los detalles que implican su entendimiento, la mente de los atacantes, las relaciones propias entre la tecnología, los procesos y las personas, las vulnerabilidades latentes, que no marginan el conocimiento de los actores de la organización, sino que potencian sus reflexiones para crear una vitrina de aprendizaje y desaprendizaje que hablan de una empresa resistente a la fallas no por excepción, sino por convicción.” IT-Insecurity 2013

En este sentido, podemos decir que son numerosos los ejemplos de ciberataques a actores Estatales alrededor del mundo, iniciando con el ocurrido en Estonia en el año 2007, hasta llegar al más reciente, ocurrido en Australia en el mes de junio de 2020, donde se intentaron afectar los sistemas informáticos del gobierno y del sector empresarial. Teniendo en consideración las investigaciones desarrolladas con respecto a estos ciberataques, se analizará el caso del ciberataque a Estonia, el cual generó gran caos y confusión al interior de dicho país, siendo de gran relevancia por ser el primer ciberataque a gran escala en contra de un Estado y claro ejemplo para el mundo con respecto a las vulnerabilidades que pueden ser explotadas a través del ciberespacio.

Estonia estuvo bajo el dominio de la Unión Soviética hasta el año de 1991; a partir de ese momento, sus nuevos gobernantes “consideraron el desarrollo de la tecnología de las

comunicaciones y la expansión de la información como factores centrales del nuevo modelo de desarrollo" (The Conference Board y Fundación Telefónica, 2011), sin embargo, esta gran oportunidad pasó a ser una amenaza. En 2007, Estonia recibió un ataque cibernético sin precedentes el cual paralizó "los sitios web operados por los ministerios del gobierno de Estonia, bancos, medios de comunicación y otras compañías" (Lee, 2007), afectando la infraestructura crítica del país. Los ataques se presumen vendrían siendo auspiciados por el gobierno de Rusia, quienes pretendían coaccionar algunas políticas de Estonia. Este gran precedente fue base para el análisis y preparación por parte de los demás Estados y organizaciones a nivel mundial y, tal fue su magnitud que algunos lo han denominado "WWI" (Web War One) que traducido significa primera guerra Web (Clarke y Knake, 2010, p.21).

En el mismo sentido, es interesante conocer, el desarrollo del conflicto a nivel del ciberespacio en la guerra de Ucrania, pasado menos de un año, del conflicto bélico con Rusia, parece un buen momento para analizar qué está pasando en la dimensión ciberespacial del conflicto.

Algunos analistas expertos en ataques ciberespaciales, han analizado este conflicto, apuntando a que Rusia, utilizara sus bastas capacidades operativas en el ciberespacio, para doblegar, aun mas a Ucrania, en razon a que se creyó que utilizaría el ciberespionaje, el cibersabotaje, la desinformación y la propaganda dentro de lo que se ha llamado la "guerra hibrida", que consiste en el empleo coordinado y sincronizado de las capacidades de un estado, en sus diferentes áreas, económicas, militares de información, diplomáticas, etc., para

combatir a su oponente sin dar lugar a una respuesta en legítima defensa, o cualquier tipo de respuesta, apuntando a que Rusia los utilizaría en forma contundente, ataques masivos, simultáneos, como lo hizo en el año 2007 frente a Estonia, como asimismo, contra Georgia y Kirguistán, por lo que diez años después, se confiaba en que Rusia, habría multiplicado en forma desbordada sus capacidades. Por cuanto Rusia, desde el año 2014, utilizo a Ucrania, para hacer pruebas con sus ciberarmas, con las campañas de desinformación y propaganda, con la convicción de que las agencias rusas, podrían haber colocado, de manera estratégica, malware, en diferentes sistemas ucranianos, como en las estructuras críticas, de servicios esenciales, de información gubernamentales, como también, de mando y control, de combate y de armas de sus fuerzas armadas, y que al llegar al momento crucial, en un mismo momento, en forma simultánea, se activarían, dando como resultado "un apagón" del ciberespacio, provocando caos, confusión, desmoralización, en los Ucranianos, hasta llegar a una no acción defensiva, y como consecuencia de ello, provocar una diversidad de acciones a través del ciberespacio, entre otras:

- "Activación de malware previamente posicionado en objetivos de interés, con fines de sabotaje.
- Ciberataques masivos de denegación distribuida de servicios (DDoS) contra sitios web ucranianos.
- Ciberataques masivos contra infraestructuras críticas y servicios esenciales de Ucrania (wipers, ransomware, DDoS).
- Defacements masivos en sitios oficiales ucranianos.

- Campañas masivas de phishing.
- Campañas masivas de suplantación de identidad en redes sociales (RRSS).
- Distribución de malware altamente sofisticado (wipers, ransomware, troyanos, exploit kits).
- Potentes campañas de desinformación y propagandarft.
- Iniciativa, manejo y control de la narrativa.” (Cubeiro Cabello/IEEE/2022)

De igual manera, señalan los analistas, que se esperaba que Rusia, no solo dirigiera esas operaciones al ciberespacio de Ucrania, sino también, que fueran contra, terceros actores, especialmente a la OTAN, la UE y a sus Estados miembros, en mayor o menor intensidad. Se consideraba, que Rusia arrasara desde un comienzo a Ucrania, manteniendo su supremacía en el ciberespacio, y sus operaciones se dirigieran en todas las áreas: terrestre, naval y aéreo. Pero no fue así, la realidad fue otra, los analistas esperaban un comportamiento diferente, debido al empleo masivo de las “herramientas hibridas”, que, con solo, apretar un botón, la guerra que comenzó, se iba a dirimir en el ciberespacio, estamos frente a una guerra convencional, con una mínima participación aérea y naval y en apariencia, en un porcentaje insignificante de “lo ciber”.

Se hace necesario dejar claro, que la guerra cibernética, es uno de los componentes de las llamadas guerras híbridas. “Consiste en un conjunto de técnicas que vienen a suplir la invasión convencional por tierra. Es complicado definir de qué instrumentos hablamos, pero incluye desde ciberataques o desinformación hasta la utilización de inmigrantes como arma,

como se ha visto en Bielorrusia", describe Andrea G. Rodríguez, investigadora en tecnologías emergentes en Cidob (Barcelona Centre for International Affairs).

Una vez establecido, el concepto de una guerra hibrida, continuamos con el análisis que nos ocupa de la guerra entre Ucrania y Rusia, pues Cubeiro Cabello/IEEE/2022 hace una recopilación, en forma cronológica de lo que sucedió en los primeros días de la guerra y con la inclusión de Ucrania en la OTAN, indicando que entre el 13 y el 15 de Enero, aproximadamente, 40 días antes de la invasión, se produjeron una serie de ataques, dejando sin servicios a numerosos sitios web del gobierno, entre ellos, del Ministerio de Relaciones Exteriores, el gabinete de Ministros y el Consejo de Seguridad y Defensa, y algunas entidades bancarias, reemplazando los atacantes, los sitios web con mensajes en ucraniano y en ruso, en los que se podían leer, textualmente: "«¡Ucranianos! ... Toda la información sobre ti se ha hecho pública. Ten miedo y espera algo peor. Es tu pasado, presente y futuro»

Pero, como consecuencia de ello, no se filtró ninguna información y los sitios web fueron restaurados a pocas horas, según las autoridades ucranianas. Detectándose por primera vez y por ese mismo tiempo, un malware, con estructura similar a un ransomware, (virus por el que se ofrece un rescate). pero que carecía de función de recuperación, puesto que su fin era servir de borrador. Textualmente "El wiper, denominado DEV-0586 o WhisperGate", afectando diferentes entidades gubernamentales y entidades civiles ucranianas, por lo que culpo a Rusia de estos ataques, siendo negado por el gobierno ruso. Razon por la cual, la OTAN, le dio acceso a Ucrania a su plataforma de intercambio de información sobre malware.

Continuando con la recopilación, Cubeiro Cabello/IEEE/2022, para el 15 de febrero, se presenta un segundo ciber ataque de denegación distribuida de servicios (DDoS), contra los sitios web del Ministerio de Defensa, el Ejercito y las dos entidades bancarias, más grandes de Ucrania, los cuales afectaron aplicaciones móviles y los cajeros automáticos de los bancos. Culpando del ataque a la Dirección Principal de Inteligencia (GRU) de Rusia, según lo señalado por el gobierno del reino Unido, como también por el Consejo de Seguridad Nacional de los EE.UU., en razon a que se pudo detectar la transmisión de considerable información desde la estructura del GRU, con destino a las IP y los dominios afectados. Pero, nuevamente desde la ciudad de Kremlin, los rusos negaron ese ataque.

Con un tercer ataque, el 23 de Febrero, con DDoS, se eliminaron varios sitios web de entidades estatales, militares y bancarias de Ucrania, en ese mismo ataque, malware, borrador de datos, llamado como, Hermetic Wiper, se detectó en centenares de dispositivos de entes estatales, como en las áreas financiera, de defensa, de aviación y de las tecnologías de la información. El cual fue compilado hasta el mes de diciembre 2021. Dicho ataque, se da en el momento en que tropas rusas hacen el reconocimiento de regiones separatistas en el este de Ucrania, siendo invadidos por soldados rusos, por lo que de nuevo fueron acusados por los EE.UU. y el Reino Unido, circunstancia que fue negada, nuevamente por Rusia.

En Twitter, El 27 de febrero, la organización hacktivista Anonymous anuncio estar «oficialmente en guerra contra el Gobierno ruso» prometiendo apoyar a Ucrania contra «la

brutal invasión del Kremlin». Y sin confirmar, declararon echado abajo el sitio web del Ministerio de Defensa ruso.

Viasat, la compañía estadounidense de comunicaciones por satélite, el 28 de febrero, procedió a investigar un ciberataque, que provoco la interrupción parcial de los servicios de banda ancha en Ucrania y en toda Europa, indicando que tal interrupción, se debió al mencionado ataque DDoS, que había amenazado a bancos y entes gubernamentales el 23 de Febrero

Avast, una compañía experta en asuntos cibernéticos, para el primero de marzo, anuncio la distribución gratuita de un descifrador para la cepa de ransomware Hermetic Wiper., período muy corto, para contrarrestar el lanzamiento de una solución frente a un ransomware.

El director de la Agencia Espacial Rusa, el 3 de marzo, desmintió el supuesto ataque de un grupo afín a Anonymous, que declaro un ataque a dicha agencia, calificando a los supuestos atacantes, textualmente de «estafadores de poca monta». De igual manera, algunos grupos de hackers, como los Conti, apoyaron a Putin y amenazando a los que actuaran en su contra. En el mismo sentido, ese día, el Servicio de Seguridad de Ucrania (SSU), anuncio que piratas informáticos atacaron diferentes sitios web de entes gubernamentales ucranianos, con los cuales distribuían falsos comunicados de capitulaciones de Ucrania

A partir del día 6 de marzo, según informes, Rusia, intensifico las campañas de phishing contra la población ucraniana, para insertar malware en sus dispositivos. Debido al éxodo masivo hacia occidente, estos ataques llegan hasta Polonia y Hungría.

El 15 de marzo, Anonymous, se concentra en atacar a las multinacionales, que siguen operando en Rusia, como Nestlé, intentando traspasar el bloqueo informativo, con el que Putin, sometió a su propia población, con operaciones masivas de SMS y WhatsApp, cuyos resultados se desconocen por el momento. Por este mismo tiempo, fuentes informan de la desarticulación del grupo Conti, por exponerse información crítica sobre dicho grupo, por parte de insiders ucranianos.

Por último y como culminación del escrito presentado por el Capitán de Navío, Enrique Cubeiro Cabello, que fue objeto de este análisis, el día 24 de marzo, miembros del grupo Anonymous, señalaban del ataque del grupo hacktivista al Banco Central de Rusia, y que, como consecuencia de ello, tuvieron acceso a muchos archivos confidenciales.

Concluye, textualmente, Cubeiro Cabello (IEEE/2022), que el panorama en el ciberespacio, en esta guerra, se ha basado en lo siguiente:

1. “Ataques rusos muy puntuales a infraestructuras críticas y servicios esenciales de Ucrania.
2. Ataques masivos rusos a sitios web de Ucrania (fundamentalmente, DDoS).
3. Numerosos defacements en sitios oficiales de Ucrania.

4. Campañas de phishing y suplantaciones de identidad a media escala en RRSS.
5. Distribución limitada de malware ruso de sofisticación media-baja.
6. Ámbito de actividad bastante circunscrito a Ucrania.
7. Anonymous y otros grupos hacktivistas han tomado partido contra Rusia (con escaso impacto hasta ahora).
8. Campañas rusas de desinformación y propaganda, con gran efectividad en territorio ruso y Estados afines y escasa en el resto del Mundo.
9. Narrativa ampliamente a favor de Ucrania, con Rusia a la defensiva y muy escasa capacidad de contranarrativa
10. Es decir, se ha cumplido lo esperado en lo referente a ataques contra sitios web, cuentas oficiales y redes sociales, e incluso podemos identificar dos fases diferenciadas:
11. Una primera, previa la invasión, iniciada en torno al 13 de enero, enfocada a la preparación del entorno operacional (esencialmente, a provocar temor, caos, confusión en la población ucraniana, debilitando su voluntad de vencer y la confianza en sus dirigentes e instituciones).
12. Una segunda, iniciada en el momento de la invasión, en la que se continuó con la metodología de la primera, intensificándose progresivamente y ampliando sus objetivos, probablemente existiendo cierta sincronización de las acciones con las del resto de ámbitos operacionales en el plano militar."

Ahora bien, en el escenario estratégico general a nivel mundial, se ha caracterizado porque a comienzos del siglo XXI, al igual que con los ya tradicionales riesgos y amenazas

para la paz, la estabilidad, el equilibrio y la seguridad internacionales, ha conllevado como consecuencia el terrorismo de carácter transnacional, con alcance global, con una capacidad enorme de causar daño en forma indiscriminada, con las diferentes modalidades que se pueden presentar en el ciberespacio. Por eso, resulta preocupante, que la superioridad militar tradicional, frente a los nuevos riesgos y amenazas, ciberespaciales, no representa un factor de disuasión exitoso, ni mucho menos garantiza, más seguridad, ni una prevención eficaz, contra ataques terroristas o ciberataques; en razon a que, por ejemplo, quedo demostrado, que la lucha contra esas amenazas, es clave en la estrategia de los países y las diferentes organizaciones de seguridad y defensa, en forma conjunta, tanto en los atentados de Nueva York, Madrid o Beslán, en cuanto al terrorismo y los ciberataques sobre Estonia, ya analizado ampliamente en este capítulo, el de Georgia y un sin número de países, se pudo evidenciar, tales circunstancias, que se deberían tener en cuenta para afrontar este tipo de amenazas. Es así como Europa, debe afrontarlas decididamente si no quiere convertirse en un objetivo fácil. Este fue el caso de los ciberataques sufridos por Georgia durante el conflicto con Rusia en Ossetia del Sur y Abkhazia. Por primera vez en la historia una operación militar fue acompañada de una serie de ciberataques a los sitios Web del gobierno Georgiano y otras páginas comerciales, dejándolos fuera de servicio en algunos casos y modificando el aspecto de las páginas en otros («Defacement»).

Analistas de Estados Unidos, han señalado que países como China, Rusia o Corea del Norte, disponen de unidades especializadas y personal capacitados para llevar a cabo ciberataques y prevén que, en los próximos diez años, se sufrirán graves consecuencias derivadas de sus acciones, en razon a que, en la actualidad, la mayor parte de los sistemas

disponen de una seguridad mínima, de procedimientos inadecuados y de un adiestramiento deficiente en seguridad. En este sentido, también se ha pronunciado, en febrero de 2010, el antiguo Director de Inteligencia Nacional de EEUU, Mike McConnell, señalo que, ante el Comité de Ciencia, Transporte y Comercio del Senado, que «el país no se está tomando con seriedad la ciberseguridad y caerá víctima de un ciberataque demoledor en los próximos años. Si la nación entrara en una ciberguerra, perderíamos…no mitigaremos este riesgo. Hablaremos de ello, agitaremos los brazos, tendremos una ley, pero no vamos a mitigar este riesgo». McConnell, dijo que el gobierno, debe asumir un papel principal en la ciberseguridad, ya que un ciberataque podría paralizar, el comercio y hacer temer la confianza de los consumidores en mercados financieros y el gobierno federal, «compitiendo con los daños de un ataque nuclear al país»., concluyo.

DE LOS CABLES SUBMARINOS ¿QUE SON Y PARA QUE SIRVEN?

La era de la información funciona gracias a delgados cables de fibra óptica enterrados en el fondo del mar, los cuales se extienden entre los continentes, para conectar a los más remotos rincones del planeta, son cables submarinos que atraviesan la Tierra. (CNN); se consideran los cables submarinos, como cables de fibra óptica que conectan países de todo el mundo a través de cables colocados en el fondo del océano. Estos cables, a menudo de miles de kilómetros de longitud, pueden transmitir grandes cantidades de datos rápidamente de un punto a otro. Según los datos de TeleGeography, actualmente hay 508 cables submarinos entre activos y proyectados. (21/03/2022).

El cable submarino se muestra como una solución robusta y eficaz, por la resistencia ante inclemencias meteorológicas, menor latencia, y mayor ancho de banda que la comunicación por satélite, todo lo cual lo posiciona como una infraestructura más fiable y de mayor capacidad, una vez instalada y probada.

Muchos analistas, han señalado que los cables submarinos, son elementos estratégicos claves que transportan el 98% del tráfico de datos del mundo, y que se trata de un elemento fundamental que pasa desapercibido en muchos análisis de riesgos de infraestructura crítica de las naciones, pues el desarrollo del internet, no solo debe estar asociado con la evolución de la infraestructura computacional, de almacenamiento y redes, sino con los cables submarinos.

Estos cables de fibra óptica son considerados, generalmente por privados o alianzas público-privadas. “Cabe mencionar que los dueños de los cables no siempre son los mismos que los que los fabrican o los que gestionan las estaciones de tierra a las que se conectan. Cada vez más, compañías privadas en conjunto con los gobiernos de las potencias mundiales forman parte de consorcios que fabrican y despliegan estas infraestructuras” (Galán, 2021). Un reciente estudio de Atlantic Council muestra muchos de estos elementos, indicando que aproximadamente el 38% de las conexiones oceánicas están participadas de una u otra manera por intereses gubernamentales (Sherman, 2021).

“Las implicaciones para la seguridad de esta infraestructura crítica son claras: quien controla las líneas posee un poder considerable. Dado que los datos se han convertido en un

activo estratégico cada vez más importante, los riesgos de seguridad podrían ser considerables en determinadas circunstancias (…). Aunque el transporte marítimo y las operaciones de pesca causan la mayor parte de los daños a los cables y los acontecimientos naturales como los terremotos, los ciclones e incluso las mordeduras de tiburón pueden interferir con las operaciones, la perspectiva de daños intencionados y maliciosos se cierne sobre ellos, ya que la cantidad de datos que atraviesan los cables transoceánicos sigue creciendo y la dependencia del almacenamiento en la nube aumenta" (Diálogo-Americas, 2022).

En ese sentido, en la invasión de Rusia a Ucrania, "uno de los avisos que Rusia ha mandado a Europa en medio de la crisis de Ucrania ha girado en torno a los cables. Un grupo de navíos y submarinos ruso han llevado a cabo en febrero prácticas militares cerca de Irlanda, tan cerca que se estaban desarrollando justo al límite de sus aguas de explotación económica exclusiva. El gobierno irlandés exigió al embajador ruso en el país que alejaran sus fuerzas militares de esta área, quien atendió la petición. Los barcos y submarinos rusos trasladaron el área de sus maniobras. ¿La tensión? Tanto la primera zona como la segunda zona oceánica elegida en las maniobras de la flota rusa estaban sobre los cables submarinos atlánticos que conectan Europa con EEUU" (Del Castillo, 2022).

El Parlamento Europeo (Cbueger et al., 2022), elaboro un documento, teniendo en cuenta esas amenazas físicas y cibernéticas, con el uso de patrones coincidentes, para generar inestabilidad y zozobra, donde establece una perspectiva del reto estratégico que a traviesa el lecho marino con los cables submarinos, detallando algunos riesgos claves a tener en

cuenta. Razon por la cual, para comprender estos ataques deliberados a esta infraestructura, cables submarinos, es necesario saber cuáles son los retos principales y de qué manera, se verán, afectados, veamos:

1. **La *v*ulnerabilidad del cable en sí mismo.** Suele ser publica, cuando se trata aguas cerca a la costa y poco profundas, esto con el fin de evitar accidentes por la puesta de anclajes y dragados, esto a diferencia de alta mar, pues no se publican las ubicaciones con precisión, en razon a que los cables son más difíciles de localizar (Cbueger et al., 2022). Es entendido, que las reparaciones en alta mar, son más difíciles y dispendiosas, por la profundidad del fondo marino, por ese motivo, una ruptura de un cable, genera un mayor impacto, por el tiempo que puede durar su reparación, perjudicándose de esta manera a los usuarios o beneficiarios, porque no tendrían señal o esta seria intermitente y no confiable.

2. **Las estaciones en tierra donde terminan los cables submarinos y se conectan con la red terrestre del operador local.** Por lo general, están cerca a la costa y ubicadas en redes eléctricas submarinas u otras infraestructuras críticas. Contienen servidores y tecnologías de enrutamiento y conmutación que proporcionan el puente a la red terrestre (Cbueger et al., 2022). Si se tiene la ubicación de puntos estratégicos y los datos de su direccionamiento, serian puntos de falla sensibles, lo que conllevaría a la negación del servicio, manipulaciones que alteren el tráfico de datos en un país, con consecuencias graves para la dinámica de la nación.

3. **Los procedimientos de reparaciones de los cables**. Estos son reparados, por una

empresa diferente a las propietarias y operadoras de dichos cables, al igual que su mantenimiento, pues estas se limitan a firmar los contratos, con esas empresas y estas disponen de almacenamiento de cables y equipos, de buques cableros, los cuales se encuentran situados en todo el mundo, con disponibilidad de las 24 horas al día, para reparar los daños que se puedan presentar (Cbueger et al., 2022). Por lo que se da una dependencia económica en los estados, pudiendo solicitar la atención ante las fallas que se presenten, como las alianzas geoestratégicas necesarias para coordinar operaciones, de atención fortaleciendo, no sólo las relaciones entre los países aliados, sino la coordinación del tráfico de datos entre los países.

En consecuencia, de lo anterior, existen como mínimo, tres clases de amenazas, para tener en cuenta en este tipo de infraestructuras críticas, o ataques a la infraestructura de red técnica de los cables submarinos (Cbueger et al., 2022), que serían:

A. Ataques físicos
B. Monitoreo
C. Robo de datos

Estos ataques físicos, pueden darse de diferentes modalidades, usando por ejemplo buques civiles, de investigación, de pesca, de transporte o simplemente yates de recreo, utilizando para ello Dispositivos de Corte Improvisados (DCI), como anclas y dispositivos de dragado que terminen afectando, no solo la integridad física del cable, sino su ubicación

y anclaje en el lecho marino, haciéndolo más susceptible a las corrientes marinas, tsunamis o eventos agrestes de naturaleza como tifones. (Cbueger et al., 2022)

El uso de explosivos estratégicamente ubicados, el cual puede ser coordinado y ejecutado de forma simultánea creando mayor inestabilidad, por la demora en restablecer el servicio, es otro ejemplo de ataque físico, más agresivo y dirigido no sólo sobre el cable en sí mismo, sino sobre el contexto donde fue instalado, para crear inestabilidades en el diseño y anclaje original que termine con la generación de daños o reparaciones que pueden ser costosas y demandantes para las naciones y empresas dedicadas a estas labores (Cbueger et al., 2022).

Los ataques físicos, también se pueden presentar, a través de barcos sumergibles, embarcaciones, o drones y submarinos de grado militar, que pueden ser tripulados o no (Cbueger et al., 2022), estas acciones son más sensibles y delicadas, en razon a que pueden ser articuladas en el poder militar naval, pudiendo terminar con acciones deliberadas o asistidas por errores estratégicos, conllevando a que se vea afectada la estructura e integridad de estos activos estratégicos de las naciones, como por ejemplo, habilitando la interceptación de datos, la vigilancia y la interrupción del tráfico, siendo objetivos más accesibles y vulnerables de las operaciones de espionaje e inteligencia (Cbueger et al., 2022). Así las cosas, se debe instar a lo proveedores para instalar software no autorizado, malicioso o de espionaje. que termine enviando información sensible a los terceros para los cuales se ha concretado la operación.

Por último, las amenazas directas, digitales, están “asociados con la aplicación de técnicas de hacking en los sistemas de gestión de la red, pudiendo proporcionar el control a los atacantes de múltiples sistemas de gestión de cables, la visibilidad de las redes y los flujos de datos, el conocimiento de las vulnerabilidades físicas de los cables y la habilidad para supervisar, interrumpir y desviar el tráfico. En este sentido, los centros de operaciones de la red, los portales de acceso remoto y otros sistemas necesarios para el funcionamiento de la red de cables -como la energía eléctrica, los enrutadores, la calefacción, la ventilación y el aire acondicionado- también son potenciales vectores de ciberataque” (Cbueger et al., 2022).

En conclusión, podemos señalar que los cables submarinos, plasman un reto geopolítico estratégico para naciones, en razon a que lo que se establece en ellos, es el ejercicio del poder en el tráfico de las redes globales, las que se pueden convertir en peajes, en el desarrollo de los ecosistemas digitales, en razon a los intereses que manejan, no solo los proveedores, sino los propietarios de los cables, al igual que el tratamiento y el flujo de datos personales, que ponen en peligro la soberanía digital de los gobiernos.

Por consiguiente, las estrategias de las organizaciones públicas, privadas, las alianzas de los estados y las empresas de telecomunicaciones, para que aporten iniciativas y trabajen en conjunto son fundamentales, para que reine la colaboración y la conectividad, en medio de los intereses económicos que se colocan en juego. Siendo por tanto, un ejercicio de coordinación de carácter multilateral e internacional, que sirva de motivación para la convergencia de alianzas, importantes entre todos los estados, y que se reconozca esta infraestructura como un bien común en beneficio de los ciudadanos, para lograr identificar,

reconocer, tratar y simular, los diferentes riesgos alrededor de la seguridad y defensa de los cables submarinos, involucrando a las empresas de telecomunicaciones, para que se puedan constituir grandes acuerdos en beneficio de todos, en aguas nacionales e internacionales.

Por otro lado, en algunos de los lugares más inaccesibles del mundo, se están utilizando pequeños enjambres de satélites, que orbitan la Tierra, para rastrear la pesca y la tala ilegales. Es así, como para el año 2020, la organización, Global Fishing Watch en Washington, DC, descubrió que China, pescaba ilegalmente en aguas de Corea del Norte, "en contravención de las leyes chinas y norcoreanas, así como Sanciones de la ONU a Corea del Norte", dice Paul Woods, cofundador y director de innovación de la organización. Como consecuencia de ello, los pescadores, norcoreanos debían ir más lejos, hasta Rusia, por lo que las pequeñas embarcaciones no estaban preparadas. "No pudieron regresar", dice Woods. China, atrapada, detuvo rápidamente sus actividades, pues muchas de esas embarcaciones, aparecían en el Japón, con norcoreanos muertos a bordo, situación que aumentaba cada año, sin tener explicación alguna, hasta que dicha organización, concede en DC Spire Global, realizo tan macabro episodio, con sus pequeños satélites en órbita terrestre, los cuales se diseñaron para "captar los pulsos de radio enviados por barcos" en todo el mundo, utilizados igualmente por barcos, para que no se choquen en alta mar y para rastrear la actividad marítima ilegal.

Con dichos satélites, señala WOODS y de acuerdo a la forma como se mueven las embarcaciones, cuando están pescando, a su velocidad, dirección o la forma como giran, se puede predecir, que clase de pesca están usando; por esa razon, con los barcos que emiten

esos pings, se logra comprobar que muchas embarcaciones están realizando actividades ilegales, según Spire Global, incluso en horarios restringidos, siendo el uso de estos satélites, una práctica muy novedosa, en materia de tecnología, pues son pequeños y se pueden volar en conjunto o en forma individual y su costo no es tan elevado, convirtiéndose en una propuesta asequible.

A este respecto, textualmente "antes de 2018, nunca se habían lanzado constelaciones de más de 100 satélites activos a la órbita terrestre, dice Jonathan McDowell, experto en satélites del Centro de Astrofísica Harvard-Smithsonian en los EE. UU. Ahora hay tres, con cerca de 20 constelaciones más en proceso de lanzamiento y unas 200 más en desarrollo. Es un "boom en las constelaciones", dice McDowell 2018.

De otro lado, son numerosas las razones para usar constelaciones, entre ellas para transmitir internet a distancias remotas, como es el caso del mega constelación Starlink de SpaceX, el cual contiene tres mil satélites, representando casi la mitad de todos los que se encuentran en orbita, aumentándose dicho enjambre a más de doce mil, al igual que el enjambre llamado AMAZON, el cual tiene planes de aumento de satélites, lo que preocupa a muchos, pues puede producirse una colisión entre los satélites en orbita, produciéndose basura espacial peligrosa,

Estos enjambres satelitales, pueden invadir el mundo, proporcionando datos importantes, rastreando las emisiones ilegales de metano, por ejemplo, o proporcionar redes de comunicaciones útiles, o entregar imágenes de la superficie de la tierra, otros enviar

paquetes de datos entre diversos dispositivos, a ubicaciones remotas, en diferentes partes del mundo. Son estos algunos ejemplos de las numerosas utilidades que pueden aportar los enjambres satelitales, en tierra, mar y aire.

Llegado a este punto, es pertinente enfocarse hacia el Estado Colombiano, el cual en la actualidad se encuentra en un esfuerzo de transformación digital, mediante la masificación del empleo de las tecnologías de la información y las comunicaciones (TIC) por medio de la Ley 1341 de 2009, así como la implementación de políticas públicas como el CONPES 3701 de 2011 "Lineamientos de Política para la Ciberseguridad y Ciberdefensa", el CONPES 3854 de 2016 "Política Nacional de Seguridad Nacional", el plan nacional de protección y defensa para la infraestructura crítica cibernética de Colombia del 2017, el decreto 1008 de 2018 "Política de Gobierno Digital" del Ministerio de las TIC (MinTic, 2018), y el CONPES 3995 de 2020 "Política Nacional de Confianza y Seguridad Digital", evolucionando así a un modelo de Estado abierto a través del uso de las TIC.

Este esfuerzo, si bien presenta una múltiple gama de ventajas a través del empleo del ciberespacio, también abre una gran variedad de vulnerabilidades para el país. Para el año 2018, Colombia ocupaba el sexto puesto de los países más vulnerables en cuanto a ataques cibernéticos en la región (Arias, 2018); para el año 2019, el National Cyber Security Index (2020), el cual mide la preparación de los países para prevenir amenazas y gestionar incidentes relacionados con seguridad digital, posicionó a Colombia en el puesto 57 entre 152 países, con un puntaje de 46,45 sobre 100 (Departamento Nacional de Planeación, 2020),

y para el año 2020, bajó a la posición 60 con un puntaje de 46,75 (National Cyber Security Index, 2020), mostrando una percepción de disminución en materia de ciberseguridad.

Finalmente, la revista Forbes (Hernández, 2020) publicó un estudio desarrollado por la compañía británica Comparitech, donde clasificaban los países más ciberseguros del mundo, donde Colombia ocupó el puesto 40 entre 76 países analizados, siendo el No. 1 el menos ciberseguro. Esto demuestra que, si bien se ha venido trabajando en temas de ciberseguridad, aún se encuentra una amplia vulnerabilidad en los procesos de ciberseguridad y ciberdefensa, teniendo en cuenta que los Estados y los diferentes actores que intervienen en el ciberespacio están usando cada vez técnicas de guerra cibernética más nuevas y mejoradas para atacarse entre sí (Aguilar, 2011).

Es prudente advertir, que los ataques cibernéticos son un factor colateral a los bienes comunes del Estado (Gómez Á. 2011); por lo tanto, trascienden al ciberespacio y generalmente ponen en riesgo la integridad de un país y de sus ciudadanos, generando así un apremio en materia de seguridad y defensa nacional, situación que implica, involucrar a las instituciones, organismos y empresas tanto del sector público como privado (Ministerio de Defensa Nacional, 2017). Consecuente con esto, el Gobierno Nacional mediante el CONPES 3701 de 2011, creó una Comisión intersectorial, encargada de fijar la visión estratégica de la gestión de la información y un grupo de respuesta a emergencias cibernéticas de Colombia (ColCERT), encargado de coordinar a nivel nacional los aspectos de ciberseguridad y ciberdefensa, el cual trabaja en apoyo y colaboración con las demás instancias nacionales.

En consecuencia, en el año 2012, se aprobó la creación y activación del Comando Conjunto Cibernético-CCOCI, cuya función más importante es ejercer la Ciberdefensa Nacional, conduciendo operaciones de nivel estratégico, de carácter militares cibernéticas, para salvaguardar la defensa y la seguridad en el ciberespacio, del país, por el Ministro de Defensa Nacional de Colombia, [Resolución Ministerial No. 7436 de 2012. Ministerio de Defensa de Colombia Documento Reservado].

En el mismo sentido, dentro de cada Fuerza, se ordenó la creación de estructuras organizacionales, con la denominación de Unidades Cibernéticas, para que a través de ellas el CCOCI, ejecute y coordine actividades tendientes a la Ciberseguridad y Ciberdefensa de la Nación, estas tres Unidades se encuentran, una en cada fuerza, una en el Ejército Nacional, otra en la Fuerza Aérea Colombiana y la tercera en la Armada Nacional. Dichas unidades, mantienen relaciones de coordinación con CCOCI, comando que tiene la misión de ejercer la Ciberdefensa, conduciendo operaciones militares Cibernéticas, en el ciberespacio, con el fin de consolidar esfuerzos en mantener las operaciones de ciberseguridad y ciberdefensa nacional, creándose grupos de apoyo y comunicaciones en el interior de cada fuerza, es así como en la Armada Nacional, se creó la Dirección Cibernética Naval

Actualmente, bajo la responsabilidad del Comando General de las Fuerzas Militares (COGFM) a través del Comando Conjunto Cibernético (CCOCI), el cual fue activado en Octubre de 2012, como un ente rector, con el fin de llevar a cabo la realización de direccionamiento, planeación, coordinación, integración, ejecución y sincronización de actividades cibernéticas, el cual depende de la Subjefatura de Estado Mayor Conjunto

Operacional (SEMCO) y de las Unidades Cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana, nuestra nación, cuenta en materia de Ciberdefensa con una estructura organizada, plasmada en la primera edición del Manual Fundamental Conjunto MFC 1.0 - Doctrina Conjunta. **COGFM. (2018**). En razon a que, cuando el Estado colombiano, emprende operaciones militares, las FF.MM. de Colombia, actúan como un solo un componente de un esfuerzo nacional que involucra a todos los instrumentos de poder nacional. El desarrollo evolutivo del ambiente operacional actual, requiere la inclusión de la información en complemento a los instrumentos tradicionales, como son informativos, diplomáticos, económicos y militares, siendo necesario inculcar esta unidad a nivel nacional y convertirla en un esfuerzo operacional, para involucrar los ministerios, instituciones, agencias del gobierno nacional, y en algunas operaciones, como es el caso de la ciberdefensa, involucrar agencias de estados extranjeros

Las unidades Militares lideran trabajos entre las instituciones del Estado en materia de Infraestructuras Criticas, con el fin de fortalecer las operaciones en ciberseguridad, lográndose establecer lazos de confianza entre los entes estales, permitiendo la colaboración y compartiendo información de amenazas y alertas, como medida preventiva para evitar la materialización de amenazas o ataques cibernéticos en contra de nuestro país.

Con todo lo anterior, y pese a los esfuerzos conjuntos, se evidencian vulnerabilidades, en la organización de objetivos estratégicos y acciones estratégicas, en favor de la defensa y en pro de salvaguardar el quinto dominio de la guerra, que es el ciberespacio.

La Armada Nacional, en el entorno marítimo y fluvial en Colombia, en la actualidad, dispone de una infraestructura naval táctica, es decir, un método, un procedimiento, para desarrollar las operaciones de Defensa de la Nación, que consiste en la búsqueda y rescate, en ayudas humanitarias y en el control del espacio marítimo y fluvial colombiano, pudiendo de esta manera, enfrentar una diversidad de amenazas de acuerdo a las operaciones de la delincuencia organizada, como por ejemplo, robo a embarcaciones en altamar, narcotráfico, contrabando, migración ilegal, ilícita actividad de pesca, para que de esta manera, no solo el estado colombiano, sino sus ciudadanos se sientan seguros, con los procedimientos y planes de defensa, que aporta esta fuerza.

De la misma manera y en pro de la defensa del Estado, la Armada Nacional, ha conseguido avances en materia de ciberseguridad y ciberdefensa, aumentando de esta forma, sus capacidades en materia de detección, gestión y análisis de eventos e incidentes, para enfrentar las amenazas y los posibles ataques cibernéticos, que se presenten en la red de datos de la Armada Nacional. En la actualidad, la Armada Nacional, implemento el Centro de Operación de Seguridad (SOC) y el Sistema de Información de Gestión de Eventos (SIEM), fortaleciendo de esta forma, su capacidad de respuesta ante posibles amenazas de origen cibernético. En consecuencia, en el Plan de Desarrollo Naval 2042, 2020, quedo estipulado, que existe más protección en lo que tiene que ver con la infraestructura crítica cibernética (ICC) naval, como lo son las unidades a flote y el Sistema Integrado de Control de Tráfico y de Vigilancia Marítima (SICTVM) de la Armada Nacional.

La Organización Marítima Internacional (OMI mayo 2016), a través del Comité de Seguridad Marítima, aprobaron la guía de gestión de ciber-riesgos marítimos, la cual es voluntaria para los países afiliados; como consecuencia, de los diferentes ilícitos que se presentan en las infraestructuras críticas, que causan impactos en las diversas operaciones y de seguridad en los buques y organizaciones, por tanto, esta guía es básica y primordial, para operaciones seguras, del transporte marítimo, ocupándose principalmente de la seguridad física, contenida en el código PBIP de OMI y de operaciones, descritas en el código IGS de OMI., es decir, en la actualidad, se creó una dependencia para fortalecer las tecnologías de la información, que abarca, no solo los buques, sino las operaciones de las organizaciones de transporte marítimo.

Es así, como las unidades de superficie, aviación naval, guardacostas, submarinos, equipamiento en desastres y emergencias, elementos de combate fluvial, y grupos de comando, son algunas de las capacidades con las que cuenta la Armada Nacional, contribuyendo a las actividades offshore y subacuáticas, a la pesca, a la seguridad, a la construcción naval, para de esta forma tener mares y océanos seguros, a más de la protección ambiental, al turismo náutico y por supuesto al disfrute de un transporte marítimo, para que se pueda decir, que lo primordial, es tener mares limpios, una navegación segura, puertos protegidos, con personal capacitado y comprometido, construyendo de esta forma un mejor país, con el firme convencimiento, para los ciudadanos, que pueden contar con una fuerza, como lo es la Armada Nacional, que les brinda seguridad y confianza de manera estratégica, cuidando y defendiendo los intereses marítimos, ejerciendo su poder, en forma integral, tanto en el agua, ya sea marítimo o fluvial, y en tierra, preservando los Derechos Humanos, al igual

que el Derecho Internacional Humanitario, de conformidad con el ordenamiento legal establecido.

Por consiguiente, la Armada Nacional, “se consolida como una fuerza estratégica para la defensa y seguridad integral de la nación; contribuye al control institucional del territorio, defiende los intereses marítimos, y ejerce el poder naval en el espacio marítimo, fluvial y terrestre bajo su responsabilidad. Todas las acciones de la Armada se realizan en el marco de las normas establecidas y del respeto de los Derechos Humanos y el Derecho Internacional Humanitario” (PEN 2020-2023).

En referencia a las estrategias, el Consejo Nacional de Política Económica y Social [CONPES 3995] (2020), enfatiza que, en Colombia se pueden generar diferencias sociales de seguridad digital, pues existen grupos poblaciones más vulnerables, en razón que, al tener una baja interacción con la tecnología tiene menos posibilidades de prevenir estas situaciones. En efecto, se estipula que los programas deben tener en cuenta la problemática plasmada de acuerdo con el contexto del país, donde se busque la adopción de modelos, estándares y marcos de trabajo que no entorpezcan la aparición de nuevas tecnologías en el futuro y permitan al Estado enfrentar amenazas y ataques de alta complejidad y sofisticación.

Ahora bien, el informe expone el concepto de “infraestructura critica cibernética nacional” el cual se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de

servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

En ese contexto, requieren de la aplicación de un sistema de seguridad social integral que, de acuerdo con sus competencias y de acuerdo con lo que se requiera se pueda coordinar la elaboración de lineamientos para los planes de mejora en seguridad digital con el objetivo de fortalecer las capacidades de dichos sistemas en el manejo, gestión e intercambio de la información, dada la condición e infraestructura critica cibernética del Sistema de Seguridad Social Integral.

En efecto, el documento propende para que en cada nación se establezcan entidades competentes donde como mínimo se definan las condiciones de seguridad esperadas para cada subsistema del Sistema de Seguridad Social Integral y sus entidades involucradas, conexas con una hoja de ruta de acciones para disminuir la brecha en seguridad digital de cada subsistema y su respectivo modelo de seguimiento y evaluación con plan de mejora [CONPES 3995], p. 3, 2020).

Es así, que reconociendo la infraestructura critica, se debe profundizar sobre la necesidad de la clasificación de expedientes, documentos e información confidencial, y la

consecuente identificación temprana de amenazas, con la implementación de estas acciones será posible reconocer información y tipificación de vulnerabilidades con el control del riesgo de divulgación, alteración o pérdida de documentos o expedientes que corresponda con información clasificada, reservada de seguridad nacional o que atenten contra los derechos fundamentales de los ciudadanos, así como la identificación y protección de los documentos vitales o esenciales para asegurar la continuidad y el funcionamiento en caso de materializarse alguna amenaza, incidente o ataque cibernético.

Para dicho fin, el Gobierno Nacional, en acompañamiento internacional, especialmente de la Organización de Estados Americanos (OEA) y a través del Comité Interamericano contra el terrorismo (CICTE), desde mayo de 2008, se organizó la mesa nacional de dialogo, en la que se había encomendado al Ministerio de Defensa Nacional el liderazgo para impulsar e implementar las políticas en seguridad cibernética, así como el diseño de la implementación de estrategias y mecanismos que den respuesta a los incidentes y delitos informáticos que afectan a la nación (Ministerio de Tecnologías de la información y las Comunicaciones, 2011), sin embargo sólo hasta después de los ataques cibernéticos del grupo Anonymous a las páginas web del Estado Colombiano y a la declaratoria de guerra del colectivo hacktivista al Ministerio de Defensa Nacional, se empezaron a generar estrategias concretas para el control del ciberespacio y protección de la infraestructura crítica del país.

No obstante, como resultado de un profundo análisis de las particularidades del esquema de seguridad nacional, las capacidades técnicas existentes en el Ministerio de Defensa y un estudio del contexto internacional. El diagnóstico final indicó que el Ministerio de Defensa tenía la mayor capacidad para manejar de manera eficiente y coordinada estos temas (Ministerio de Tecnologías de la información y las Comunicaciones, 2011). Lo que ha motivado al Ministerio de Defensa Nacional a promover dentro de la agenda nacional en los últimos años el dialogo y la reglamentación e implementación de políticas de ciberseguridad.

Ahora bien, cabe destacar que el tema de Ciberseguridad fue incluido en el Plan Nacional de Desarrollo 2018-2022, Pacto por Colombia, pacto por la equidad, como una estrategia en la promoción de una política de Estado para la transformación digital y el aprovechamiento de la cuarta revolución industrial, a través de la interoperabilidad de plataformas, contacto a través del Portal Único del Estado, uso de tecnologías emergentes, seguridad digital, formación en talento digital, y fomento del ecosistema de emprendimiento. Así las cosas, la seguridad digital contempla, según la Política de Gobierno Digital que lidera el MINTIC, un componente denominado TIC para el estado que incluye tres habilitadores transversales como son: seguridad y privacidad, servicios ciudadanos digitales y arquitectura (MINTIC, 2021).

2. IDENTIFICAR EL ESTADO DE MADUREZ, DESDE LAS METODOLOGÍAS EXISTENTES, DE LAS CAPACIDADES CIBERNÉTICAS DE LA ARMADA DE COLOMBIA.

En Colombia la ciberdefensa y seguridad de la información, está siendo apoyada por el Ministerio de Defensa, a través de semilleros, económicamente y con profesionalización, pues este sistema en nuestro país, ha evolucionado notablemente y es así como se han adquirido nuevas y mejores tecnologías, en pro de las Fuerza Militares, a través del Comando Conjunto Cibernético, encargado de la defensa en el ciberespacio y la Policía Nacional de la seguridad ciudadana, en razon, a que son estas entidades las encargadas activamente, de apoyar los incidentes que se presentan en los activos informáticos y los estratégicos del país, a más de la comisión intersectorial, encargada de proveer la asistencia técnica de los dispositivos inteligentes y electrónicos, equipando, entre otras cosas, el desarrollo de capacidades operativas, la información de inteligencia cibernética y la capacidad de inteligencia de nuestras Fuerza Militares, para de esa forma, apoyar y asesorar en la ciberdefensa al COLCERT.

El COLCERT, recordemos que se creó para coordinar a nivel nacional, todo lo que se relaciona con la seguridad informática, de conformidad con las políticas para la ciberdefensa y ciberseguridad, creciendo de tal forma, que ha fortalecido las diferentes capacidades que tiene la fuerza pública, es así como la ciberdefensa, está a cargo del Comando Cibernético, apoyado por las fuerzas militares y la Policía Nacional, a cargo de la seguridad de la información de la ciudadanía.

Se debe entender que la Armada Nacional, como tal, hace parte del Comando Conjunto Cibernético, COCOCI, **(Resolución Ministerial No. 7436 de 2012. Ministerio de Defensa de Colombia Documento Reservado),** apoyando en debida forma y de acuerdo a la experiencia, a los estudios e investigaciones que ha adquirido y realizado, así mismo, forma parte activa del COLCERT, el cual en este momento ha adquirido las siguientes capacidades:

Capacidad de análisis y fuga de información.

Protegiendo, direccionando y respaldando la información de acuerdo a las necesidades de cada institución, brindando apoyo y capacitando a la Unidades Militares, de policía y a entidades civiles y a través de la generación de doctrina para la Protección de la Información: Da lineamientos para establecer, mantener y actualizar los controles de protección en lo referente a la protección de la información.

Capacidad de búsqueda y recolección de Información.

Creando, manteniendo y actualizando la base de datos de los potenciales riesgos que tiene la información. Buscando y recolectando a través de las técnicas que se utilizan por la amenaza para vulnerar los sistemas de información de las instituciones públicas y los activados estratégicos del país; de igual manera, apoya a las entidades públicas, a las empresas privadas y a los activos estratégicos de la nación en caso de incidentes de seguridad con la información y activos automatizados. Establece, además, una metodología de cómo se realiza un ataque y así mismo crear una línea base. para capacitar al personal de las instituciones y empresas privadas en la protección de los activos informáticos, es decir, en caso que se presente un ataque, crear un perfil único del atacante y de esta forma lograr su

neutralización en tiempo, modo y lugar, estableciendo una metodología de la forma como se realiza un ataque, capacitando al personal de las diferentes entidades públicas y privadas en la protección de dichos activos informáticos.

Capacidad de planificación, ejecución y mitigación

Se crea para minimizar los riesgos en la investigación informática, actualizando las normas y políticas de seguridad y protección de la información a través de las normas técnicas internacionales, mediante las cuales se establecen los estándares, los protocolos procedimientos y los respectivos procesos, protegiendo la información y de esta manera se sensibiliza a los ciudadanos en general, involucrando a los funcionarios de empresa públicas y privadas en el uso de la información, generando cultura de seguridad informática en todos los entes involucrados.

Razon por la cual, es importante la implementación de las diferentes herramientas, software y hardware informáticos, para que a través de ellos se pueda mitigar y minimizar la ocurrencia de incidentes en la información y en los activos estratégicos informáticos

Capacidad de análisis y control

En esta capacidad se deben tener en cuenta el uso de las normas referentes al análisis de los sistemas de información, para de esta forma, controlar que los activos informáticos sean usados de manera adecuada y para el fin establecido de acuerdo a los lineamientos del CONPES 3701, implementando, alimentando y actualizando, las estadísticas de incidentes informáticos. El cumplimiento y protección de las políticas de seguridad que se han creado,

se deben verificar, por medio de las inspecciones de seguridad de la información y su integridad, confidencialidad y la confiabilidad de dichos sistemas, al igual que los backups de la información en caso que se presente una crisis

Es decir, que las fuerzas militares, como una fuerza conjunta e independiente, realiza operaciones conjuntas, tendientes a ejecutar actividades electromagnéticas del ciberespacio, casi siempre, en coordinación con entes multinacionales, interinstitucionales, gubernamentales o no, durante todo el desarrollo operacional. Es así como cada componente, tiene operaciones propias del ciberespacio, necesidades del espectro electromagnético y capacidades de guerra electrónica, en pro de unificar y sincronizar en forma integral sus conocimientos, garantizando el propósito, que estas operaciones del ciberespacio y de guerra electrónica, sean conjuntas, y se dispongan en forma coordinada con las de información, las del ciberespacio, las de guerra electrónica, las de gestión del espectro y las de doctrina.

Si bien es cierto, que los métodos de operaciones del ciberespacio y de guerra electrónica son complejos y van evolucionando a medida que avanza la tecnología, también es cierto, que las Fuerzas, como es el caso de la Armada Nacional, la cual está preparada y es capaz de enfrentar la guerra que se avecina a su llegada, con capacidad de lucha; en este momento, debe capacitar al personal de sistemas, para que estos sean competentes en el uso de las herramientas, los sistemas y los procesos de guerra ciberespacial, coordinando todas sus capacidades necesarias para ejecutar las operaciones de prevención y desarrollarlas en forma eficaz, en un momento oportuno. Es indiscutible, que en la guerra se pueden presentar desafíos únicos, como es el caso que el personal entrenado a más, de su capacidad física,

requiera el uso de otras herramientas como teléfonos o medios virtuales; que se presenten limitaciones en las operaciones del ciberespacio y de guerra electrónica, debido a las leyes existentes o políticas a seguir o reglamentos; en razon, a que algunas operaciones, para pruebas, capacitaciones o mantenimiento, pueden exigir aditamentos especiales.

La Armada Nacional, a través de la Jefatura de Inteligencia, ha adoptado estrategias, para realizar inteligencia naval en ambientes marítimos, navales y fluviales, de conformidad con lo normado en objetivos y políticas propias, encontrando oportunidades de desarrollo en pro de la defensa y seguridad del país, como así mismo, de la Armada Nacional.

La Armada Nacional, por intermedio de la Jefatura de Inteligencia Naval, y a través de recursos técnicos y humanos, ha conseguido tener acceso, de alta calidad, en forma oportuna y confiable a información, siendo elaborada y desarrollada por parte de la Inteligencia Naval, poniéndola a disposición de la Fuerza, materializándose positivamente en resultados operacionales de alto nivel.

Con las nuevas tecnologías y la incursión de delitos cibernéticos, han hecho que la defensa y seguridad tengan nuevos retos de guerra como el ciberespacio, logrando, que la Armada Nacional, realice adelantos importantes de ciberseguridad, ciberdefensa y ciberinteligencia, aumentando de esta forma, sus capacidades de detención, gestión y análisis de sucesos e incidentes cibernéticos, en la red de datos dentro de la Armada Nacional. Como consecuencia de ello, se creó el Centro de Operación de

Seguridad (SOC) y el Sistema de Información de Gestión de Eventos (SIEM), fortaleciendo en gran manera, la capacidad de respuesta, ante las incidencias de orden cibernético.

Como consecuencia de los avances de los ataques cibernéticos a diferentes entidades públicas y privadas, la Armada Nacional, puso en práctica un sistema de monitoreo y protección cibernético mediante el Sistema de Detección de Intrusos a nivel de host; igualmente, considero necesario, ejercer una mayor protección de la infraestructura critica cibernética (ICC) naval, fortaleciendo el Sistema Integrado de Control de Tráfico y Vigilancia Marítima (SICTVM) y las unidades de flote.

De la misma manera, la Armada Nacional, en tratándose, de las amenazas cibernéticas, logro ratificar la situación real de la seguridad cibernética en varias unidades v de las redes institucionales, con la puesta en práctica de "pruebas de penetración, análisis y escaneo de vulnerabilidades" para tener un conocimiento directo del estado y de la conciencia situacional de las unidades.

Igualmente, se han puesto en práctica lineamientos de seguridad naval, para prevenir el uso de situaciones con aeronaves no tripuladas (RPAS), vehículos aéreos no tripulados (VANT), llamados drones, que sean avisados en prácticas y en sobrevuelos nocturnos, sin autorización sobre las estructuras y unidades de la Armada Nacional, para que no haya espionaje, sabotaje, fuga de información o el peor de los casos, atentados contra las instalaciones o contra el personal de la Fuerza.

3. PROPONER RECOMENDACIONES PARA LA IDENTIFICACIÓN Y FORTALECIMIENTO DE LAS CAPACIDADES CIBERNÉTICAS DE LA ARMADA DE COLOMBIA

Dentro de este objetivo, se debe tener en cuenta que varias entidades han puesto empeño en crear guías, manuales para llevarse a cabo protocolos en la gestión de los ciberriesgos marítimos, entre ellos el Comité de Seguridad Marítima de la Organización Marítima Internacional, reconociendo que en el sector marítimo, ocurren riesgos que afectan de una manera directa, la ciberseguridad marítima, que pueden producir impactos operacionales y de seguridad en organizaciones y buques; por tanto y de acuerdo con dicha organización, existe una dependencia de las tecnologías de la información para las operaciones de las organizaciones de transporte marítimo y sus buques, la cual se ocupa primordialmente de la seguridad física y de operaciones; siendo por tanto, la gestión de riesgos fundamental en las operaciones seguras del transporte marítimo.

De acuerdo con la Organización Marítima Internacional, existen en los buques, unos sistemas que son vulnerables y que se ven afectados, en caso de producirse un ciber ataque, algunos de esos sistemas son: Del puente, de manipulación y gestión de la carga, de propulsión y gestión de las máquinas y de control de suministro eléctrico, de control de acceso, de servicio a los pasajeros y de organización de los mismos, de redes públicas para los pasajeros, administrativos y de bienestar de la tripulación y de comunicación, siendo este último sistema el más importante, en tratándose de las amenazas cibernéticas.

Así las cosas, es necesario traer a colación que cada país es responsable de brindarle a sus ciudadanos unas funciones mínimas, para garantizarles sus necesidades básicas, de defensa y que ellos puedan vivir en armonía y tranquilidad, ya sea en forma directa o a través de entidades que de manera coordinada puedan delegarle esas funciones, para que cumplan con el fin propuesto por el Estado, es así como una de esas funciones, se traduce en la seguridad y defensa, implementando un a infraestructura sólida, de gestión, de respaldo y que la misma quede plasmada dentro del plan de políticas públicas, siendo estas llamadas Infraestructuras críticas de la información y comunicación, según Linares (2018).

Estas infraestructuras se encuentran plasmadas en diferentes sectores, públicos y privados, como son la de seguridad y defensa nacional, de administración del estado, industrias como la nuclear, la militar, la petroquímica, la de integración y desarrollo, etc.

Como lo hemos mencionado, cada Estado ha creado una variedad de estrategias frente a las amenazas y en relación, al Sistema de Ingeniería y Navegación, para fortalecer en forma colectiva, un modelo de seguridad cibernética, direccionando sus planes en pro de la defensa cibernética.

En consecuencia, de lo anterior, la Organización Marítima Internacional, para direccionar los riesgos de ciberseguridad en las compañías y buques, ha señalado cinco elementos funcionales, que deberían ser puestos en práctica en forma permanente y unificados, estos son: Identificar, Proteger, Detectar, Responder y Recuperar. Textualmente estos elementos son definidos así:

1. “Identificar: definir las funciones y responsabilidades del personal en la gestión de los riesgos cibernéticos, e identificar los sistemas, activos, datos y capacidades que, si se interrumpen, plantean riesgos para las operaciones de los buques.
2. Proteger: implantar procedimientos y medidas para el control de los riesgos, así como planificación para contingencias, a fin de proteger ante cualquier suceso cibernético y garantizar la continuidad de las operaciones del transporte marítimo.
3. Detectar: crear las actividades necesarias para detectar un suceso cibernético oportunamente.
4. Responder: crear e implantar actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones o servicios de transporte marítimo que hayan sido afectados por un suceso cibernético.
5. Recuperar: determinar medidas para copiar y restaurar sistemas cibernéticos necesarios para las operaciones de transporte marítimo que hayan sido objeto de un suceso cibernético.”

Con estos elementos funcionales y las medidas que se incorporan en ellos, se está asegurando que se lleve a cabo, una acción segura y eficaz de las amenazas cibernéticas. Estos elementos no son sucesivos y en la práctica deberían presentarse sincronizados y simultáneos, para que de esta forma integren un campo en la gestión de los riesgos.

En consecuencias, estos elementos funcionales contienen todas las acciones y los frutos deseados de una gestión positiva, frente a las amenazas cibernéticas, a todos los procedimientos decisivos que afectan todas las actividades marítimas y a la interrelación de

la información, constituyendo un desarrollo continuo con estructuras prácticas y reales de retroalimentación.

Las gestiones positivas de las amenazas cibernéticas, deben asegurar una categoría de conocimiento idóneo sobre los riesgos cibernéticos en todos los campos de una organización. El campo de conocimiento y preparación debe ser el idóneo y eficaz para las funciones y compromisos del sistema de gestión de los riesgos y de las amenazas cibernéticas.

De acuerdo con la OMI (2016) la guía BIMCO, utiliza cuatro pasos, desde una óptica coherente, para la gestión de riesgos de ciberseguridad en buques, estos son: comprender las ciber amenazas, evaluar y reducir el ciberriesgo, y por ultimo desarrollar planes de contingencia. Indicando que la guía BIMCO, contiene una variedad de controles que considera importantes para la ciberseguridad a bordo de buques, textualmente, estos son: "Limitación y control de puertos de red, protocolos y servicios, Configuración de dispositivos de red como cortafuegos, enrutadores y conmutadores y Configuración segura de hardware y software, Protección de navegación web y correo electrónico, Comunicaciones por satélite y radio, Control de redes inalámbricas y Seguridad en las aplicaciones, Diseño de red seguro, Seguridad física y Defensas perimetrales"

Existen igualmente, en la guía BIMCO, planes y protocolos, que hacen referencia a controles procedimentales para el uso de los sistemas de a bordo por la tripulación, entre otros: formación y conocimientos, mantenimiento de software y actualizaciones, actualizaciones de anti-virus y uso de privilegios de administrador (OMI, 2016).

De la misma manera, la guía OMI (2016) contiene el estándar ISO 27001 de gestión de ciberseguridad. Desde este punto de vista, plantea los estándares de ciberseguridad ISO 27000, siendo aplicable a cualquier organización, siendo reconocidas en el sector de la ciberseguridad. (Guía OMI ciber-riesgo y NIST CSF.

En el mismo sentido, la guía OMI (2016) contiene un plan de ciberseguridad, así, en la guía NIST CSF (2014) trae una perspectiva para la gestión de la ciberseguridad en Infraestructuras Críticas IICC y, por consiguiente, se ajusta a los rasgos que corresponden al sector del transporte marítimo. Por tanto, los cinco elementos funcionales, que recomienda la OMI (2016) para la gestión del riesgo son los establecidos en la guía NIST CSF (2014), cuyo objetivo principal, en cuanto a ciberseguridad se refiere, es colaborar con las organizaciones, en varios elementos, textualmente: “Describir la situación actual en ciberseguridad. Definir la situación requerida como objetivo en ciberseguridad. Identificar y priorizar oportunidades de mejora mediante un proceso continuo. Evaluar el progreso de la organización hacia el objetivo en ciberseguridad. Comunicar a las partes interesadas dentro y fuera de la organización los riesgos relevantes en ciberseguridad.”

En ese mismo orden de ideas, se tiene que las amenazas cibernéticas se dan de dos clases, y para que la gestión de los riesgos sea exitosa, se deben tener en cuenta dichas amenazas:

- Se da como consecuencia del mantenimiento inapropiado que se hace a los programas informáticos.

- A través de la piratería informática, introduciendo programas informáticos maliciosos, entre otros.

La vulnerabilidad, se puede dar como consecuencia de un plan, integración o el mantenimiento inapropiado del sistema, como es el caso de las contraseñas poco seguras, que son en forma directa o indirectas como, el no existir separación de redes, traduciéndose estas en consecuencias graves en la protección, confidencialidad, integridad y disponibilidad de la información.

En el caso de la Armada Nacional, se pueden poner en peligro sistemas importantes y de alta complejidad, como es el caso, por ejemplo, de algunos sistemas necesarios de propulsión o de la navegación en el puente, cuando se da alguna vulnerabilidad de la tecnología operacional o de la información, esto debido a una conexión inapropiada a los sistemas de tecnología inapropiada, o errores que se hayan presentado en los funcionarios que operan el sistema o por terceras personas.

Debido a los cambios frecuentes de la tecnología y de la variedad de amenazas, se hace más compleja la forma de enfrentar los riesgos, no solo a través de normas técnicas, sino de carácter operacional, pues se aconseja seguir un plan para enfrentarlos, que debe ser el que ofrezca más invulnerabilidad en tecnología y de una mayor transformación, para ofrecerles seguridad y protección, por esa razon, las organizaciones, entidad, empresas, deben analizar diferentes mecanismos de control para disminuir los riesgos cibernéticos, estos mecanismos

o controles, podrían ser: de gestión, operacionales o de procedimiento y técnicos. **.** (OMI, 2017)**.**

En este punto, y como consecuencia de los resultados obtenido, se hace necesario, presentar una proposición militar, para llevar a cabo el desarrollo de las capacidades cibernéticas de todas las Fuerzas Militares, basada en la norma de planeamiento por capacidades, denominada: Doctrina, Organización, Material, Personal, Infraestructura, Liderazgo, Entrenamiento, Mantenimiento (DOMPILEM), permitiendo plasmar, capacidades en la demostración operativa indispensable para afrontar las recientes amenazas cibernéticas

En el mismo sentido y para capacitar el personal adscrito a las fuerzas militares, que deben enfrentar los riesgos frente a las amenazas que se presentan, existen algunas convergencias, importantes entre la DICIB, el Ministerio de las TIC, el Ministerio de Defensa Nacional, las unidades Cibernéticas de las FF.MM. y la Armada de Colombia.

De otro lado, se requiere a más de la capacitación del personal, que existan, leyes, que se puedan sancionar para obtener un marco legal, acorde con los ilícitos cibernéticos, desarrollando el marco legal para esta clase de riesgos cibernéticos, en unión de todas las fuerzas, organizaciones e identidades, para presentar iniciativas ante el Congreso de la Republica y el Ministerio de Defensa, pues son estos actores, los que impiden llevar a buen recaudo, los planes y las estrategias, necesarios para fortalecer ejercer una ciberdefensa, exitosa y segura, en razon a que es el Ministerio de Hacienda, quien debe proveer a la

Armada Nacional de un buen presupuesto y de esta forma fortalecer sus capacidades cibernéticas, toda vez que es un actor potencialmente fuerte, pues ha puesto todas sus capacidades, frente al aumento de las acciones de los grupos hacktivistas y los ataques por parte de las APT.

Finalmente, son varias las recomendaciones que se pueden hacer, en pro de una ciberdefensa segura, ágil y exitosa y que se ha evidenciado a lo largo de este capítulo, para citar algunas de ellas, se hace necesario:

- En primer lugar, se debe analizar y realizar un estudio, en el cual, evalúe la Armada de Colombia, cuales acciones son inherentes a ella y cuáles no, cuales se deben priorizar, dándoles un valor de importancia y gobernabilidad, para ejercer acciones en favor de una ciberdefensa exitosa, frente a la delincuencia del ciberespacio
- Aumentar el nivel de sinergia entre los Ministerio de Defensa, las TIC, COLCERT, CCOCI y unidades cibernéticas de la FF.MM. y de policía, presentando proyectos de ley e iniciativas de uso del ciberespacio, o modificando alguna de ellas, como es el caso de la Ley de Inteligencia.
- Implementar un plan de carrera, de cursos avanzados, para el personal de la Armada, que está a cargo de operaciones cibernéticas y en general, para todas las unidades de la Armada, en forma obligatoria, como también de capacitaciones de actualización en esta materia.
- Crear un plan o manual, donde se consignen en él, todas las acciones y estrategias de ciberdefensa, frente a las amenazas cibernéticas, por parte de la Armada Nacional.

- Realizar y desarrollar, un sistema de intercambio de información de amenazas cibernéticas como la plataforma MISP.

Nos encontramos, pues, dentro de un nuevo escenario estratégico en el que la política de seguridad demanda planteamientos novedosos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad de adaptación de las Fuerzas Armadas a las circunstancias de cada momento.

VI. CONCLUSIONES

Es de anotar, que a la par de los avances a nivel tecnológico, se han desarrollado vulnerabilidades, colocando en peligro la seguridad de la información, soportada al interior de las Fuerzas Armadas, entidades del control y por supuesto, al mismo Estado, es así, la Armada Nacional, tiene una infraestructura naval, en la cual realiza operaciones en defensa de la nación, como es búsqueda y rescate, ayudas humanitarias y control del espacio marítimo colombiano, pero también debe enfrentar, amenazas de diferentes clase, a manera de ejemplo, migración de personas, tráfico ilegal de sustancias ilícitas, pesca ilegal, etc., consiguiendo por esta razon, importantes descubrimientos, en relación a la ciberseguridad y ciberdefensa, desarrollando sus capacidades de detección, gestión y análisis de eventos e incidentes cibernéticos en su red de datos, creando como consecuencia el Centro de Operación de Seguridad (SOC) y el Sistema de Información de Gestión de Eventos (SIEM), reforzando, ante los riesgos cibernéticos, su capacidad de respuesta, logrando que exista una mejor protección a la Infraestructura Critica Cibernética Naval (ICCN), como por ejemplo, brinda una protección mayor, a las unidades a flote y al Sistema Integrado de Control de Tráfico y de Vigilancia Marítima (SICTVM) de la Armada Nacional

Para los sectores, político, social, económico, el ciberespacio, se convierte en una carga que da perdidas, al no ser, un área segura, por no estar protegido, frente a los ilícitos cibernéticos, es vulnerable, se convierte en una amenaza latente, para la defensa nacional, siendo una prelación, la Seguridad y Defensa de Colombia, por lo que es necesario realicen

capacidades en el ciberespacio, con resultados veraces, agiles y contundentes, en forma organizada y con el apoyo de organizaciones de todos los sectores y en forma mancomunada, con todas las fuerzas, para afrontar las amenazas que se presentan en contra de la ciberdefensa de nuestro país, planteándose un modelo basado en estrategias puntuales, con referencia del modelo DOMPILEN, delimitando las capacidades de todas las Fuerza Militares, a fin de realizar capacidades militares en operaciones cibernéticas. En este sentido, y de acuerdo al avance de la tecnología y al crecimiento de los riesgos cibernéticos, la Ciberdefensa, es primordial, e involucra diferentes actores, siendo la base fundamental las Fuerzas Militares, para que sean ellas quienes enfrenten el quinto dominio de la guerra: el ciberespacio.

Para combatir los actores que cometen ilícitos cibernéticos, a más de las penas normadas en el Código Penal, se han establecido, la incautación de activos (automóviles, barcos, dinero en efectivo, acciones, etc.,) embargos de bienes inmuebles inmuebles, la confiscación del producto del ilícito, son fundamentales, para que los delincuentes se beneficien, de la delincuencia organizada transnacional. Para combatirlos y que se hagan enjuiciamientos eficaces, a estos delincuentes por los ciberdelitos, se han creado técnicas especiales de investigación, con el fin de que se ejerza vigilancia electrónica, que se desarrollen operaciones encubiertas, siendo una herramienta necesaria, para combatir la ciberdelincuencia organizada, siendo primordial los conocimientos especiales y la utilización de instrumentos tecnológicos avanzados, como la vigilancia electrónica a través del uso de las TIC para interceptar, especialmente, comunicaciones.

Podemos concluir, que globalmente existen innumerables descubrimientos, en cuanto a las comunicaciones y la tecnología se refiere, eso ha permitido que se pruebe la necesidad y adicción frente al área de la cibernética y las comunicaciones, a través del conocimiento y la innovación. Por eso algunas definiciones, en relación con las infraestructuras críticas, el ciberespacio y las múltiples amenazas que se desprenden de éste, han logrado que se desarrolle, aún más el conocimiento en relación con la cibernética, produciendo una conciencia en la seguridad digital, sacando la mejor ventaja al ciberespacio y dando la oportunidad de percibir la variedad de riesgos, que pueden conllevar, por ignorancia o malas prácticas en su empleo

Para la Armada de Colombia, es importante desarrollar su capacidad naval, en sus dominios físicos, como lo son tierra, agua, aire y espacial, y en la misma forma el dominio cibernético, por la cantidad de amenazas cibernéticas, que se encuentran a nivel global, los cuales han sido realizados por actores del estado y no estatales, a través del ciberespacio, en razon a que crecimiento de capacidades probables, son el fundamento de la estrategia de la disuasión, siendo uno de los elementos, consagrados en la estrategia del poder e importante dentro existencia de las diferentes armadas del siglo XXI, globalmente. Razon por la cual, se logró identificar, varias características primordiales, que hacen parte de la disuasión, como es la percepción de intenciones, de capacidades y como elemento importante, textualmente, “la credibilidad”, es decir, cada actor que disuade debe ser creíble, siendo este el obstáculo primordial para lograr la ciberdisuasión.

Dentro de este capítulo, se pudo establecer ciertas estrategias, recomendables para la Armada Nacional, que se pueden llevar a la práctica y de esta manera aumentar la apreciación de credibilidad, generando una mejor y mayor ciberdusacion, para el desarrollo de su nivel operacional, las cuales son necesarias para ejecutar estrategias de ciberdusacion creíbles y exitosas, estas son: Realizando un estudio, en el cual, evalúe la Armada de Colombia, cuales acciones son inherente a ella y cuáles no, cuales se deben priorizar, dándoles un valor de importancia y gobernabilidad, para ejercer acciones en favor de una ciberdefensa exitosa, frente a la delincuencia del ciberespacio, aumentar el nivel de sinergia entre los Ministerio de Defensa, las TIC, ColCERT, CCOCI y unidades cibernéticas de la FF.MM. y de policía, presentando proyectos de ley e iniciativas de uso del ciberespacio, o modificando alguna de ellas, como es el caso de la Ley de Inteligencia, implementar un plan de carrera, de cursos avanzados, para el personal de la Armada, que está a cargo de operaciones cibernéticas y en general, para todas las unidades de la Armada, en forma obligatoria, como también de capacitaciones de actualización en esta materia, crear un plan o manual, donde se consignen en él, todas las acciones y estrategias de ciberdefensa, frente a las amenazas cibernéticas, por parte de la Armada Nacional, realizar y desarrollar, un sistema de intercambio de información de amenazas cibernéticas como la plataforma MISP.

Así mismo, es primordial, establecer un modelo especial, de los diferentes planes de carrera y de capacitación para todo el personal, al interior de cada una de las instituciones, permitiendo fortalecer los mecanismos defensivos en Ciberdefensa y Ciberseguridad al interior de nuestro país.

De lograrse realizar esas estrategias, se fortalecerá aún más el poder naval que tiene la Armada Nacional, frente a las capacidades cibernéticas y en desarrollo de las mismas en forma contundente, en la utilización del ciberespacio, conllevando a que exista mayor conciencia digital dentro de la misma Fuerza, para de esta forma desarrollar sus capacidades frente a las nuevas tecnologías, utilizadas por los grupos hacktivistas, que a través del espacio buscan amenazar las Infraestructuras Criticas Cibernética Navales (ICCN),a cargo de la Armada Nacional.

La Estrategia de Ciberdefensa y Ciberseguridad establece los lineamientos para desarrollar capacidades ofensivas, defensivas, disuasivas y de inteligencia para la protección del Estado, definiendo estándares y compromisos para asegurar el manejo de la información digital como una forma de gestionar y mitigar el riesgo frente a un ciberataque, manteniendo la capacidad de resiliencia para responder, recuperar y restaurar las áreas afectadas.

Por lo tanto, la Estrategia se centra en la integración, interacción y cooperación entre el sector público y privado de manera transversal, comprometiendo todos los campos político, económico, sicosocial y militar. Integra aspectos legales y estratégicos y la coordinación internacional con énfasis en dos áreas: tecnológico y judicial. Define riesgos, amenazas y desafíos; traza un límite no superior al 2024 para el desarrollo de la industria digital nacional y la gobernanza del internet, teniendo en cuenta los cinco pilares establecidos por la Unión Internacional de Telecomunicaciones: medidas legales; medidas

técnicas; medidas organizacionales; capacidades de construcción y desarrollo; y medidas de cooperación.

Así mismo, se considera de vital importancia establecer el diseño específico de los diferentes planes de carrera y de capacitación al interior de cada una de las instituciones, lo que finalmente, nos permitirá fortalecer los mecanismos defensivos en Ciberdefensa y Ciberseguridad en nuestro país.

Desde otro punto de vista, es necesario hablar de las metas que tiene el COMANDO GENERAL DE LAS FFMM, en razon a que estas se encuentran plasmadas, una a una, y con preocupación se observa que en ellas no está contenida, en forma taxativa, ninguna referente a la defensa y seguridad del ciberespacio, como cuarto componente; haciéndose necesario, recomendar el fortalecimiento y hacer énfasis en la capacitación, que se le debe hacer al personal de las fuerzas, para que en su momento y dada la clase de amenaza que se presente, puedan llevar a feliz término, una operación determinada en defensa, no solo de la soberanía del estado, sino de la población en general.

Estas metas son:

1. “Consolidar a nuestras Fuerzas Militares como las más preparadas de Latinoamérica.
2. Fortalecer las campañas de transparencia institucional, cero tolerancias con la corrupción.

3. Contribuir decisivamente a la consecución de la paz total, mediante el desarrollo de operaciones militares y el acompañamiento a la intención política sobre el conflicto.

4. Desarrollar, entender y aplicar la doctrina militar conjunta y apoyar el desarrollo doctrinal de las Fuerzas.

5. Optimizar los procesos del Estado Mayor Conjunto y su sinergia con los Estados Mayores de las Fuerzas, con una vocación eminentemente operacional.

6. Fortalecer los sistemas y metodologías de planeamiento a todo nivel (arte y diseño operacional, proceso militar de toma de dediciones, procedimiento de comando, metodología de diseño de Fuerza).

7. Respeto por los Derechos Humanos, las leyes y normas consagradas en el corpus legal del Estado; será una prioridad de este Comando.

8.Satisfacer las necesidades básicas del soldado y velar por su desarrollo integral (personal y profesional).

9.Preservar los valores y tradiciones militares.

10. Los principios, la ética, el honor y los valores institucionales guiarán el actuar de todos los miembros de la institución.

11. Velar por el respeto a los veteranos y reservas de las Fuerzas Militares, dando cumplimiento a la ley 1979 del 2019.

12. Articular las competencias distintivas de cada Fuerza, aprovechando sus capacidades en pro de la conjuntes.

13. Velar por una verdadera equidad de género.

14. Potenciar los sistemas de ciencia y tecnología de cada Fuerza.

15. Modernizar las Fuerzas desde los componentes de capacidad.

16. Preservar la historia y la memoria histórica institucional.

17. Cumplir cabalmente el proceso de las operaciones de acuerdo a la doctrina de cada Fuerza, en especial la evaluación.

18. Contribuir al desarrollo de los 7 componentes de la seguridad humana (Seguridad económica, seguridad alimentaria, seguridad sanitaria, seguridad medioambiental, seguridad personal, seguridad comunitaria y seguridad política) en el marco de la Acción Unificada del Estado.

Una vez, puestas en conocimiento dichas metas, podemos identificar la primera, (Consolidar a nuestras Fuerzas Militares como las más preparadas de Latinoamérica.) la cuarta (. Desarrollar, entender y aplicar la doctrina militar conjunta y apoyar el desarrollo doctrinal de las Fuerzas) y la catorceava, (. Potenciar los sistemas de ciencia y tecnología de cada Fuerza.), las cuales hacen referencia, si bien, no en forma taxativa, a acciones a desarrollar, como se dijo, del cuarto componente, sí las podemos incluir, medianamente en estas metas, que de forma trasversal están impactando el estado final deseado, de las Fuerzas Militares y por ende de la Armada Nacional.

4. REFERENCIAS

Afanador, G. (13 de julio de 2020). El mundo no está preparado para una CiberPandemia. Itrustconsulting. Obtenido de http://www.itrustconsulting.com/uncategorized/el- mundo-no-esta-preparado-para-una-ciberpandemia/

Aguilar, L. (2011). Introducción. Estado del arte de la ciberseguridad. Cuadernos de estrategia(149),11-46. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3837217

Arias, D. (11 de abril de 2018). Colombia: el sexto país con más ataques cibernéticos en A. Latina. Obtenido de https://www.enter.co/empresas/seguridad/colombia-sexto-pais- ataques-ciberneticos/ Arreolo, A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. doi:https://doi.org/10.25062/1900-8325.212

https://www.armada.mil.co/es/content/descripci%C3%B3n-general#:~:text=La%20Armada%20Nacional%20ejerce%20presencia,los%20intereses%20de%20la%20Naci%C3%B3n.

Barredo, Á. (2017). Tras cinco colisiones en un año, sospechas de ciberguerra en el Pacífico. https://www.eshoy.cl/2019/07/04/la-necesidad-de-establecer-una-estrategia-de-ciber-disuasion/

Cárdenas , W. (junio de 2015). Ciberdefensa y Ciberseguridad en el Sector Defensa de Colombia. Obtenido de http://polux.unipiloto.edu.co:8080/00002590.pdf

Centro de Doctrina del Ejército Nacional de Colombia. (septiembre de 2017). Manual Fundamental de Referencia del Ejército MFRE 1-02. Términos y Símbolos Militares. Obtenido de https://www.dipor.co/%7CDoctrina%20Publica%7C/2%20Ejercito%20Nacional/Manuales/MFRE%201-02%20TERMINOS%20Y%20SIMBOLOS.pdf

Cyber Wars: A Paradigm Shift from Means to Ends». Autor: Amit Sharma, del Institute for System Studies and Analysis» del Ministerio de Defensa de la India. Juan Díaz del Río Durán

Cbueger, C., Liebetrau, T. & Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. Policy Department for External Relations. European Parliment.. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf-

Clarke, R., & Knake, R. (2010). Cyber war: The next threat to national security and what to do about it. (H. Collins, Ed.)

Consejo Nacional de Política Económica y Social, República de Colombia, & Departamento Nacional de Planeación. (11 de abril de 2016). Documento CONPES 3854. Política Nacional

de Seguridad Digital. Obtenido de https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=

Crawford, J. (2019). Ciberataque al transporte marítimo ¿Amenaza real o ciencia ficción?

Del Castillo, C. (2022). Rusia podría lanzar un ataque contra la infraestructura global de Internet, como los cables submarinos, sin verse afectada por las consecuencias. elDiarioAR. https://www.eldiarioar.com/mundo/rusia-lanzar-ataque-infraestructura-global-internet-cables-submarinos-verse-afectada-consecuencias_1_8769494.html

Departamento Nacional de Planeación. (julio de 2020). CONPES 3995. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Department of Defense Dictionary of Military and Associated Terms. (2016). Joint Publication 1-02. Obtenido de https://fas.org/irp/doddir/dod/jp1_02.pdf

Diálogo-Américas (2022). Guerras de cables submarinos: La competencia por el control de las redes hace aflorar los riesgos de seguridad a largo plazo. https://dialogo-americas.com/es/articles/guerras-de-cables-submarinos-la-competencia-por-el-control-de-las-redes-hace-aflorar-los-riesgos-de-seguridad-a-largo-plazo/

Díaz, H. (2018). Infraestructura crítica vulnerable a la ciberguerra. En Centro de Estudios Estratégicos CEEAG,

Doffman, Z. (06 de may de 2019). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. Obtenido de https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and- destroys-hamas-cyber-hq-in-world-first/#14891939afb5

Escuela Superior de Guerra. (2017). Escenarios y Desafíos de la Seguridad Multidimensional en Colombia. Bogotá: Ediciones ESDEGUE.

Ganga, R. (1984). La Disuación. Obtenido de https://revistamarina.cl/revistas/1984/5/ganga.pdf

Ganuza, N. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. Cuadernos de estrategia(149), 165-214. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3837337

Galán, J. (2021). Los riesgos (y el valor estratégico) de los cables submarinos. CincoDías. https://cincodias.elpais.com/cincodias/2021/10/11/opinion/1633954196_539682.html

Gazapo, M. (21 de Marzo de 2018). Ciberespacio: Inseguridad, Carrera de Armamentos y Disuasión en el Siglo XXI. Obtenido de https://www.universidadviu.com/ciberespacio-inseguridad-carrera-armamentos- disuasion-siglo-xxi/

Godet, M., & Durance, P. (2009). La prospectiva estratégica para las empresas y los territorios. Cuaderno del Lipsor. Obtenido de https://administracion.uexternado.edu.co/matdi/clap/La%20prospectiva%20estrateg ica.pdf

Gómez, D. A. (2017). Análisis del Ciberataque para la Seguridad de los Estados y su Incidencia en la Transformación del Status Quo: Stuxnet el Virus Informatico. Obtenido de https://repository.urosario.edu.co/bitstream/handle/10336/13705/GomezLlinas-DanielAlejandro-2017.pdf?sequence=5

Gómez, Á. (2011). El ciberespacio factor transversal en los "Global Commons".

https://www.wired.co.uk/article/satellite-constellations

https://atalayar.com/blog/el-ciberespacio-en-la-guerra-de-ucrania

1&isAllowed=y

Kello, L. (2017). *The virtual weapon and international order*. New Heaven, CT. Yale University Press.

La Vanguardia. Obtenido de https://www.lavanguardia.com/tecnologia/20170826/43795922582/marina-eeuu- gps-ciberguerra-pacifico.html

La Ciberguerra: Sus Impactos y Desafíos (págs. 45-58). Santiago de Chile: Centro de Estudios Estratégicos CEEAG.

La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas, 697-708. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3887810

Revista Marina(970), 15-23. Obtenido de https://revistamarina.cl/revistas/2019/3/jcrawfordc.pdf

Sherman, J. (2021). Cyber defense across the ocean floor: The geopolitics of submarine cable security. Atlantic Council Report. https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

The Fourth Industrial Revolution, by Klaus Schwab | World Economic Forum. Recuperado marzo 11, 2018, de https://www.weforum.org/about/thefourth-industrial-revolution-by-klaus-schwab

Triana, R. E. (2015). Intereses Geopolíticos de Colombia. Estudios en Seguridad y Defensa. 10(19), 71-86. https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/69