Estrategia militar de ciberdefensa para las fuerzas militares de Colombia de cara a las amenazas cibernéticas que imponen las tecnologías disruptivas al 2022

Milena Elizabeth Realpe Díaz

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

ESTRATEGIA MILITAR DE CIBERDEFENSA PARA LAS FUERZAS MILITARES DE COLOMBIA DE CARA A LAS AMENAZAS CIBERNÉTICAS QUE IMPONEN LAS TECNOLOGÍAS DISRUPTIVAS AL 2022

ALUMNO: MY. MILENA ELIZABETH REALPE DÍAZ

DIRECTOR: DR. JEIMY JOSÉ CANO MARTÍNEZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

Estrategia Militar de Ciberdefensa para las Fuerzas Militares de Colombia de cara a las amenazas cibernéticas que imponen las tecnologías disruptivas al 2022

Mayor Milena Elizabeth Realpe Díaz

Director

Doctor Jeimy José Cano Martínez

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de grado

Bogotá – Colombia

2019

Nota de aceptación:

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., septiembre de 2019

Agradecimientos

Agradecimiento a Dios, por permitirme alcanzar una meta más, a mi esposo y mis hijos por su apoyo incondicional y los sacrificios realizados por amor.

Agradecimiento al Ministerio de Tecnologías de la Información y las Comunicaciones, por el apoyo económico y por pensar en el bienestar tecnológico del país.

Agradecimiento a las Fuerzas Militares y especialmente al Ejército Nacional por todas las oportunidades brindadas para capacitarme en este tema tan apasionante.

Agradecimiento a la Escuela Superior de Guerra, alma mater de este excelente programa.

Agradecimiento al asesor de este trabajo de grado, a mi gran amigo, Jeimy José Cano Martínez, gracias por tus aportes, consejos, por tu conocimiento y experiencia.

Resumen

La Constitución Política de Colombia, en el artículo 217 establece que la Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional, así como los intereses nacionales sin hacer distinción alguna de los dominios donde debe ejercerlo. Es por esto que, a pesar de que el ciberespacio se constituye en el más nuevo de los dominios de guerra, para sostener estos valores el Estado necesita un sistema complejo o estrategia integral de ciberdefensa basada en una visión a corto, mediano y a largo plazo.

Las amenazas cibernéticas que imponen las tecnologías disruptivas a las Fuerzas de Ley de un Estado, reflejan una tendencia peligrosa a la seguridad y defensa nacional. Para mitigar los riesgos en el ciberespacio se requiere una estrategia integral que permita contrarrestar y, si es necesario, resistir los ataques perturbadores y destructivos. En consecuencia, este documento presenta un análisis general de la situación actual en materia de ciberdefensa en Colombia. Se identifican las amenazas cibernéticas latentes y emergentes, considerando al instrumento denominado la Ventana de AREM, de cara a siete (7) tecnologías disruptivas analizadas por el Instituto Tecnológico de Massachusetts a corto plazo, con el fin de proponer una estrategia militar de ciberdefensa que permita responder a las amenazas cibernéticas con una visión integral, sistémica y prospectiva.

Contenido

Lista de tablas

Lista de figuras

Abreviaturas, siglas y acrónimos

C4ISR: Comando, Control, Comunicaciones, Ciberdefensa, Vigilancia, Reconocimiento.

CCOCI: Comando Conjunto Cibernético.

CESEDEN: Centro Superior de Estudios de la Defensa Nacional.

COARC: Comando Armada Nacional de Colombia.

COEJC: Comando Ejército Nacional de Colombia.

COFAC: Comando Fuerza Aérea Colombiana.

COGFM: Comando General de las Fuerzas Militares.

OCDE: Organización para la Cooperación y el Desarrollo Económico.

OEA: Organización de Estados Americanos.

OTAN: Organización Tratado Atlántico del Norte.

TI: Tecnologías de Información.

TO: Tecnologías de Operación.

Introducción

La globalización y el uso de las Tecnologías de la Información y las Comunicaciones, así como las tecnologías de operación en todas las áreas del conocimiento y la sociedad, traen consigo nuevos retos, escenarios y riesgos en el ecosistema digital. Este escenario genera un espacio propicio para la incubación de amenazas cibernéticas, que pueden poner en riesgo la prosperidad económica y social de un país, así como a su seguridad y defensa nacional.

Dichas amenazas cibernéticas son múltiples y muy variadas, mutan sus vectores de operación en cuestión de segundos. Es una realidad que las "nuevas tecnologías traen oportunidades y vulnerabilidades para los países más desarrollados y al mismo tiempo contribuyen a aumentar la brecha tecnológica hacia los países en vías de desarrollo, especialmente en lo que se refiere a los campos de la seguridad y la defensa nacional" (Ferreira, 2018). Según lo afirma el Capitán de fragata, ingeniero José María Riola Rodríguez en el documento de trabajo 12/2015, *Plan de Investigación Anual 2015, Tecnologías Disruptivas y sus efectos sobre la Seguridad del CESEDEN*, afirma: "En todos los sectores, incluido el de Defensa, la diferencia entre identificar y desarrollar una tecnología disruptiva y no hacerlo, supone un factor de superioridad que puede ser decisorio tanto en una situación de conflicto y constantemente como impacto disuasorio" (CESEDEN, 2015, p 20). Aunado a este comportamiento, los perpetradores de ataques (o adversarios), no descansan en su intento por buscar nuevas y mejores formas de explotación para lograr sus objetivos de manera más fácil y eficiente, creando un escenario complejo y dinámico que debe ser afrontado por las Fuerzas Militares de la forma más adecuada, tanto para anticipar como para evitar que se produzca una afectación a la seguridad nacional.

Se debe agregar que, como lo afirman el autor Schwab y Botín (2016, p. 16), la revolución digital en su esencia, "No cambia lo que hacemos, sino que cambia lo que somos". Esto marca un inicio para repensar y evolucionar el concepto de la defensa nacional al nuevo entorno operacional llamado ciberespacio,[1] con el fin de comprender la dinámica de las vulnerabilidades y los retos ante la nueva revolución industrial.

En este nuevo dominio, es posible que un ataque cibernético realizado a las plataformas tecnológicas que soportan los servicios esenciales brindados a la población debilite o impida la gobernabilidad de un país, imposibilite la prestación de servicios esenciales ocasionando sufrimiento y, en otros casos, la muerte, e incluso desequilibre la economía. Estos hechos en conjunto pueden desestabilizar la seguridad y defensa nacional.

Lo dicho hasta aquí supone que es necesario considerar el ciberespacio como un nuevo escenario de confrontación bélica, que combinado con los poderes de tierra, mar, aire y espacio constituirán una verdadera capacidad y superioridad de cualquier Estado o Nación. En consecuencia, las Fuerzas Militares de Colombia, están asumiendo procesos de transformación y profesionalización, replanteando las estrategias militares y sus componentes organizacionales, de tal manera que

---

[1] Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009) (Gobierno de Colombia, 2011).

permitan visionar, determinar, proyectar y preparar el desarrollo de capacidades de ciberdefensa en respuesta a las amenazas potenciales e inminentes en o a través del ciberespacio, así como fortalecer la resiliencia cibernética nacional.[2]

Con respecto a la evolución y el crecimiento tecnológico, es preciso decir que toman cada vez menos tiempo, por lo que, para hablar del futuro del ciberespacio, este documento establece como referencia el año 2022, considerando el estudio realizado por Instituto Tecnológico de Massachussets (MIT) (Segars, 2018) y las reflexiones de Klaus Schwab (2018), en su libro *La cuarta revolución industrial*, donde se pronostica que "las innovaciones tecnológicas más importantes están a punto de generar un cambio trascendental en todo el mundo y es inevitable" (Schwab, 2018, p. 9). En este sentido, este trabajo plantea una estrategia a corto plazo para Colombia, para contar con una ventana estratégica de acciones preventivas y proactivas.

En consecuencia, los riesgos asociados a las nuevas tecnologías generan la necesidad de cambiar técnicas, tácticas y procedimientos aplicados en el ámbito de la defensa. Los conflictos actuales están cada vez más asistidos por métodos de guerra asimétrica, con muchas actividades que tienen lugar en el ciberespacio. En este contexto, también debe ser ágil el desarrollo de medidas y

---

[2] "Resiliencia cibernética" se define como la capacidad de los sistemas y las organizaciones para resistir a los eventos cibernéticos, medida mediante la combinación del promedio de tiempo necesario para que se produzca un fallo y del promedio de tiempo necesario para la recuperación (World Economic Forum, 2012). (Forum, 2012)

contramedidas que hagan uso de este tipo de tecnologías, u otras que se pudiesen identificar en el futuro. Como lo vienen haciendo la mayoría de los ejércitos, como lo afirma el Capitán de fragata, ingeniero José María Riola Rodríguez en el libro *Tecnologías Disruptivas y sus Efectos sobre la Seguridad*, "En la actualidad se ha entendido y consolidado la actividad de vigilancia, evaluación, prospectiva y predicción tecnológica en la mayoría de los ejércitos, de modo que la tecnología forma parte de los procesos de planeamiento de Defensa desde sus etapas más prematuras" (CESEDEN, 2015, p. 20).

Una piedra angular para desarrollar un sistema eficiente de ciberdefensa en Colombia fue un requisito del gobierno anclado en el Plan de Acción del CONPES 3701 de 2011, "Lineamientos de Política para Ciberseguridad y Ciberdefensa" (Gobierno de Colombia, 2011), donde se estableció la creación y el fortalecimiento de la ciberdefensa y se asignó la responsabilidad de defensa cibernética al Comando Conjunto Cibernético de Colombia, en adelante CCOCI.

Con sano criterio se puede definir que la propuesta de Estrategia Militar de Ciberdefensa para las Fuerzas Militares de Colombia planteada de cara a las amenazas cibernéticas que imponen las tecnologías disruptivas, parte de un análisis de capacidades existentes en las instituciones responsables de la ciberdefensa nacional de las Fuerzas Militares, en lo que refiere a doctrina, organización, material, personal, infraestructura, liderazgo, educación, entrenamiento, mantenimiento u otras variables que permitan determinar la situación actual y así, proyectar un estado deseado. De igual forma, se realiza la identificación y estudio de las amenazas cibernéticas latentes y emergentes que imponen las tecnologías disruptivas a la ciberdefensa nacional en Colombia con base en el instrumento llamado la "Ventana de AREM" (Cano, 2017).

Finalmente, con los resultados obtenidos se presenta una propuesta militar estratégica de ciberdefensa, fundamentada en el modelo de planeamiento por capacidades DOMPILEM (Doctrina, Organización, Material, Personal, Infraestructura, Liderazgo, Entrenamiento y Mantenimiento), complementado con otras variables estratégicas que permitan el despliegue operativo necesario para responder ante las nuevas amenazas cibernéticas.

1. Planteamiento de la investigación

1.0 Introducción

Este proyecto comprende una monografía de estudio descriptivo que se realizó a partir de la revisión bibliográfica de los principales trabajos de investigación, estrategias, artículos científicos, libros, autores y entidades relacionados con la temática de las amenazas cibernéticas a la defensa nacional, que pueden surgir como consecuencia de la apropiación de tecnologías disruptivas; se analizan también las medidas que se pueden adoptar para contrarrestarlas. Para este propósito, se hizo necesario conocer sobre la estrategia y la ciberdefensa; por tanto, se tomaron como referente algunos de los autores más representativos en el tema, para resaltar sus enfoques o pensamientos.

En el desarrollo de esta monografía, también se analizaron las estructuras organizacionales de las unidades militares de ciberdefensa a nivel nacional y se estudiaron algunas estrategias militares de ciberdefensa a nivel internacional. Esta investigación busca reconocer, a partir de las experiencias de otros países que llevan más tiempo de desarrollo en materia de ciberdefensa, los aspectos relevantes, a fin de que sean apropiados en la realidad nacional.

1.1 Descripción y formulación del problema

Hoy el mundo se encuentra interconectado, donde las empresas públicas y privadas, la fuerza pública, la academia y la sociedad en general basan su funcionamiento en el ciberespacio, enfrentando la llamada "Cuarta revolución digital" marcada por las altas velocidades en que evoluciona la tecnología; por la amplitud y profundidad con que las combina y por el impacto que tiene en los sistemas; la que trae consigo múltiples beneficios, sin embargo, genera también un espacio propicio para la incubación de amenazas cibernéticas, que podrían poner en riesgo la

seguridad y defensa de Colombia. Como lo expresan los autores Schwab & Botin en su libro La cuarta Revolución Industrial (2016), "La convergencia de tecnologías digitales, físicas y biológicas marcan el advenimiento y despliegue de la Cuarta Revolución Industrial", que genera un cambio con impacto en los sistemas a gran escala y a toda velocidad en el mundo que conocemos. Si se analizan las múltiples fuentes de información, la tecnología es cada día más accesible y permite que surjan nuevas amenazas procedentes de regímenes ilegítimos, grupos terroristas, grupos al margen de la ley y delincuencia organizada, quienes pueden tener acceso al ciberterrorismo, ciberdelincuencia, armas de destrucción masiva, mercado negro armamentístico, etc. Esto implica un cambio en la idea de la amenaza tradicional procedente de enemigos identificados (CESEDEN, 2015).

Partiendo de este contexto, es evidente que la ciberdefensa toma un papel protagónico, en cuanto involucra diversos actores, dándole un eje fundamental a las Fuerzas Militares, para proponer una visión que garantice la resiliencia y continuidad de las infraestructuras críticas cibernéticas, en el quinto dominio de la guerra: el ciberespacio. Cada vez más se difumina la línea entre el mundo cibernético y el mundo físico para enfrentar la convergencia de la Defensa y la Ciberdefensa.

De otra parte, es preciso decir que, pese a que existen instituciones como el Comando Conjunto Cibernético (CCOCI) y tres unidades cibernéticas (una en el Ejército Nacional, otra en la Armada Nacional y una tercera en la Fuerza Aérea Colombiana), se ha identificado que las capacidades de ciberdefensa en las Fuerzas Militares de Colombia, no son suficientes para responder ante las actuales amenazas cibernéticas, porque existen variables como la falta de personal experto en ciberdefensa, la ausencia de laboratorios especializados y la alta rotación del personal

especializado, entre otras, que introducen una brecha tecnológica y operacional que refleja un rezago importante en la ciberdefensa nacional.

Adicionalmente, se presentan grandes debilidades a la hora de enfrentar las adversidades en el ciberespacio en situaciones de conflicto, bien sea en o a través del ciberespacio. Esto como consecuencia de la ausencia de doctrina en materia de operaciones cibernéticas que regulen y establezcan el accionar de las Fuerzas Militares en el ciberespacio.

De igual manera, es importante reconocer que elementos como la convergencia tecnológica (Cano, 2018), la densidad digital (Accenture, 2015) y los productos y servicios digitalmente modificados (Cano, 2018), han incrementado los niveles de riesgo cibernético nacional. En este contexto, se revela que numerosos países se encuentran frente a una serie de retos que exigen altos niveles de dependencia tecnológica, que despliegan un escenario de oportunidades, pero también complejo y desafiante, de cara al crecimiento exponencial de las amenazas y vulnerabilidades cibernéticas a la ciberdefensa nacional.

Cabe señalar que Colombia, al igual que otros países que vienen adoptando las tecnologías de información y las tecnologías de operación para optimizar el desarrollo de sus procesos productivos, económicos, sociales, políticos e incluso de seguridad y defensa nacional, se encuentra frente a un escenario de cambios revolucionarios a los cuales se hace necesario adaptarse y prepararse para evitar, defender, contener y/o anticipar posibles daños de alto impacto en las infraestructuras críticas cibernéticas del país que afecten directamente la prestación de los servicios básicos a la población.

Por consiguiente, en el contexto de seguridad y defensa nacional, donde surgen continuamente nuevos desarrollos tecnológicos disruptivos, es cada vez más necesario el pensamiento innovador: nuevos conceptos operacionales, nuevos modelos organizativos y el establecimiento de estrategias a largo plazo, donde la tecnología se contempla como catalizadora de capacidades militares, con impacto tanto en las Fuerzas Militares como en los propios conceptos de los sistemas (CESEDEN, 2015). Es una realidad, Colombia es vulnerable en este mundo conectado. Hoy en día la dependencia de la confidencialidad, disponibilidad e integridad de los datos está marcada en contraste con la insuficiencia en materia de ciberseguridad y ciberdefensa. Si bien no es posible proteger o eliminar las vulnerabilidades cibernéticas a nivel de país, la implementación de mejoras estratégicas y las buenas prácticas en la ciberseguridad y la ciberdefensa puede hacer que sea más difícil la materialización de una amenaza y que los ataques tengan éxito; además de conseguir disminuir el impacto de los que logren materializarse. Así mismo, estas mejoras incrementan las posibilidades para disuadir, mitigar o neutralizar ciberataques e incrementan la resiliencia cibernética nacional para resistir a los ataques perturbadores y destructivos. Con el propósito de plantear una alternativa nacional, se formula la pregunta de la investigación: ¿cómo las unidades militares de ciberdefensa en Colombia pueden afrontar las amenazas cibernéticas que imponen las tecnologías disruptivas a la ciberdefensa nacional?

1.2 Objetivos de la investigación

Objetivo general

Diseñar una estrategia militar de ciberdefensa que permita afrontar las amenazas cibernéticas que imponen las tecnologías disruptivas a la ciberdefensa nacional al 2022.

Objetivos específicos

a) Analizar el contexto actual en materia de organización y estrategias de las unidades militares responsables de la ciberdefensa.

b) Identificar y detallar las amenazas cibernéticas latentes y emergentes que imponen las tecnologías disruptivas a la ciberdefensa nacional en Colombia.

c) Diseñar una propuesta militar estratégica operacionalizable basada en el planeamiento por capacidades DOMPILEM (Doctrina, Organización, Material, Personal, Infraestructura, Liderazgo y Educación, Entrenamiento y Mantenimiento).

1.3 Justificación

La evolución tecnológica cada vez toma menos tiempo, así que para hablar de un futuro en el ciberespacio basta tomar como referencia el año 2022, para el cual se cuenta con informes y proyectos de fuentes confiables (Segars, 2018) que pronostican la disponibilidad de una gran cantidad de tecnologías disruptivas que harán parte integral de la vida cotidiana de las personas, las empresas y los Estados.

Un gran número de fuerzas de disrupción e innovación están marcando el futuro inmediato, pero también dan lugar al surgimiento de nuevas amenazas y ataques en el ciberespacio, que podrían llegar a afectar infraestructuras cibernéticas, provocando incluso daños físicos. Por lo tanto, los perpetradores de ataques no descansan en su intento por buscar nuevas y mejores formas de explotación para lograr sus objetivos de manera más fácil y eficiente.

Por su parte, las amenazas cibernéticas son múltiples y muy variadas. Mutan sus vectores de operación en cuestión de segundos, y se soportan en la masificación de las tecnologías disruptivas,

entre ellas: computación generalizada, redes inalámbricas, biotecnología, impresión 3D, aprendizaje de máquina, nanotecnología y robótica (Cano, 2017). Todas estas tecnologías se combinan entre sí y ofrecen un escenario complejo y dinámico que debe ser afrontado por las Fuerzas Militares de la forma más adecuada, para evitar que se produzca un impacto profundo a la defensa en Colombia.

Sumado a lo anterior, la llamada Cuarta Revolución Industrial o la revolución digital (Kanlli, 2015), es una fuente de crecimiento y competitividad para cualquier Estado. No obstante, esta revolución marca el inicio para repensar la defensa nacional en el nuevo dominio de guerra, el ciberespacio. En este escenario, es totalmente viable que un ataque cibernético a gran escala en un país pueda debilitar o impedir su gobernabilidad, e imposibilitar la prestación de servicios esenciales, ocasionando sufrimiento y en ocasiones muerte a la población. Así mismo, puede causar pérdidas económicas que desestabilicen la economía del país, hechos que aunados podrían conseguir, en un momento dado, doblegar el componente militar de un país.

Uno de los casos más visibles fue el de Estonia en el 2007. Este país fue víctima de agresiones cibernéticas en forma masiva sobre su infraestructura, siendo considerado el primer asalto cibernético dirigido a la seguridad nacional de un país (Ashmore y William, s. f.).

Para algunos autores como Klaus Schwab, estamos frente a una cuarta y distinta revolución que fusiona tecnologías a través de los mundos físicos, digitales y biológicos: la revolución digital marcada por las altas velocidades en que evoluciona la tecnología; por la amplitud y profundidad con que las combina y por el impacto que tiene en los sistemas.

En materia de política pública a nivel nacional, el panorama es similar, las Fuerzas Militares y el país en general reconocieron, a través del documento CONPES 3701 de julio de 2011 (Gobierno

de Colombia, 2011), y lo reafirmaron mediante el documento CONPES 3854 (Gobierno de Colombia, 2017) de abril de 2016, que existe una "nueva amenaza permanente" en el contexto de una sociedad de la información y el conocimiento. De igual manera, se confirmó que el país cuenta con infraestructuras críticas cibernéticas que son requeridas para mantener la operación y gobernabilidad de la Nación.

Para tal fin, el Ministro de Defensa Nacional aprobó la creación y activación del Comando Conjunto Cibernético (CCOCI), con la función principal de ejercer la ciberdefensa de la Nación y conducir operaciones militares cibernéticas a nivel estratégico, para la seguridad y defensa de la nación en el ciberespacio. La creación de esta unidad militar se convirtió en un factor estratégico que permitió a las Fuerzas Militares unificar esfuerzos para la defensa del Estado en el ciberespacio. De igual forma, se ordenó la creación de estructuras organizacionales al interior de cada Fuerza denominadas unidades cibernéticas, con las cuales el CCOCI ejecutará y coordinará actividades de ciberseguridad y operaciones de ciberdefensa del país de acuerdo al tipo de amenaza, rol, naturaleza, función propia a cada Fuerza y la reglamentación que se establezca.

Como consecuencia de la revolución de las tecnologías de la información, comunicaciones y operación, el ciberespacio es también el entorno social donde las personas pueden interactuar en armonía, cooperación y/o conflicto. Sin embargo, considerar el ciberespacio como un quinto dominio de la guerra, sigue siendo objeto común de reflexión de múltiples expertos y agencias públicas y privadas nacionales e internacionales, como lo afirma el Capitán Enrique Cubeiro (en Newmeyer, 2015) en el artículo "Ciberespacio, ciberseguridad y ciberguerra", donde señala:

> No existe la claridad que hay en otros ámbitos en los que se utilizan unas armas y unas técnicas de combate completamente diferentes a las anteriores, o las que se han utilizado

> hasta ahora en los campos de batalla tradicionales. Un dominio en que no existe ningún tipo de control armamentístico y en el que además existen mucho más actores que en el resto de dominios. En el mar, en la tierra, en el aire; el armamento está normalmente en poder de los ejércitos o de las fuerzas y cuerpos de seguridad del Estado. En el ciberespacio el armamento está prácticamente en poder de toda la humanidad. A ello se suma un entorno legal y complejo y si ya no es muy complejo; el ámbito del cibercrimen la cosa se complica todavía mucho más, cuando lo trasladamos al campo militar. Es muy difícil trasladar conceptos hasta ahora conocidos como ataque armado, como autodefensa, como acto hostil, como intento hostil al espacio. Podemos decir en cierto modo que el ciberespacio es una especie de Estado fallido, en el que esta autoridad favorece como siempre al agresor (pp. 88-89).

En contraste con lo anteriormente dicho, el ciberespacio se vislumbra como un nuevo escenario de confrontación bélica, que, combinado con los poderes de tierra, mar, aire y espacio, constituirá un verdadero poderío y superioridad de cualquier Estado o Nación. Este nuevo dominio es vital para influir, diseñar y desarrollar futuras operaciones militares.

Cabe señalar que las Fuerzas Militares de Colombia, requieren abordar el ciberespacio como un ámbito estratégico, operativo y táctico para organizar, entrenar y equipar las unidades militares responsables de la ciberdefensa nacional, a fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permitan fortalecer las capacidades de ciberdefensa para enfrentar las amenazas o incidentes de naturaleza cibernética que puedan afectar la infraestructura crítica cibernética del país y poner en riesgo la seguridad nacional, la defensa de la soberanía y el

orden constitucional del Estado, así como causar daños masivos, debilitar la economía y/o dañar la moral pública y la confianza.

Es necesario recalcar que, dado el dinamismo del ciberespacio, muchos países han reconocido la necesidad de trabajar juntos para defender los intereses comunes y promover la seguridad. La relación de las Fuerzas Militares de Colombia con sus aliados estratégicos y socios internacionales proporciona una base sólida sobre la que se debe avanzar en la cooperación del ciberespacio. La continua colaboración internacional, la legítima defensa colectiva y el establecimiento de normas internacionales del ciberespacio también servirán para fortalecer el beneficio de todos.

Finalmente, es importante pensar que a pesar de que la moderna tecnología ha revolucionado la mayor parte de las dimensiones materiales de la guerra desde el siglo XIX, la lógica de los conflictos permanece básicamente inalterable. Esto explica porque obras como *De la Guerra* de Karl Von Clausewitz (2010 [1832]) y *El arte de la guerra* de Sun Tzu (2003 [siglo V a.C.]), permanecen como marcos conceptuales relevantes para el estudio de la política y la estrategia incluso en nuestros días. Por lo tanto, a pesar de que la estrategia militar es una disciplina en constante evolución, la estrategia propuesta no puede ni debe ignorar las enseñanzas de los clásicos.

1.4 Alcances y limitaciones del estudio

El presente estudio muestra una propuesta de estrategia militar de ciberdefensa, con base en las necesidades que demandan las amenazas cibernéticas latentes y emergentes, tomando como base los documentos CONPES en materia cibernética. Sin embargo, es preciso anotar que, para que esta propuesta se desarrolle, se requiere la voluntad política, legislación nacional y acciones operativas

específicas, las cuales manifiestan limitaciones inherentes para su despliegue e implementación de planes de protección, contención o mitigación de amenazas en asuntos relacionados con el ciberespacio.

2. Revisión de la literatura

2.0 Introducción

El análisis y revisión de literatura de los tres grandes elementos que hacen parte de este estudio, como son la ciberdefensa nacional, las unidades cibernéticas de las fuerzas militares colombianas y las amenazas cibernéticas latentes y emergentes, servirá de base para el desarrollo de la propuesta, al tiempo que permitirá una mejor comprensión de la estrategia presentada.

2.1 Ciberdefensa nacional

2.1.1 Panorama de la ciberdefensa a nivel nacional

Hoy en día, la tecnología y el internet hacen parte integral en el desarrollo económico, político y social de Colombia y, por ende, de su seguridad y defensa nacional. Es por esto que la ciberdefensa nacional debe ser asumida con un enfoque sistémico y multidimensional que requiere un trabajo conjunto y coordinado con los diferentes sectores e instituciones del país, para dar cumplimiento a los objetivos e intereses del Estado.

En este sentido, sus 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 de ciberdefensa, para enfrentar las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país y poner en riesgo la seguridad nacional, la defensa de la soberanía y el orden constitucional del Estado, así como causar daños masivos, debilitar la economía, y/o dañar la moral pública y la confianza.

El General de División, Evergisto de Vergara, y el Contralmirante, Gustavo Adolfo Trama, de la reserva activa de Argentina, señalan que:

> [...] los aspectos que influyen en la vida diaria con respecto al uso del espacio cibernético tienen amplia difusión. Todas las acciones que se desarrollen en este campo afectarán al componente armado del poder nacional desde varias perspectivas. La primera de ellas es el uso de la fuerza convencional militar como respuesta a un ataque cibernético masivo. Se contempla esta posibilidad porque los países más poderosos en aplicaciones cibernéticas de uso diario son justamente los más vulnerables en este aspecto. Se dice que los efectos de un ataque masivo cibernético multiplicado varias veces a lo ocurrido en Estonia en el año 2007 tendrían los mismos resultados devastadores que un ataque nuclear. No todos los países adhieren a esta postura porque daría lugar al uso arbitrario de la fuerza convencional por causas que luego originarían disculpas efusivas, pero sin efectos que puedan retrotraerse. La segunda implica el uso del poder militar convencional de los países ante el ataque cibernético a infraestructuras civiles. Las consecuencias sobre la población civil de un ataque a las infraestructuras críticas podrán requerir el empleo inmediato de fuerzas militares para paliar los efectos en tareas que seguramente excederán a la ayuda humanitaria, como por ejemplo la prevención de saqueos y vandalismos. Este empleo militar forzoso en ayuda humanitaria puede, además, complementarse con un ataque militar convencional (Vergara y Adolfo, 2017, pp. 43-49).

Por lo dicho anteriormente, para obtener una visión de los retos que enfrentan las Fuerzas Militares, especialmente en un país como el nuestro que es garante del Estado de Derecho, respeto por los derechos humanos, las libertades ciudadanas y el derecho internacional humanitario, es necesario establecer controles encontrando un balance entre las necesidades públicas y privadas, para actuar de manera precisa en la identificación, detección, prevención y respuesta ante actividades agresoras y/o terroristas en el ciberespacio (COGFM, 2018).

Es por esto que la ciberdefensa nacional, debe ser asumida con un enfoque sistémico y multidimensional que requiere un trabajo conjunto y coordinado con los diferentes sectores e instituciones del país para dar cumplimiento a los objetivos e intereses del Estado, de la mano del componente tecnológico y el internet, que hacen parte integral en el desarrollo económico y social del país y por ende, de su seguridad y defensa nacional.

Desde la perspectiva estratégica, se ha venido recreando en la polemología el concepto de centro de gravedad, el cual pretende categorizar aquellos puntos más vulnerables que puede poseer un Estado-Nación al ser atacado o agredido por una amenaza. A lo largo de la historia, en esta esfera conceptual se han incluido las vías de comunicación, las fábricas industriales, la moral, los centros administrativos gubernamentales, los bastiones militares, las fuentes de energía e incluso la población (Gaitán, 2012, p. 63).

En la guerra tradicional, cuando algún Ejército pretendía impactar alguno de los centros de gravedad de su enemigo, el empleo de tecnología bélica, en los escenarios de conflagración terrestres, marítimos y aéreos fue la lógica. En la era de la información, la guerra se ha extendido a la dimensión ciberespacial, y allí los Estados han generado nuevos puntos neurálgicos que

soportan la determinación política de un Estado y la voluntad de sus tropas de continuar con la contienda, es decir, nuevos centros de gravedad (Gaitán, 2012, p. 63).

> El "salvaje cerebral", por excelencia Clausewitz, presentó una serie de construcciones intelectuales, teorías y conceptos de los principales filósofos, científicos y otros pensadores de su tiempo con el fin de comprender y describir lo que observó cómo los diversos aspectos de la guerra. Varios de sus conceptos fricción, polaridad, y el centro de gravedad son analogías o metáforas extraídas de las "ciencias mecánicas" (la física de hoy). En particular, el texto original en alemán de Vom Kriege, revela que Clausewitz utiliza el centro de gravedad como una metáfora más de cincuenta veces. Él parece haber derivado su concepto (centro de gravedad, o punto principal) militar de un centro de gravedad después de escuchar una serie de conferencias por el físico alemán Paul Erman, profesor de la Universidad de Berlín y el prusiano Allgemeine Kriegsschue. El uso de Clausewitz del centro de gravedad en la Guerra sigue siendo esencial y consistente con la representación del concepto en las ciencias mecánicas. La mayoría de las fuentes en idioma inglés que citan su definición de un centro de gravedad se basan principalmente en uno de los dos pasajes, páginas 485-86 del Libro VI ("Defensa"), o páginas 595-96 del Libro VIII ("Planes de guerra"), de la traducción de On War de Sir Michael Howard y Peter Paret (Echevarría, 2003, p 110).

Por lo tanto, "los centros de gravedad"[3] en la actualidad no solo pueden ser deshabilitados mediante el armamento convencional, sino también mediante computadores. Clausewitz afirma que,

> [...] la guerra se debe tener siempre como objetivo el sometimiento del enemigo, el cual, al mismo tiempo, intentará defender sus intereses particulares de acuerdo con las circunstancias. Estos intereses del enemigo formarán un Centro de Gravedad, que es un centro de fuerza y movimiento del que depende el conjunto, y al que tiene que dirigirse el golpe concentrado de nuestras fuerzas (Clausewitz, 2005, pp. 655-656).

Por lo expuesto hasta aquí, las Fuerzas Militares de Colombia 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 de ciberdefensa, para enfrentar las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país y poner en riesgo la seguridad nacional, la defensa de la soberanía y el orden constitucional del Estado, así como causar daños masivos, debilitar la economía, y/o dañar la moral pública y la confianza. En consecuencia, se establece cómo las Fuerzas Militares de Colombia han asumido procesos de transformación y

[3] Clausewitz definió el "Centro de Gravedad como "El centro de todo poder y movimiento del cual todo depende". (Clausewitz 2005: 655-656).

profesionalización, donde se evidencia que se han replanteado las estrategias militares y sus componentes organizacionales de tal manera que permitan visionar, determinar, proyectar y preparar el desarrollo de capacidades de ciberdefensa en respuesta a las amenazas potenciales e inminentes en o a través del ciberespacio, así como fortalecer la resiliencia cibernética nacional. Desde el punto de vista internacional, el horizonte muestra mayores avances, especialmente para los países miembros de la OTAN, como se evidencia en el siguiente numeral.

2.1.2 El panorama de ciberdefensa a nivel internacional

Durante el desarrollo de la Cumbre de Lisboa del 18-19 de noviembre de 2010, la OTAN decidió desarrollar un esfuerzo concertado para encarar los nuevos retos de la seguridad global y la evolución del espectro de la amenaza, eligiendo la defensa cibernética (ciberdefensa) como una prioridad estratégica para la alianza e imponiendo como tarea urgente el desarrollo de una capacidad de protección de la alianza contra este tipo de ataques, pues de ella depende su propia seguridad. En febrero de 2014, la Alianza de Ministros de Defensa de la OTAN desarrolló una adición a la política de defensa, en cuanto a ciberdefensa colectiva, asistencia a los aliados, gobernanza, consideraciones legales y relaciones con la industria. Posteriormente, en abril de 2014, el North Atlantic Council (NAC) accedió a cambiar el nombre del Comité de Política y Planes de Defensa (Defensa Cibernética) como el Comité de Defensa Cibernética y en junio de 2014, los Ministros de Defensa de la OTAN aprobaron la nueva política de defensa cibernética, que se está aplicando en la actualidad. La nueva política y su aplicación se mantendrán bajo estricta revisión, tanto a nivel político como técnico dentro de la alianza. Las normativas se perfeccionarán y se actualizarán de acuerdo con la evolución de la amenaza cibernética.

Es necesario resaltar que, dado el dinamismo del ciberespacio, muchos países han reconocido la necesidad de trabajar juntos para defender los intereses comunes y promover la seguridad. La relación de las Fuerzas Militares de Colombia con sus aliados estratégicos y socios internacionales proporciona una base sólida sobre la que se debe avanzar en la cooperación del ciberespacio. La continua colaboración internacional, la legítima defensa colectiva y el establecimiento de normas internacionales del ciberespacio, también servirán para fortalecer el beneficio de todos.

De acuerdo a información obtenida del portal del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, reconocido centro de defensa cibernética multinacional e interdisciplinario, a través del cual se realizan apoyos en ciberdefensa a sus países miembros y se fomenta la cooperación de naciones de ideas afines, a octubre de 2018 existían cuatro (4) países que habían publicado y compartido sus estrategias de ciberdefensa, así:

Tabla 1

Estrategias militares de ciberdefensa internacionales

País	Documento	Año
República Checa	Cyber Defence Strategy (NCOC, 2018)	2018
Países Bajos	Defence Cyber Strategy (MoD, 2012)	2012
Portugal	Political Guidance for Cyber Defence (Rui, 2013)	2013
Estados Unidos	National Cyber Strategic (DoD, 2013)	2013
	National Cyber Strategic (DoD, 2018a)	2018

Fuente: elaboración propia.

Para este caso de estudio, se tomaron en cuenta los cuatro documentos descritos y se realizó un análisis comparativo sobre la misión global, los objetivos estratégicos y los principios rectores sobre los cuales se enfocan las estrategias de ciberdefensa.

2.1.2.1 República Checa

Para la República Checa, la *Defence Strategy of the Czech Republic* tiene como objetivo global alcanzar un estado en el que Centro Nacional de Operaciones Cibernéticas (NCOC) sea capaz de garantizar la ciberseguridad de la República Checa, llevar a cabo actividades militares, operaciones en el ciberespacio y desempeñar un papel activo en el entorno internacional. Para este fin, se establecieron cinco (5) objetivos estratégicos (NCOC, 2018, p. 6):

1. Definición de marco legal.
2. Construcción y desarrollo de infraestructura NCOC.
3. Desarrollo de capacidades de defensa en el ciberespacio.
4. Establecimiento de la cooperación y el desempeño de la educación y la formación.
5. Compromiso en garantizar la seguridad cibernética dentro del Ministerio de Defensa.

2.1.2.2 Países Bajos

La Estrategia de Defensa Cibernética para los Países Bajos, *Defence Cyber Strategy*, tiene seis puntos focales en los cuales la organización Defensa se esforzará para la realización de sus objetivos en el ciberespacio (MoD, 2012):

1. La adopción de un enfoque integral.

2. Fortalecimiento de la defensa cibernética de la organización Defensa (elemento defensivo).
3. El desarrollo de la capacidad militar para llevar a cabo operaciones cibernéticas ofensivas (elemento ofensivo).
4. Fortalecimiento de la posición de inteligencia en el ciberespacio (elemento de inteligencia).
5. Fortalecimiento de la posición, conocimiento y la fuerza innovadora de la organización de defensa en el ciberespacio, incluyendo el reclutamiento y retención de personal cualificado (adaptativa y elementos innovadores).
6. La intensificación de la cooperación, tanto a nivel nacional como internacional (elemento cooperación).

2.1.2.3 Estados Unidos

La estrategia cibernética del Departamento de Defensa 2018, representa la visión del Departamento para abordar esta amenaza y la implementación de las prioridades de la Estrategia de Seguridad Nacional y la Estrategia de Defensa Nacional para ciberespacio.

Adicionalmente, el documento establece que:

> Los Estados Unidos no pueden permitirse la inacción: nuestros valores, la competitividad económica y la ventaja militar están expuestos a amenazas que se vuelven más peligrosas cada día. Debemos defender con firmeza nuestros intereses en el ciberespacio por debajo del nivel de conflicto armado y garantizar la

preparación de nuestros operadores del ciberespacio para apoyar a la Fuerza Conjunta en situaciones de crisis y conflicto (DoD, 2018, p. 2).

Los objetivos establecidos en este documento para el Departamento del Defensa en el ciberespacio, son:

1. Asegurar que la Fuerza Conjunta pueda lograr sus misiones en un entorno de ciberespacio disputado.
2. Fortalecimiento de la Fuerza Conjunta mediante la realización de operaciones en el ciberespacio que mejoren las ventajas militares de los Estados Unidos.
3. Defender la infraestructura crítica de los Estados Unidos de la actividad cibernética maliciosa que, por sí sola, o como parte de una campaña, podría causar un incidente cibernético significativo.
4. Proteger la información y los sistemas DoD contra la actividad cibernética maliciosa, incluida la información DoD en redes que no son propiedad de DoD.
5. Expansión de la cooperación cibernética del DoD con socios interinstitucionales, industriales e internacionales.

2.1.2.4 Portugal

El documento *Political Guidance for Cyber Defence*, tiene como objetivo determinar los principios esenciales, fijar objetivos y establecer las directrices correspondientes de los esfuerzos dentro de

la defensa nacional, con el objetivo primordial de potencializar las capacidades nacionales de ciberdefensa.

Los objetivos de esta política de defensa cibernética, son (MoF, 2013):

1. Para garantizar la protección, la resistencia y la seguridad de las redes y Sistemas de Información Críticos (SIC) y la defensa nacional contra ataques cibernéticos.
2. Para garantizar la libertad de acción en el ciberespacio y el país, cuando sea necesario la exploración activa del ciberespacio para impedir o dificultar su uso hostil contra el interés nacional.
3. Contribuyen de manera cooperativa para la seguridad cibernética nacional.

Según un artículo publicado este año en la revista de la OTAN, edición digital, varios países están desarrollando cada vez más "capacidades de Ciberdefensa", ya que "una buena Ciberdefensa puede hacer que estas amenazas sean manejables hasta el punto de que los riesgos remanentes resulten aceptables, como ocurre con las amenazas clásicas" (Theiler, 2011, párr. 20).

En consonancia con esta afirmación, se observa que los países analizados enfocan su estrategia al cumplimiento de un objetivo global y unos objetivos para garantizar la Seguridad y Defensa Nacional, y en todos los casos, utilizan como referencia la OTAN.

Adicionalmente y para comprender las capacidades actuales en Colombia, se hace necesario estudiar y comprender el alcance de las responsabilidades de las unidades militares cibernéticas en Colombia y el estado de madurez de sus capacidades operativas en la actualidad.

2.2 Unidades de ciberdefensa

En la actualidad, Colombia cuenta con una estructura organizacional en materia de ciberdefensa en los niveles estratégico, operacional y táctico. De acuerdo con el Manual de Ciberdefensa Conjunta del CCOCI (FFMM, 2016), la estructura organizacional de ciberdefensa se encuentra bajo la responsabilidad del Comando General de las Fuerzas Militares (COGFM) a través del Comando Conjunto Cibernético que depende de la Subjefatura de Estado Mayor Conjunto Operacional (SEMCO) y de las Fuerzas Militares a través de las unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

En efecto, el Comando Conjunto Cibernético fue creado y activado en octubre de 2012 como ente rector para el direccionamiento, planeación, coordinación, integración, ejecución y sincronización de operaciones cibernéticas conjuntas. Este Comando, tiene la misión de ejercer la ciberdefensa y conducir operaciones militares cibernéticas a nivel estratégico, para la seguridad y defensa de la Nación en el ciberespacio. Para tal fin, mantiene relaciones de coordinación con las Unidades Cibernéticas del Ejército, Armada y Fuerza Aérea, con el propósito de consolidar esfuerzos e integrar capacidades para el desarrollo de operaciones de ciberseguridad y ciberdefensa (FFMM, 2016).

El Ministro de Defensa Nacional del año 2012, aprobó la creación y activación del Comando Conjunto Cibernético (CCOCI) (MinDefensa, 2012), con la función principal de ejercer la ciberdefensa de la nación y conducir operaciones militares cibernéticas a nivel estratégico, para ser garantes de la seguridad y defensa de la Nación en el ciberespacio. De igual forma, se ordenó la creación de estructuras organizacionales al interior de cada Fuerza denominadas unidades cibernéticas, así: una en el Ejército Nacional, otra en la Armada Nacional y una tercera en la Fuerza

Aérea Colombiana, con las cuales el CCOCI ejecutará y coordinará actividades de ciberseguridad y operaciones de ciberdefensa del país, como se muestra en la siguiente gráfica:

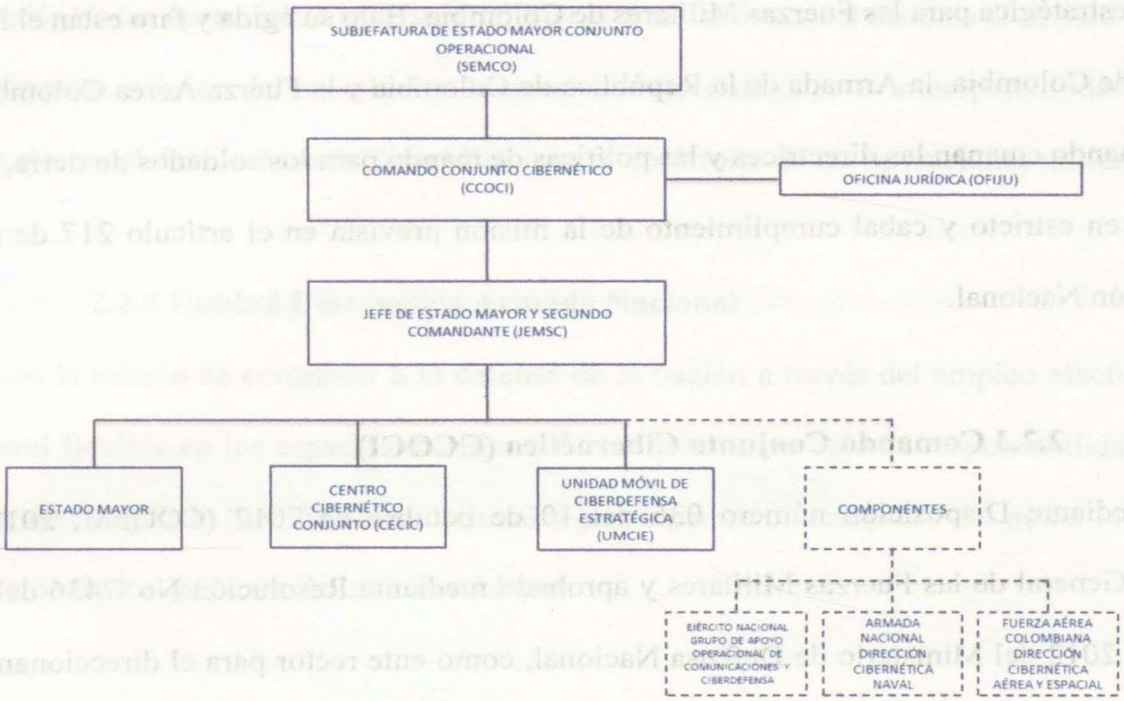

Figura 1. Organización CCOCI.

Fuente: CCOCI.

2.2.1 Ministro de Defensa Nacional

Con su misión principal de dirigir las Fuerzas Militares y la Policía Nacional, de acuerdo con la Constitución y la Ley.

2.2.2 Comando General de las Fuerzas Militares (COGFM)

El Comando General de las Fuerzas Militares es la entidad de más alto nivel de planeamiento y dirección estratégica para las Fuerzas Militares de Colombia. Bajo su égida y faro están el Ejército Nacional de Colombia, la Armada de la República de Colombia y la Fuerza Aérea Colombiana. De su comando emanan las directrices y las políticas de mando para los soldados de tierra, de mar y de aire, en estricto y cabal cumplimiento de la misión prevista en el artículo 217 de nuestra Constitución Nacional.

2.2.3 Comando Conjunto Cibernético (CCOCI)

Creado mediante Disposición número 036 del 10 de octubre de 2012 (COGFM, 2012), del Comando General de las Fuerzas Militares y aprobado mediante Resolución No. 7436 del 31 de octubre de 2012 del Ministerio de Defensa Nacional, como ente rector para el direccionamiento, planeación, coordinación, integración, ejecución y sincronización de operaciones cibernéticas conjuntas.

Este Comando, mantiene una relación de coordinación con las unidades cibernéticas del Ejército, Armada y Fuerza Aérea, con el propósito de consolidar esfuerzos e integrar capacidades para el desarrollo de operaciones de ciberseguridad y ciberdefensa.

El Comandante del Comando Conjunto Cibernético, establece un canal de coordinación con los comandantes de las unidades cibernéticas de cada Fuerza. Su misión consiste en ejercer la ciberdefensa y conducir operaciones militares cibernéticas a nivel estratégico, para la seguridad y defensa de la Nación en el ciberespacio.

2.2.4 Unidad Cibernética Ejército Nacional

Creada con la misión de conducir tareas de comunicaciones en apoyo al planeamiento, ejecución y supervisión de las operaciones militares del Ejército, en las áreas del Sistema C-5, para brindarle a los diferentes niveles del mando las herramientas tecnológicas e interoperabilidad que les permitan ejercer el debido Mando Tipo Misión en el desarrollo de las operaciones militares.

2.2.5 Unidad Cibernética Armada Nacional

Creada con la misión de contribuir a la defensa de la nación a través del empleo efectivo de un poder naval flexible en los espacios marítimo, fluvial y terrestre bajo su responsabilidad, con el propósito de cumplir la función constitucional y participar en el desarrollo del poder marítimo y la protección de los intereses de los colombianos.

2.2.6 Unidad Cibernética Fuerza Aérea Colombiana

Creada con la misión de planear, conducir y ejecutar operaciones de ciberseguridad y ciberdefensa para propender por la seguridad y defensa de su infraestructura crítica cibernética, con el propósito de contribuir a garantizar la supervivencia de la Fuerza y el empleo adecuado de los recursos y medios aéreos para el cumplimiento de la misión institucional. Así mismo, de manera coordinada, conjunta y combinada realizar operaciones para la defensa y seguridad nacional.

Adicionalmente, estas unidades militares lideran trabajos interinstitucionales en materia de infraestructuras críticas cibernéticas, con el propósito de avanzar en el desarrollo de Políticas y Planes de Protección y Ciberseguridad para sus activos estratégicos nacionales. Como resultado, se han logrado establecer lazos de confianza y amistad entre los diferentes sectores del país que

han permitido conformar redes de colaboración para compartir información de amenazas y alertas tempranas como medida preventiva para evitar la materialización de amenazas o ataques sobre las infraestructuras cibernéticas del país. Sin embargo, pese a los esfuerzos realizados, se evidencia la carencia de unas políticas y directrices integrales, positivas y comunes que describan y detallen las oportunidades y desafíos en el quinto dominio de la guerra, el ciberespacio, para empoderar a cada sector en materia cibernética, estableciendo objetivos estratégicos y líneas de acción claras que permitan obtener un control institucional en materia cibernética para conseguir los objetivos nacionales.

Sin embargo, pese a los esfuerzos realizados, se evidencia la carencia de una estrategia militar de ciberdefensa integral, positiva y común que describa y detalle las oportunidades y desafíos en el ciberespacio, que permita empoderar y articular a los militares en materia cibernética, estableciendo objetivos estratégicos y líneas de acción claras que permitan obtener un control institucional para conseguir los objetivos nacionales en o a través del ciberespacio.

En resumen, y partiendo de la definición establecida en el documento CONPES 3854 de 2016, es preciso decir que la ciberdefensa desde la perspectiva de la Defensa Nacional es "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". (Gobierno de Colombia, 2016, p. 87). Es preciso decir que el Ministerio de Defensa Nacional, asignó la responsabilidad de la ciberdefensa nacional a las Fuerzas Militares a través del Comandante General.

La responsabilidad de la ciberdefensa en Colombia se atribuyó a las Fuerzas Militares, las cuales, a través de la creación del Comando Conjunto Cibernético y las Unidades Cibernéticas en cada

Fuerza, buscan contribuir a incrementar la seguridad y la capacidad de actuar en red, tanto en el área militar como en diferentes sectores del gobierno y la sociedad, asumiendo el compromiso de protección de las infraestructuras críticas cibernéticas, como lo establece el documento CONPES 3701 (Gobierno de Colombia, 2011).

A octubre de 2018, el Comando Conjunto Cibernético presentó ante la Dirección de Planeación del Ministerio de Defensa, la curva de madurez de las capacidades cibernéticas de estas unidades, donde se pudo evidenciar que, en promedio general, las unidades militares responsables de ciberdefensa se encuentran en un nivel intermedio.

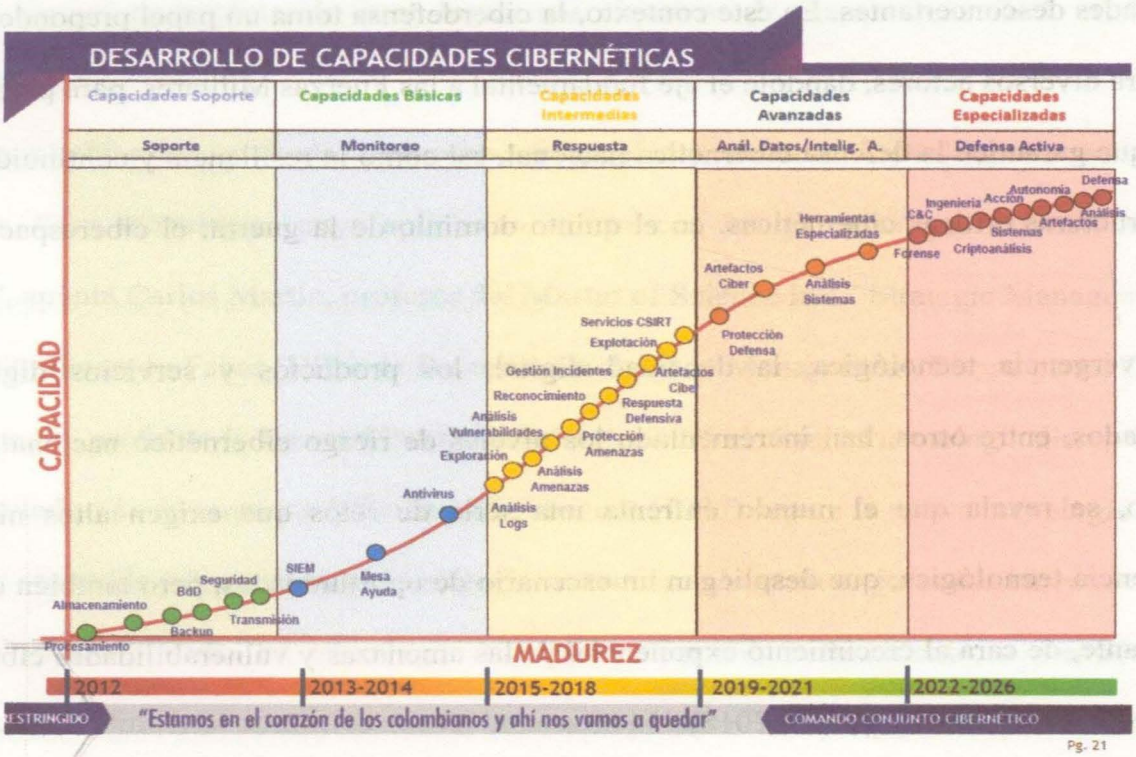

Figura 2. Curva de madurez capacidades cibernéticas.

Fuente: CCOCI.

En el siglo de la Revolución Digital, la tecnología se ha vuelto un factor de vital importancia. Sin embargo, internet puede tornarse un arma de doble filo, presentándose en ocasiones como una herramienta útil y, en otras, como una amenaza que debe mantener siempre alerta a las instituciones que controlan la Seguridad y Defensa de un Estado. (Amaral, 2013).

2.3 Amenazas cibernéticas de cara a la ciberdefensa nacional en Colombia

La actualidad tecnológica exige un mundo de sistemas complejos e interconectados, que trae como consecuencia el crecimiento de las amenazas cibernéticas a ritmos exponenciales y a velocidades desconcertantes. En este contexto, la ciberdefensa toma un papel preponderante que involucra diversos actores, dándole el eje fundamental a las Fuerzas Militares, para proponer una visión que garantice la defensa cibernética nacional, así como la resiliencia y continuidad de las infraestructuras críticas cibernéticas, en el quinto dominio de la guerra: el ciberespacio (DoD, 2015).

La convergencia tecnológica, la densidad digital, los productos y servicios digitalmente modificados, entre otros, han incrementado los niveles de riesgo cibernético nacional. En este contexto, se revela que el mundo enfrenta una serie de retos que exigen altos niveles de dependencia tecnológica, que despliegan un escenario de oportunidades, pero también complejo y desafiante, de cara al crecimiento exponencial de las amenazas y vulnerabilidades cibernéticas a la ciberdefensa nacional (Cano, 2018).

En este sentido, Colombia viene adoptando tecnologías de información y las tecnologías de operación para optimizar el desarrollo de sus procesos productivos, económicos, sociales, políticos e incluso de seguridad y defensa nacional. Se encuentra frente a un escenario de cambios

revolucionarios, en los cuales se hace necesario adaptarse y prepararse para anticipar y evitar (en la medida de lo posible) que pueda ocasionar daños de alto impacto en las infraestructuras críticas cibernéticas del país, que afecten directamente la prestación de los servicios básicos a la población y por consiguiente, comprometan la prosperidad económica y social de la nación.

En realidad, un gran número de fuerzas de disrupción e innovación están marcando el futuro inmediato, pero también dan lugar al surgimiento de nuevas amenazas y ataques en el ciberespacio, que podrían llegar a afectar infraestructuras cibernéticas, provocando incluso daños físicos. Por lo tanto, los perpetradores de ataques, no descansarán en su intento por buscar nuevas y mejores formas de explotación para lograr sus objetivos de manera más fácil, eficiente y anónima.

Para iniciar a hablar de tecnologías disruptivas, es preciso empezar por definirlas: las tecnologías disruptivas, "son tecnologías cuya aplicación rompe con los patrones que existían hasta el momento", apunta Carlos Martín, profesor del Master of Science in IT Strategic Management de la Universitat Pompeu Fabra (UPF) de Barcelona, School of Management. Por su parte, Clayton M. Christensen, profesor de Harvard Business School, acuñó el término tecnología disruptiva. En su libro titulado *The Innovator's Dilemma*, Christensen (1997) separa la nueva tecnología en dos categorías: sostenida y disruptiva. La tecnología sostenida se basa en mejoras incrementales a una tecnología ya establecida. La tecnología disruptiva carece de refinamiento, a menudo tiene problemas de rendimiento porque es nueva, atrae a un público limitado y puede que aún no tenga una aplicación práctica probada (tal fue el caso de la "máquina de habla eléctrica" de Alexander Graham Bell, que ahora llamamos el teléfono).

Para algunos autores como Klaus Schwab, estamos frente a una cuarta y distinta revolución que fusiona tecnologías a través de los mundos físicos, digitales y biológicos: "la revolución digital", marcada por las altas velocidades en que evoluciona la tecnología, por la amplitud y profundidad con que las combina y por el impacto que tiene en los sistemas.

Por otra parte, considerando que en estos tiempos modernos se enfrenta un mundo de sistemas complejos e interconectados, y en consecuencia las amenazas y ataques cibernéticos crecen a ritmos exponenciales y a velocidades desconcertantes, un reflejo de esta tendencia a la militarización de las cuestiones públicas se observa en el hecho de que la mayoría de los llamamientos al desarrollo de capacidades de ciberdefensa se sustentan en una "advertencia" sobre lo que podría pasar en un futuro cercano. Esto significa que no están basados en el conocimiento práctico de los efectos reales de las operaciones cibernéticas (Eissa, Gastaldi, Poczynok y Zacarias, 2012).

Conviene subrayar que los ataques cibernéticos son instrumentos ideales para dañar objetivos políticos, económicos, sociales u otros, y también una herramienta sólida para que los atacantes hagan cumplir su propia voluntad. Por tanto, es posible reflexionar sobre la afirmación de que los objetivos principales de las amenazas o ataques cibernéticos pueden ser especialmente los sistemas que interconectan estrechamente el entorno digital con la infraestructura real, lo cual es muy factible. Al mismo tiempo, es a menudo muy difícil de identificar al atacante (atribución), principalmente en tiempo real, lo que disminuye el riesgo de una potencial respuesta adecuada. No obstante, la Oficina de la Dirección Nacional de Inteligencia de Estados Unidos en el 2014, definió "No existe un proceso técnico simple o una solución automatizada para determinar la responsabilidad de las operaciones cibernéticas. El trabajo minucioso en muchos casos requiere

semanas o meses de análisis de inteligencia y análisis forense para evaluar la culpabilidad", (Office of the Director of National Intelligence, 2014). De igual forma, el autor James A. Green en su libro *Cyber Warfare, a multidisciplinary analysis* (2015) señala:

> La atribución de los ciberataques en la guerra cibernética es un problema difícil pero no imposible. La gran escala y la efectividad del ataque a menudo brindan oportunidades de rastreo y análisis que no son posibles con los ciberataques criminales comunes que vemos más regularmente en Internet. Aun así, la evidencia que obtenemos generalmente será circunstancial y difícil de usar en procedimientos legales a menos que se puedan buscar computadoras y dispositivos de los presuntos atacantes (Green, 2015, p. 70).

Estos hechos, junto con las relativas limitaciones o ausencia de capacidades cibernéticas, ofrecen una gran ventaja al atacante. Dicho de otra manera, el concepto de tecnologías disruptivas, implica, entre otras cosas, una revolución tecnológica. Un estudio realizado por el Instituto Tecnológico de Massachusetss (MIT), define que hay siete tecnologías que cambiarán el mundo, las cuales serán objeto del presente estudio (Segars, 2018).

2.4 Tendencias tecnológicas y tecnologías disruptivas

El concepto de "tecnologías disruptivas", implica, entre otras cosas, una revolución tecnológica: "En el ámbito militar la aplicación de tecnologías disruptivas produce, si se quiere obtener una superioridad en el enfrentamiento, cambios operativos con sus consecuencias organizativas y con ello cambios doctrinales y estratégicos profundos que tendrán también un carácter disruptivo" (CESEDEN, 2015, p. 8).

Hecha esta salvedad, y con el fin de identificar las megatendencias y transmitir su amplio impacto, el autor Klaus Schwab, basó su libro *La cuarta revolución industrial*

> [...] en la investigación desarrollada por el Foro Económico Mundial para agruparlas en tres grandes grupos que están estrechamente relacionados y cuyas tecnologías se benefician entre sí, cada uno de estos grupos, a su vez compuesto de impulsores o facilitadores tecnológicos, llamados por otros autores "tecnologías disruptivas" (Schwab, 2018, pp. 8-11).

Dichos grupos son los siguientes: tendencias físicas, fáciles de detectar debido a su carácter tangible; tendencias digitales, aplicaciones o conexiones entre el mundo físico y digital; y tendencias biológicas, innovaciones en el campo biológico y la genética.

El concepto de "tecnologías disruptivas", dicho de otra manera, implica, entre otras cosas, una revolución tecnológica que cada vez toma menos tiempo, así que, para hablar de un futuro en el ciberespacio, basta tomar como referencia el año 2022, para el cual se cuenta con informes y proyectos de fuentes confiables como el generado por el profesor distinguido Albert H. Segars, del Massachusetts Institute of Technology (Segars, 2018), quien pronostica la disponibilidad de una gran cantidad de tecnologías disruptivas que harán parte integral de la vida cotidiana de las personas, las empresas y los Estados.

El estudio presentado por el Instituto Tecnológico de Massachusetss (MIT), define que hay siete tecnologías que cambiarán el mundo, las cuales serán analizadas desde la perspectiva de sus posibles efectos y afectaciones en el contexto de las amenazas cibernéticas y afectaciones a la seguridad nacional.

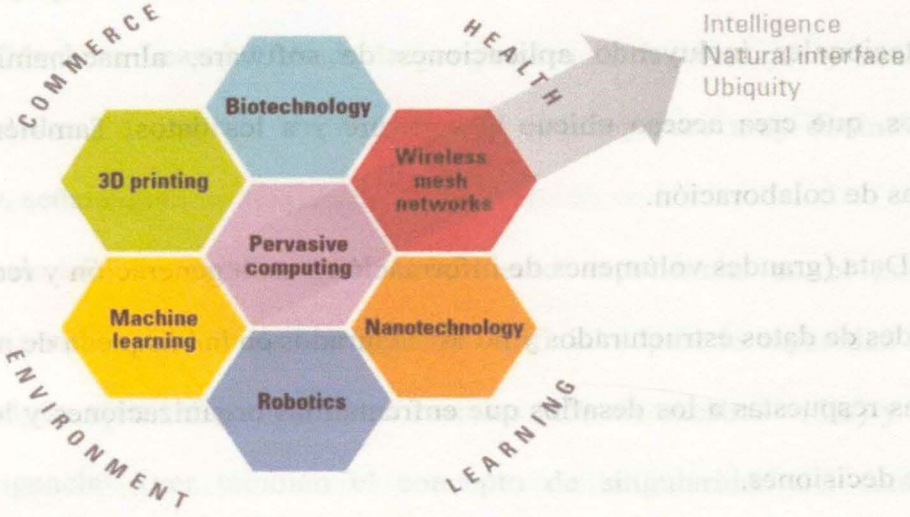

Figura 3. Las siete tecnologías que están cambiando el mundo

Fuente: Segars (2018).

2.4.1 Machine learning (autoaprendizaje o aprendizaje automático)

De acuerdo con el estudio realizado por el MIT, el aprendizaje automático abarca un amplio contexto de tecnologías y capacidades. Según ellos, existen tres enfoques diferentes:

a) Perspectiva de la computadora, programas que "aprenden".

b) Una perspectiva relacional, abarca reconocimiento de patrones basados en computadora, modelado estadístico y análisis para la toma de decisiones.

c) Perspectiva holística, combina algoritmos informáticos, patrones estadísticos e inteligencia artificial.

Hoy, hay tres principios tecnológicos que, cuando se agrupan, desbloquean los aspectos clave de cada perspectiva: Cloud Computing, Big Data e inteligencia artificial.

- Cloud Computing (computación en la nube): es el acceso por demanda a recursos computacionales incluyendo aplicaciones de software, almacenamiento, redes y otros servicios, que crea acceso ubicuo al software y a los datos. También dio lugar a formas creativas de colaboración.
- Big Data (grandes volúmenes de información): es la generación y recopilación de grandes cantidades de datos estructurados y no estructurados en la búsqueda de nuevos conocimientos y nuevas respuestas a los desafíos que enfrentan las organizaciones y los responsables de la toma de decisiones.
- Big Artificial Intelligence (inteligencia artificial): es la programación y los algoritmos que permiten a los dispositivos digitales acceder, combinar y compartir datos para aprender, explicar y pronosticar eventos, procesos y tendencias.

Como resultado, la computación cognitiva en la actualidad pretende extraer conocimiento de los grandes volúmenes de datos que se generan a una velocidad creciente y de una gran variedad, y hacer un uso inteligente de esos datos que se encuentran disponibles en diferentes formatos. El análisis de todos esos datos proporciona conocimiento para tomar decisiones, pero también las técnicas y herramientas de analítica predictiva, que permiten una gran capacidad para conocer las tendencias de futuro para las organizaciones y empresas. En la computación cognitiva, las tecnologías se entrenan y aprenden a partir de su propio conocimiento y no de la programación, como ocurre en la computación tradicional (Joyanes, 2017).

2.4.1.1 Apreciación

Cuando se analiza el Machine Learning desde la perspectiva de las ventajas y beneficios, se determina como inofensivo y favorable; sin embargo, el futuro parece muy distinto. El autor Roman V. Yampolskiy, señala que:

> El ritmo acelerado de cambio y el crecimiento exponencial en el poder de la computación conducirá a que la Inteligencia Artificial supere la capacidad intelectual humana en algún momento en el futuro cercano (aún en nuestras vidas) y alcance la "súper inteligencia" (ver también el concepto de singularidad del futurista Ray Kurzweil). Por un lado, la superinteligencia tendrá impactos positivos y resolverá los problemas más importantes de las humanidades (piense, por ejemplo, en la cura del cáncer), pero seguramente también tendrá impactos negativos. Tanto las ventajas como las desventajas son difíciles de predecir y se encuentran parcialmente en el campo de las "incógnitas desconocidas" (Yampolskiy, 2017, p. 6).

Es por esto que se hace necesario cuestionar, ¿qué ocurriría si esta tecnología se despliega para llevar a cabo ataques cibernéticos?

2.4.2 Nanotecnología

La nanotecnología, que abarca la ingeniería molecular, es una ciencia de la ingeniería que está diseñando y fabricando circuitos y dispositivos extraordinariamente pequeños que se construyen a nivel molecular de materia, típicamente de 1 a 100 nanómetros. Las combinaciones de nanomateriales pueden marcar el comienzo de una nueva era que nos proporciona computadoras y otros dispositivos con un poder de procesamiento hasta ahora inalcanzable. Con la

nanotecnología, todo tipo de medios y materiales que no han tenido capacidades de procesamiento y entrega de información pueden convertirse en nuevos portales de comercio y comunicación. Los materiales de nanoingeniería adoptarán nuevas propiedades físicas que son muy diferentes y más útiles que las propiedades físicas de sus estados naturales.

2.4.2.1 Apreciación

Esta tecnología también se desarrolla en el límite de lo desconocido, y como tal se sujeta al umbral de la incertidumbre. Al manipular los materiales a esta escala, los riesgos pueden ser impredecibles e imperceptibles a los sentidos, incrementando los grados de complejidad en lo que refiere a afectaciones éticas, legales, ambientales y de salud, entre otras. En lo que refiere específicamente a las Fuerzas Armadas, el autor Jürgen Altmann, afirma que:

> Se prevé que la nanotecnología (NT) traerá cambios revolucionarios en muchas áreas, con el potencial de grandes beneficios y grandes riesgos. El desarrollo en el Ejército podría implicar peligros específicos, cuya contención requerirá un análisis y esfuerzo especiales. La investigación y el desarrollo militar en NT se está expandiendo rápidamente. Las posibles aplicaciones futuras abarcan todas las áreas de guerra. Pueden surgir peligros especiales para el control de armas y la estabilidad de nuevas armas biológicas y microrobots. Para los humanos y la sociedad, los implantes corporales no médicos, posiblemente más aceptables a través del Ejército, plantean una serie de problemas relacionados con la naturaleza humana. Se necesita más investigación para encontrar la mejor manera de evitar posibles peligros. Para el corto y mediano plazo, se sugieren varias

pautas para límites y restricciones. Como primer paso, se debe mejorar la transparencia y la cooperación internacional (Altmann, 2004, p. 9).

2.4.3 Robotics (robótica)

La robótica no es una tecnología nueva en sí misma, pero en la última década, la robótica ha sufrido una transformación radical impulsada por tres características:

- Precisión: la capacidad de realizar tareas extremadamente exactas.
- Agilidad: la capacidad de realizar una variedad de tareas de forma rápida y fácil.
- Inteligencia: la capacidad de adquirir y aplicar nuevos conocimientos y habilidades.

Los robots son cada vez más utilizados en todos los sectores, en un sinnúmero de tareas en educación, agricultura, salud e incluso en la seguridad y defensa. Su rápida evolución pronto hará que la colaboración entre seres humanos y máquinas sea una realidad cotidiana, incrementando la eficiencia, precisión y velocidad, reduciendo los riesgos de tareas peligrosas y minimizando costo. Estos se suelen clasificar en cuatro grandes categorías: robots industriales, robots humanoides, robots colaborativos y robots virtuales (*bots* y *chatbots*) que, si bien son programas de software integrados en dispositivos físicos, se consideran robots virtuales o asistentes virtuales (Joyanes Aguilar, 2017).

2.4.3.1 Apreciación

Las personas que abogan más por el desarrollo y despliegue de los sistemas de armamento autónomos normalmente resaltan varias ventajas militares. En primer lugar, los sistemas de armamento autónomos actúan como un multiplicador de fuerza, es decir, se necesita un menor

número de soldados para cumplir una misión dada y se incrementa la eficacia de cada soldado. En segundo lugar, los defensores adscriben la expansión del campo de batalla a los sistemas de armamento autónomos, que permiten que el combate alcance áreas que previamente eran inaccesibles. En último lugar, los sistemas de armamento autónomos pueden reducir el número de bajas al quitar a los combatientes humanos de las misiones peligrosas (Marchant, 2011). Por otra parte, el autor Paul Scharre, en su libro *Army of None: Autonomous Weapons and the Future of War*, señala que "Una de las primeras áreas donde los países se verán obligados a lidiar con la elección de delegar la autoridad letal a la máquina será para los aviones de combate no tripulados diseñados para operar en áreas disputadas" (Scharre, 2019, p. 4). Por consiguiente, cuando se analiza esta tecnología con una visión mal intencionada, es preciso pensar que los contras para la seguridad y defensa de una nación podrían ser devastadores. ¿En quién podría recaer la responsabilidad cuando se despliegan los sistemas de arma que generan daños a la población, o cuando un sistema sea capaz de asumir su propio control?

2.4.4 3D printing (impresión en tres dimensiones)

Consiste en crear un objeto físico mediante la impresión capa por capa de un modelo o un dibujo en 3D. Con el tiempo, las impresoras 3D superarán los obstáculos de velocidad, costo y tamaño y su uso será más generalizado.

La impresión en 3D se usa principalmente para crear prototipos y producir componentes individuales. Estos métodos son conocidos también como fabricación aditiva, los cuales serán usados para producir pequeños lotes de productos personalizados que ofrecen ventajas de construcción, como son los diseños ligeros y complejos (Joyanes, 2017).

2.4.4.1 Apreciación

Esta tecnología ofrece ventajas y también varias desventajas, relacionadas con la creación propia de productos de forma automatizada mediante una impresora 3D. Entre las ventajas están la flexibilidad y prototipado rápido, reducción de costos, personalización, nueva industria y sector, así como aplicaciones múltiples aún por descubrir. Sin embargo, analizado desde la orilla de los malintencionados, existe la posibilidad de crear objetos tales como armas de fuego, y el peligro de llegar a una falsificación sin límites, impresión de drogas y armas, entre otros. Adicionalmente, los riesgos cada día son mayores, según lo afirma la empresa Sculpteo en su artículo "The state of 3D Printing": "La disminución de costos sigue siendo, con mucho, la tendencia más citada, año tras año. Esto tiene sentido ya que un menor costo de impresión 3D significa un uso más fácil de esta tecnología. Además, la impresión 3D en metal sigue apareciendo como una de las tendencias con mayor impacto" (Sculpteo, 2018).

2.4.5 Biotechnology (biotecnología)

Es el uso de sistemas vivos y organismos para desarrollar o fabricar productos. En la actualidad, los avances en tecnología digital, ingeniería genética, informática, tecnología celular y ciencias químicas están ampliando enormemente los límites de la biotecnología. La noción de la ingeniería de las células vivas y el surgimiento de la industria de las ciencias de la vida cambiará radicalmente los límites de la atención médica, la agricultura y los productos químicos.

2.4.5.1 Apreciación

La biotecnología apunta a ser una de las áreas de mayor importancia en la sociedad, particularmente en el siglo XXI. Pero a pesar de las ventajas que aporta, también conlleva una serie de riesgos, principalmente en el medio ambiente y en la salud, como la modificación de la estructura del genoma humano, clonación y la manipulación del material genético de nuestra especie, entre otros. Según un estudio de percepción realizado por los autores Kirkpatrick, Klobentz, Palmer, Denton y Tiu en su artículo "Biotechnology Governance: Landscape and Options", realizado en 2018: "El rápido avance de las técnicas de edición del genoma, y su adopción por una amplia gama de usuarios, ha despertado la preocupación de que tanto los actores estatales como los no estatales puedan tratar de aprovechar los avances del genoma para sus propios fines hostiles" (Kirkpatrick, Klobentz, Palmer, Denton, 2018, p. 2).

2.4.6 Wireless Mesh Networks (redes de malla inalámbricas)

Las redes de malla inalámbricas (WMN) son circuitos *ad hoc* de conectividad inalámbrica en los que solo un dispositivo requiere una conexión a internet. Estas son redes inteligentes de dispositivos inalámbricos que se pueden formar, dispersar y reformar según el comando del usuario. En cuanto las WMN se crean de abajo hacia arriba mediante conexiones entre dispositivos, sus capacidades de autoformación y autocuración aseguran una comunicación robusta y confiable en cualquier lugar a bajo costo y sin infraestructura fija. Las WMN amplían la informática generalizada integrada en el IoT, haciéndolo más dinámico.

2.4.6.1 Apreciación

Esta tecnología presenta muchos beneficios. Entre los más significativos están: la innovación y menor costo, al tiempo que los contras se consolidan en que no existen sistemas de regulación para controlar este tipo de tecnología y con ello, se integran un sinnúmero de delitos cibernéticos. Las redes inalámbricas de malla se consideran una solución prometedora para ofrecer acceso de bajo costo a servicios de banda ancha; sin embargo, uno de los principales desafíos en el diseño de estas redes es su vulnerabilidad a los ataques de seguridad (Sgora, Vergados, & Chatzimisios, 2013).

2.4.7 Pervasive computing (computación omnipresente)

También conocida como computación ubicua, la cual brinda información, medios, contexto y poder de procesamiento, donde sea que estemos. Esta clase de tecnologías se caracteriza por amplias redes de microprocesadores conectados o incrustados en objetos cotidianos, los datos se integran y se intercambian en las redes públicas.

La computación omnipresente es la tecnología que impulsa internet de las cosas (IoT), pero es más preciso pensar en ella como el motor de todo el internet. Las capacidades de información, intercambio y colaboración de estas redes no se limitan a ningún dispositivo o ubicación fija; se distribuyen por todo el mundo en el que vivimos. Además, el factor de forma de la informática dominante puede ser móvil, usable o implantable.

2.4.7.1 Apreciación

El internet de las cosas como toda tecnología disruptiva, su revolución conlleva una serie de ventajas y de desventajas. Entre los riesgos más significativos que aporta esta tecnología a la

seguridad nacional están: la falta de compatibilidad, la complejidad que representan y la falta de privacidad y seguridad, considerando que existe la posibilidad de que el software pueda ser vulnerado y los datos personales mal empleados.

En consecuencia, cada una de estas tecnologías, sin lugar a dudas, marcará un cambio profundo y sistémico en la sociedad, facilitará los procesos y hará más eficiente la vida. Sin embargo, estas tecnologías también traerán consigo novedosas y peligrosas amenazas y ataques de tipo cibernético que pondrán en riesgo no solo a los individuos, sino a la nación.

2.4.8 La ventana de AREM

En esta sección se analizarán las amenazas cibernéticas haciendo uso del instrumento denominado "Ventana de AREM" (Cano, 2014), el cual brinda una visión más amplia de las amenazas, riesgos y vulnerabilidades cibernéticas, con el fin de avanzar hacia una gestión y gobierno de los riesgos empresariales basado más en las posibilidades que en las probabilidades, a fin de visualizar la incertidumbre. En este sentido, se plantea la Ventana de AREM, como una vista estratégica y táctica de actuación de los altos mandos, para comprender los aspectos conocidos y desconocidos de las capacidades militares en materia cibernética, en el contexto de aquellos riesgos y amenazas propias del entorno, así como de los vectores de inestabilidades emergentes que se deben identificar dentro y fuera de la realidad institucional (adaptado de Cano, 2014).

A continuación, se presenta la Ventana de AREM que establece las diferentes zonas de alcance de las amenazas y riesgos conocidos, focalizados, latentes y emergentes como una forma de motivar el análisis del alto mando y provocar las ideas que "en tiempos de guerra" permitan encontrar

maneras de sobrevivir ante posibles escenarios adversos. Las amenazas y riesgos conocidos son las situaciones tradicionales que se presentan en la institución.

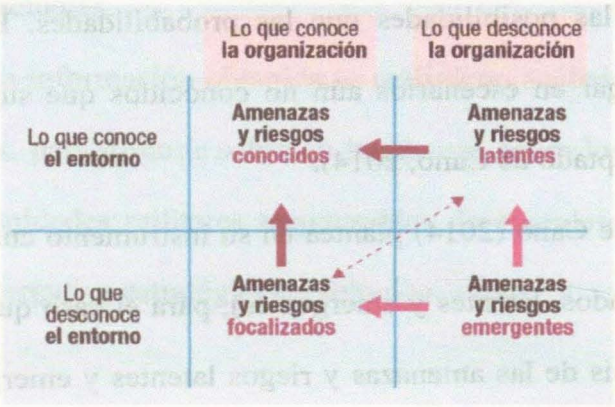

Figura 4. La ventana de AREM

Fuente: Cano (2017).

Las amenazas y riesgos latentes, son aquellas circunstancias que se advierten en el entorno y que son generalmente desconocidas en el contexto de negocio de las empresas. Dichas situaciones se manifiestan de manera frecuente y son detectadas por los analistas, sugiriendo patrones y condiciones particulares a través de las cuales se pueden presentar. Su comportamiento es asimétrico y genera ruido e incertidumbre en el entorno, condiciones propias de una sorpresa predecible. Las amenazas y riesgos focalizados son situaciones propias de una industria o sector de negocio, que afectan la competitividad y posicionamiento de una empresa en un nicho específico. Son escenarios por lo general desconocidos en el entorno, pero conocidos por la institución, dado que esta última reconoce y sabe el comportamiento de su sector. Este tipo de amenazas y riesgos focalizados deben instar al sector militar a estudiar de manera permanente los avances y novedades en materia de ciberdefensa, para identificar nuevas formas de hacer las cosas y crear los escenarios donde la institución pueda movilizarse sobre las inestabilidades del sector y

alcanzar una posición privilegiada. Finalmente, y no menos importante, son las amenazas y riesgos emergentes. Esos momentos, ideas y propuestas de contextos que retan las capacidades del sector militar y privilegian más las posibilidades que las probabilidades. En este sentido, se hace necesario pensar e investigar en escenarios aún no conocidos que suponen per se cambios o situaciones disruptivas (adaptado de Cano, 2014).

Sin embargo, a pesar de que Cano (2014) plantea en su instrumento cuatro tipos de amenazas o riesgos (conocidos, focalizados, latentes y emergentes), para el caso que nos ocupa, el presente estudio se limitará al análisis de las amenazas y riegos latentes y emergentes que presentan las tecnologías disruptivas para Colombia a corto plazo, a fin de plantear una estrategia militar que permita dar respuesta y ser efectiva de cara a un análisis prospectivo a 2022.

En primer lugar, partiendo de las definiciones de amenaza latente (el analista se ha enterado de que tal amenaza existe y no sabe si la organización tiene alguna estrategia de mitigación) y amenaza emergente (el analista nunca había escuchado de tal amenaza) (Cano, 2018), para aplicar este instrumento un analista de riesgos recolectó y analizó durante un tiempo (generalmente un año), material suficiente de tendencias visibles y emergentes sobre nuevas y posibles amenazas o vectores de ataque, las cuales se valoraron y priorizaron de acuerdo con su nivel de impacto en la organización, novedad del ataque y capacidad de respuesta actual de las unidades de ciberdefensa. Con base en este resultado, se estableció una lista de posibles amenazas y riesgos cibernéticos contrastadas con cada una de las siete tecnologías disruptivas mencionadas en la sección anterior, a fin de identificar las posibles amenazas que podrían afectar la seguridad y defensa nacional en un futuro inmediato, las cuales fueron valoradas por los investigadores asistidos con la Ventana de AREM. Posteriormente, se priorizaron y compilaron los diferentes análisis, identificando las

mayores coincidencias en las ubicaciones en los diferentes cuadrantes, para luego afinarse con el conocimiento del autor de este trabajo de investigación, en las realidades concretas del país y sus niveles de aseguramiento actuales.

Por consiguiente, con la información obtenida se realizó un análisis detallado de cada una de las amenazas identificadas, para discutir sobre su incidencia sobre los dos primeros elementos: ciberdefensa nacional y unidades militares responsables de ciberdefensa, para de esta manera proceder a plantear una alternativa estratégica de solución.

3. Estrategia militar de ciberdefensa

3.0 Introducción

Colombia se enfrenta a una amenaza cibernética, pero esta situación está ocurriendo también en varios países del mundo. Las grandes naciones europeas, como el Reino Unido y Francia, centran sus esfuerzos defensivos en medidas proactivas, que buscan neutralizar las amenazas antes de que se materialicen. Otra herramienta de los grandes poderes es la disuasión mediante el escarmiento, un intento de prevenir acciones hostiles con la promesa de represalias severas. Así lo afirma el autor Joseph Nye:

> El escarmiento es posible tanto contra los Estados como contra los delincuentes, pero los problemas de atribución a menudo lentos y contundentes determinan los efectos negativos. Con tiempo y esfuerzo, es probable que una agencia militar o de inteligencia importante penetre en la mayoría de las defensas, pero la combinación de amenaza de castigo más defensa efectiva puede influir en los cálculos de costos y beneficios (Nye, 2017, p. 68).

Los poderes más pequeños, por el contrario, carecen de los recursos necesarios para implementar medidas proactivas o disuasión. En su lugar, se centran en métodos reactivos como la resistencia y la redundancia, que buscan absorber el daño del ataque. Se esfuerzan por evitar ataques cibernéticos importantes al participar en organizaciones regionales como la OTAN. Independientemente de sus diferencias en el enfoque doctrinal, las pequeñas y grandes naciones enfrentan un desafío común: cómo vencer una amenaza novedosa en ausencia de una experiencia concluyente sobre la cual se hace necesario revisar la estrategia (Van der Meer, 2016).

Es por esto que la estrategia militar de ciberdefensa asegura un enfoque conjunto, integral y sistémico que permita integrar los diferentes frentes y aristas relacionadas con la ciberseguridad y

ciberdefensa nacional para mejorar la eficacia operacional en el ciberespacio, proporcionando principios fundamentales que guíen el empleo de las unidades de las Fuerzas Militares de Colombia (FF.MM.) hacia un objetivo común. Es necesario aclarar que las Fuerzas Militares de Colombia es el término usado para denotar colectivamente todos los componentes del Ejército, Armada y Fuerza Aérea (COGFM, 2018).

3.1 DOMPILEM

Los componentes de capacidad abreviados en la sigla DOMPILEM son aquellos aspectos que deben observarse en el planeamiento por capacidades, tanto en las soluciones materiales como en las no materiales, ante los requerimientos de la Fuerza para afrontar los retos presentes y futuros. Esta sigla también es empleada en la OTAN con una "I" adicional al final para indicar interoperabilidad, o con una "P" para incluir aquellas políticas gubernamentales o institucionales que afectan la capacidad (EJC, 2017, p. 19).

La doctrina es generalmente el primer aspecto, ya que a menudo es el más fácil y rápido de actualizar y puede afectar drásticamente el desarrollo de las operaciones. En algunos casos, el impacto de los cambios en los otros componentes no puede realizarse plenamente sin alterar de manera significativa la doctrina. Además, la doctrina también puede servir como base para la evolución en las otras categorías DOMPILEM (EJC, 2017):

- Doctrina: cómo se combate. Arte operacional, tácticas, técnicas, procedimientos, tareas.
- Organización: cómo es el diseño de la fuerza. Funciones, estructura y protocolo organizacional.

- Material: elementos necesarios para equipar las Fuerzas con el fin de que puedan operar de manera efectiva. Disponibilidad.
- Personal: recurso humano necesario para combatir en la guerra, enfrentar contingencias o participar en operaciones de paz.
- Instalaciones: bienes inmuebles.
- Liderazgo y educación: cómo preparar a los comandantes en cada uno de los escalones para conducir el combate a través del desarrollo profesional.
- Entrenamiento: cómo debe ser la preparación para el combate desde la formación básica hasta la formación individual de especialistas y el entrenamiento en los diferentes escalones.
- Mantenimiento: actividades que se requieren para el sostenimiento de la capacidad en el tiempo. Niveles de mantenimiento, sistemas de abastecimiento.

3.2 Estrategia basada en DOMPILEM

El desarrollo de una estrategia presupone analizar

> [...] cuál ha sido, y será en el futuro, la incidencia de la evolución industrial del hombre en la guerra. No se puede desconocer, que sumado a elementos como la estrategia, la moral, el entrenamiento, logística y doctrina, el factor tecnológico ha sido determinante en el desarrollo de los conflictos armados (Gaitán, 2012, pp. 61-69).

Adicional a esto, se hace necesario estudiar el ejercicio de emplear los computadores, el internet y el ciberespacio por parte de un Estado (mediante sus fuerzas de defensa y seguridad) con el objetivo de defender, neutralizar o causar daños suntuarios sobre otro (adversario, enemigo),

mediante el desarrollo de ataques que van dirigidos por lo general hacia su infraestructura crítica militar y civil en o a través del ciberespacio.

Por lo tanto, se hace necesario conocer los componentes y características del ciberespacio que lo convierten en un dominio de guerra diferente a los que se conocen hace mucho tiempo: tierra, mar, aire y espacio. El ciberespacio debe comprenderse de manera estratégica, ya que solo así es posible entender también de qué manera puede ser utilizado para las intervenciones entendidas como ciberguerra. Ese espacio no está restringido a internet; ese es apenas el medio por el cual los ataques se podrían manifestar.

Según los autores Richard A. Clarke y Robert K. Knake's en su libro *Cyber War: The Next Threat to National Security and What to Do About It* (2010), afirman que el ciberespacio es dominio tanto físico como virtual, sin límites claros, donde hasta la fecha no existe ninguna ley o doctrina internacional que rige el ciberespacio global. Según los autores, el ciberespacio tiene cuatro (4) elementos: contexto físico, fundamentos lógicos, contenidos y actores. Sin embargo, basados en la doctrina militar de varios países que fueron estudiados, los componentes del ciberespacio son cuatro (4), como se indica en la siguiente tabla:

Tabla 2

Componentes del ciberespacio

Componente gobernanza		
Componente de sistemas	Componente de contenido y aplicaciones	Componente de personas y sociedad

Fuente: Clarke y Knake (2010).

- Componente de sistemas: consiste en los aspectos técnicos, infraestructura y la arquitectura del ciberespacio. Este componente incluye la plataforma tecnológica y de telecomunicaciones (hardware y software), la que permite brindar servicios al exterior.
- Componente de contenido y aplicaciones: se refiere a la información que se contiene en el ciberespacio y las herramientas utilizadas para acceder y procesar esa información. Este componente se basa en el componente de sistemas y proporciona las aplicaciones, programas y desarrollos de software para que los usuarios puedan gestionar y compartir información. Es un componente dinámico, por el desarrollo permanente de nuevas aplicaciones que permiten a los usuarios interactuar entre sí y su información de una manera más flexible y sensible.
- Componente de personas y sociedad: se refiere a las comunicaciones e interacciones entre las personas en el ciberespacio y la información que comparten. Los dos anteriores componentes del ciberespacio permitieron el crecimiento de las personas y componente social por facilitar la creación de comunidades en el ciberespacio para acceder y compartir información entre los usuarios.
- Componente de gobernanza: este componente afecta a todos los componentes anteriores de ciberespacio. Los mecanismos para la gobernanza de internet son extremadamente complejos y requieren la inversión de recursos considerables para lograr los objetivos de ser abierta y democrática, transparente, dinámica, adaptable, responsable, eficiente y eficaz.

Con esto en mente, y tomando como referencia el modelo DOMPILEN, se determinaron las necesidades para las unidades militares responsables de la ciberdefensa para cada uno de los elementos.

3.2.1 Doctrina

La doctrina, (manuales y reglamentos) representa uno de los factores fundamentales para el desarrollo de las operaciones militares cibernéticas, considerando que son documentos elaborados sistemáticamente para indicar las actividades que deben ser cumplidas por las Unidades responsables de la ciberdefensa y la forma en que las mismas deberán ser realizadas, ya sea conjunta o separadamente en concordancia con la misión, visión y objetivos de las Fuerzas Militares.

3.2.1.1 Manuales

- Desarrollar doctrina militar cibernética conjunta y por cada Fuerza de acuerdo a su rol funcional.
- Actualizar periódicamente la doctrina generada en materia cibernética.

3.2.1.2 Reglamentos

- Definir reglamentos de ciberdefensa, dirigidos a la generalidad, que las unidades responsables de ciberdefensa y demás actores están obligados en su conjunto a respetar, aunque no afecte a todos por igual, ya que puede estar dirigido a la Seguridad Nacional.

3.2.2 Organización

La organización de las unidades militares cibernéticas se plantea a corto plazo; sin embargo, el panorama internacional muestra cómo las grandes potencias como Rusia, Alemania, China y

Estados Unidos han optado por la conformación de Fuerzas para afrontar las amenazas del nuevo dominio de la guerra.

3.2.2.1 Unidades militares cibernéticas

Con base en la experiencia vivida durante ocho años y en los *benchmarking* desarrollados al interior del Comando Conjunto Cibernético en el año 2018, fue posible evidenciar que el desarrollo de las capacidades cibernéticas de las Fuerzas Militares en Colombia solo será posible si en el Ejército Nacional, Armada Nacional y Fuerza Aérea Colombiana, se cuenta con unidades militares operativas expertas en ciberdefensa, dedicadas única y exclusivamente al desarrollo de operaciones militares cibernéticas, de acuerdo con su rol funcional.

3.2.2.2 Equipos de combate

Cada Fuerza debe contar con mínimo una unidad militar cibernética, la que a su vez deberá estar conformada por mínimo seis (6) equipos de combate cibernético, capaces de desplegar operaciones militares cibernéticas, capacitados de acuerdo con su funcionalidad: defensa, ataque o inteligencia. Los equipos de combate, podrán desplegar operaciones desde la ciudad principal que operen, o podrán desplazarse a la unidad de mando adelantada que lo requiera.

3.2.3 Material

Dotar a las unidades cibernéticas de las fuerzas y el comando general de infraestructura adecuada para el cumplimiento de las funciones de ciberseguridad y ciberdefensa.

3.2.3.3 Plataformas tecnológicas y de comunicaciones

- Fortalecer las plataformas tecnológicas y de comunicaciones, a fin de garantizar el cumplimiento de funciones de ciberseguridad y ciberdefensa.
- Garantizar que las Tecnologías de la Información y Comunicaciones adquiridas por las Fuerzas Militares, sean sometidas a unos protocolos de verificación y certificación de seguridad.
- Hacer uso de la industria 4.0 para sacar provecho de sus beneficios, siempre y cuando no impacten la seguridad y defensa nacional.

3.2.3.4 Dotación de unidades especiales y laboratorios

- Implementación de unidades especiales de forma descentralizada a nivel nacional.
- Implementación de laboratorios especializados en ciberdefensa, juegos de simulación de crisis cibernéticas para infraestructuras críticas, juegos de guerra cibernéticos y prácticas forenses.
- Implementación de unidades móviles y de respuesta rápida.

3.2.3.5 Plataformas de ciberdefensa

- Adquirir plataformas que hayan sido debidamente probadas y aprobadas por la Junta de Ciberseguridad y Ciberdefensa.
- Garantizar la adquisición centralizada para herramientas cibernéticas a fin de garantizar economía de escala e interoperabilidad.

- Fortalecer el desarrollo de herramientas y artefactos cibernéticos (hardware y software) propias de las Fuerzas para la Seguridad y Defensa de la Nación.

3.2.4 Personal

Corresponden al componente fundamental dentro de la estrategia, al cual se debe fortalecer y brindar garantías en diferentes componentes, con base en los siguientes principios.

3.2.4.1 Selección de personal

- Fortalecer la incorporación de personal en las especialidades requeridas para desarrollar tareas propias de ciberseguridad y ciberdefensa.
- Realizar selección del personal de ciberdefensa por competencias.
- Garantizar que durante el proceso de selección se realizarán estudios de seguridad y pruebas de confiabilidad.
- Dotar a las Fuerzas Militares de personal técnico especializado en ciberseguridad y ciberdefensa. El personal que desempeñe funciones de expertos cibernéticos en sus diferentes niveles en las unidades cibernéticas, será personal militar (oficiales, suboficiales y soldados). Sin embargo, se podrán contratar asesores especializados para temas específicos que requieran la experticia en determinado tema donde la Fuerza no cuente con dicho personal.
- Evaluar el área de desempeño del personal, de acuerdo a sus competencias y formación.

- Considerar los heridos en combate para incorporarlos en las unidades de ciberdefensa y ciberseguridad de las Fuerzas.

3.2.4.2 Rotación de personal

Garantizar traslados entre las unidades cibernéticas de las Fuerzas y el Comando General en periodos mínimos de cuatro (4) años, a fin de optimizar la inversión realizada en cada uno de los funcionarios y garantizar el retorno de inversión.

3.2.4.3 Plan de carrera personal de ciberdefensa

- Desarrollar el plan de carrera para oficiales, suboficiales y soldados, basado en roles y perfiles que garanticen la operación cibernética.
- Mantener actualizado el plan de carrera del personal, de acuerdo a los avances en materia de ciberseguridad y ciberdefensa.
- Contemplar como obligatorio el estudio de una segunda lengua extranjera en la formación del personal de las unidades cibernéticas.
- Especializar al personal de suboficiales en el área técnica a través de cursos con certificación a nivel internacional.
- Orientar y enfocar la capacitación del personal, de acuerdo con sus competencias o perfil.

3.2.4.4 Incentivos al personal experto en ciberdefensa

- Gestionar estrategias, políticas o mecanismos que incentiven la permanencia del personal de ciberdefensa en la institución.
- Gestionar un incentivo económico o "prima de ciberdefensa", para el personal que se desempeñe en actividades de ciberdefensa.
- Crear medallas, condecoraciones y distintivo de ciberdefensa que identifique al personal de ciberdefensa y lo incentive a pertenecer a las unidades cibernéticas.
- Reconocer la labor del personal destacado mediante capacitaciones en el exterior o universidades de prestigio a nivel nacional.

3.2.5 Instalaciones

Dotar a las unidades cibernéticas de las Fuerzas y el Comando General de infraestructura física (instalaciones) adecuada para el despliegue de operaciones cibernéticas.

3.2.5.1 Edificio inteligente

Contar con unas instalaciones donde puedan ubicarse las unidades cibernéticas de las tres Fuerzas y el Comando General.

3.2.5.2 Centro de cómputo conjunto

Garantizar un centro de cómputo único que permita compartir plataformas tecnológicas entre las unidades cibernéticas de las tres Fuerzas y el Comando General.

3.2.6 Legislación y educación

Se hace necesario garantizar la existencia de un marco legal, normativo y doctrinario que proteja las actividades y operaciones cibernéticas.

3.2.6.1 Ley de ciberdefensa

Promover iniciativas o participar de aquellas que permitan desarrollar el marco legal que respalde las actuaciones en el ciberespacio, especialmente a los organismos que desarrollarán operaciones cibernéticas.

3.2.6.2 Reglas de enfrentamiento en el ciberespacio

- Definición, regulación, y protección de los cibercomandos y las actuaciones de las Fuerzas Militares en el ciberespacio.
- Definición de las reglas de enfrentamiento en el ciberespacio, alineadas con los Derechos Humanos (DD.HH.) y el Derecho Internacional Humanitario (DIH).
- Regulación, facultades para la declaración e intervención en una ciberguerra, y las normas y leyes que las regirán.

3.2.6.3 Programas de ciberdefensa

- Crear programas de ciberdefensa que puedan ser aplicados a diferentes niveles educativos, como escuelas de formación y cursos de capacitación.
- Realizar ejercicios de simulación o juegos de guerra que permitan adiestrar el personal militar en manejo de crisis y toma de decisiones en ciberdefensa.

- Desarrollar programas de capacitación especializados en ciberseguridad y ciberdefensa.
- Generar programas de formación avanzada en ciberseguridad y ciberdefensa.
- Participación en eventos y foros de actualización nacionales e internacionales.

3.2.6.4 Centros de investigación y pensamiento

- Promover la creación de centros de investigación y pensamiento cibernético que contribuya al mejoramiento y desarrollo de capacidades de ciberdefensa con base en la experiencia, entrenamiento, conocimientos, investigación para la producción y desarrollo de conocimiento.
- Coordinación de esfuerzos encaminados a fortalecer y fomentar el desarrollo, investigación e industrialización de nuevas e innovadoras tecnologías a través de la investigación y el desarrollo centrado en robustecer el ecosistema de la ciberdefensa del país.
- Crear, ampliar y fortalecer la comunidad de investigación nacional pública, privada y militar, fomentando y brindando las herramientas y recursos necesarios, mediante la colaboración nacional e internacional.
- Fomentar la línea de investigación de ciberseguridad y ciberdefensa con proyectos de innovación cibernética que permitan apropiarse de la cadena logística de aprovisionamiento de los equipos activos de seguridad.

- Crear un centro de excelencia en ciberseguridad y ciberdefensa con capacidades de entrenamiento, capacitación, investigación, desarrollo, generación de lecciones aprendidas y consultoría.
- Generar publicaciones de alto nivel, realizar ejercicios de ciberdefensa y cursos técnicos, promover iniciativas de creación de leyes nacionales e internacionales para el manejo de las operaciones cibernéticas,
- Establecer el Observatorio Nacional que permita recopilar y procesar la información de los ataques e incidentes que pasan en Colombia a nivel de infraestructuras críticas cibernéticas.

3.2.6.5 Programas de prevención y sensibilización

- Desarrollar programas de prevención/sensibilización en las unidades a nivel nacional, a fin de evitar ataques a la infraestructura crítica del sector Defensa.
- Desarrollar y fomentar la creación e implementación de herramientas y recursos adecuados para la creación y mantenimiento de una cultura cibernética en las Fuerzas Militares.
- Desarrollar módulos virtuales de aprendizaje en ciberseguridad y ciberdefensa, que permitan sensibilizar en forma masiva al personal de las FF.MM.
- Desarrollar un programa de difusión de una cultura de ciberseguridad y ciberdefensa.

3.2.7 Entrenamiento

Garantizar la preparación para el combate cibernético desde la formación básica hasta la formación individual de cibercomandos y el entrenamiento en los diferentes escalones.

3.2.7.1 Centro de excelencia en ciberdefensa

Implementar un centro de excelencia en ciberdefensa, como centro principal de ciberdefensa para el país, donde se trabajarán diferentes aspectos como investigación, innovación, desarrollo, monitoreo y educación.

3.2.7.2 Intercambios académicos

- Realizar intercambios académicos con unidades militares cibernéticas o comandos cibernéticos de los países amigos, a fin de compartir experiencias e información de ciberdefensa.
- Apoyar el desarrollo e implementación de las iniciativas, mediante incentivos académicos, que logren el fin común de fortalecer la ciberdefensa del país.
- Establecer convenios de cooperación académica y de investigación que promuevan la movilidad de: docentes, alumnado, y publicaciones tanto físicas como virtuales.

3.2.8 Mantenimiento

Garantizar el mantenimiento y renovación de las plataformas tecnológicas, permitirá garantizar la permanencia y fortalecimiento de las unidades cibernéticas del país.

3.2.8.1 Plataformas tecnológicas

Garantizar el mantenimiento preventivo y correctivo de las plataformas tecnológicas de información, comunicaciones y operación, para soportar el desarrollo de las operaciones militares cibernéticas.

3.2.8.2 Instalaciones

Realizar el mantenimiento de las instalaciones de las unidades cibernéticas para garantizar su correcto funcionamiento.

La aplicación del modelo DOMPILEN permitió identificar el planeamiento necesario para desarrollar capacidades de ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia, tanto en las soluciones materiales como en las no materiales, ante los requerimientos y necesidades de las unidades cibernéticas de las Fuerzas para afrontar los retos presentes y futuros en materia cibernética.

En la siguiente tabla, se presenta la relación de los procesos, líneas estratégicas que de manera articulada y continua podrán entregar productos para el desarrollo de capacidades de ciberseguridad y ciberdefensa, conforme a los lineamientos políticos y las prioridades estratégicas de defensa y seguridad, en las capacidades operacionales requeridas para la proyección y el desarrollo en una estructura de fuerza flexible, adaptable y sostenible.

Tabla 3

Relación de los procesos, líneas estratégicas y productos con base DOMPILEM

Elemento	Línea estratégica	Producto
Doctrina	Manuales	Fundamento legal
	Reglamentos	Organización
Organización	Unidades militares	C4ISR
	Equipo de combate	Operaciones militares
Material	Plataformas TIC y TO	Disponibilidad medios
	Dotación equipo cibernético	Movilidad
	Plataformas de ciberdefensa	Defensa y ataque
	Armas cibernéticas	Fuegos
Personal	Selección personal	Competencias
	Rotación	Capacidades permanentes
	Plan de carrera	Fortalecimiento capacidades
	Incentivos	Retención
Instalaciones	Edificio inteligente	Medios físicos
	Centro cómputo	Capacidad cómputo conjunta
Legislación/Educación	Ley ciberdefensa	Fundamento legal
	Reglas enfrentamiento	Límites
	Programa ciberdefensa	Capacitación persistente
	Centros de investigación/Laboratorios	I+D+i
	Programas de prevención	Minimizar riesgos
Entrenamiento	Centro de excelencia	Capacidades cibernéticas
	Intercambios académicos	Complemento educativo
Mantenimiento	Plataformas tecnológicas	Funcionamiento/actualización
	Instalaciones	Funcionalidad

Fuente: Elaboración propia.

De esta manera, se evidencia que el modelo de planeamiento por capacidades, se ajusta a la planeación de la ciberdefensa nacional, a fin de prever los requerimientos necesarios para desarrollar la capacidad de planear y ejecutar operaciones militares cibernéticas.

3.3 Relaciones del modelo

Los productos obtenidos a través del modelo DOMPILEM, permitirán dar respuesta a los requerimientos de las unidades de ciberdefensa, con el propósito de desarrollar capacidades que permitan el desarrollo de operaciones militares cibernéticas.

De esta manera, es posible evidenciar cómo cada uno de los productos contribuye notablemente para ejercer la ciberdefensa nacional a cargo de las unidades militares dentro de su ámbito de competencia, conforme a la ley, para defender y proteger la soberanía, los intereses nacionales, los activos críticos cibernéticos y recursos clave para mantener las capacidades frente a amenazas o ataques de naturaleza cibernética, cuando estos afecten la seguridad nacional.

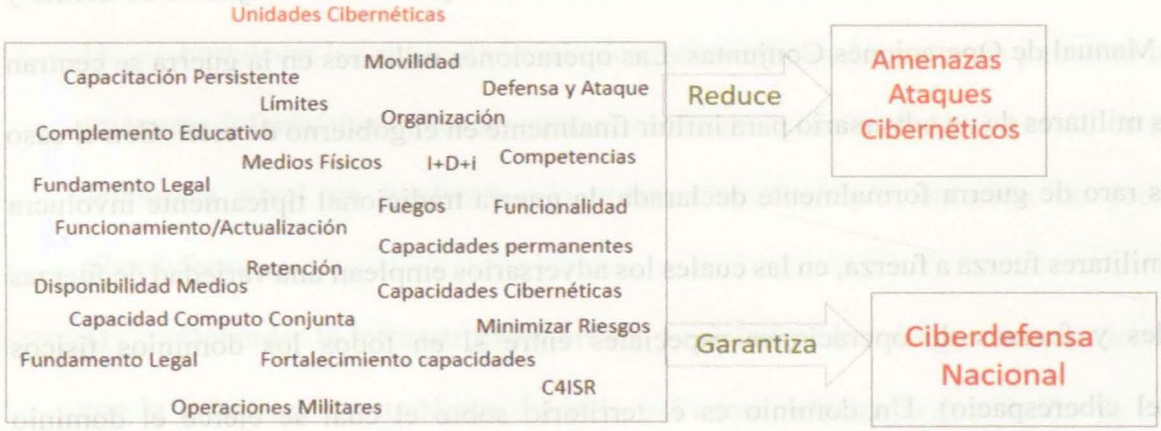

Figura 5. Relación productos vs. elementos esenciales

Fuente: Elaboración propia.

3.4 Estrategia propuesta

Como resultado del análisis de la amenaza y el contexto actual, se propone contar con una estrategia militar conjunta, integral y sistémica que permita integrar los diferentes frentes y aristas

relacionadas con la ciberseguridad y ciberdefensa nacional y admita mejorar la eficacia operacional en el ciberespacio, proporcionando principios fundamentales que guíen el empleo de las unidades de las Fuerzas Militares de Colombia (FF.MM.) hacia un objetivo común. Es necesario aclarar que las Fuerzas Militares de Colombia, es el término usado para denotar colectivamente todos los componentes del Ejército, Armada y Fuerza Aérea (COGFM, 2018, pp. 1-2).

En este orden de ideas, la estrategia propuesta contempla los principios de la guerra a los que se acogen las Fuerzas Militares de Colombia, los cuales se encuentran enunciados en el manual fundamental de referencia del Ejército MFRE 3-0, enfocadas para su empleo en el ámbito conjunto. La aplicación de estos principios clásicos en la conducción de operaciones conjuntas se define y amplía en el Manual de Operaciones Conjuntas. Las operaciones militares en la guerra se centran en las fuerzas militares de un adversario para influir finalmente en el gobierno de este. Con el caso cada vez más raro de guerra formalmente declarada, la guerra tradicional típicamente involucra operaciones militares fuerza a fuerza, en las cuales los adversarios emplean una variedad de fuerzas convencionales y fuerzas de operaciones especiales entre sí en todos los dominios físicos (incluyendo el ciberespacio). Un dominio es el territorio sobre el cual se ejerce el dominio (terrestre, marítimo, aéreo, espacial y el ciberespacio) (COGFM, 2018, pp. 1-29).

Así mismo, con base en los niveles de la guerra: a) estratégico nacional, b) teatro estratégico, c) operacional y d) táctico (MFC 1.0 (1-44)), se definió y clarificó la relación entre los objetivos nacionales, el enfoque operacional y las tareas tácticas, toda vez que no hay demarcaciones o límites definidos entre estos niveles, pero ayudan a los comandantes a diseñar y sincronizar operaciones, asignar recursos y tareas al comando apropiado. En otras palabras, el propósito

estratégico, operacional o táctico del empleo depende de la naturaleza del objetivo, la misión o la tarea (COGFM, 2018, pp. 1-16).

Es por esto que la estrategia de ciberdefensa propuesta se centra en la construcción y fortalecimiento de capacidades para el desarrollo de operaciones cibernéticas para operar en un entorno donde se disputa el acceso al ciberespacio. Funciona en un entorno donde el acceso a las comunicaciones podría ser interrumpido, con el propósito de impedir y anticipar los ataques y hacer la defensa del país contra cualquier adversario que intenta hacer daño a los intereses nacionales en tiempos de paz, crisis o conflicto, para así, dar cumplimiento a las funciones asignadas al CCOCI mediante el CONPES 3701 "Lineamientos de Política para Ciberseguridad y Ciberdefensa" del año 2011, así:

1) Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.

2) Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.

3) Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional (capacidades cibernéticas integradas para apoyar las operaciones militares y planes de contingencia) (Gobierno de Colombia, 2011).

Mediante esta estrategia se propone planificar, desarrollar y utilizar las capacidades de las Fuerzas Militares de manera efectiva, y asegurar que las operaciones cibernéticas se produzcan de manera consistente con los valores que promueve Colombia tanto a nivel nacional como internacional.

Introducción

El ciberespacio es, por naturaleza, un espacio abierto carente de características tangibles, donde los sectores público y privado, civiles y militares, nacionales y actores internacionales interactúan simultáneamente de forma interdependiente e interconectados. Este dominio, no es un espacio seguro y protegido, por lo que es vulnerable a los ataques cibernéticos, lo que puede resultar en pérdidas significativas para los sectores económico, político, social y/o constituir una seria amenaza para la defensa o los intereses nacionales. Se entiende, por lo tanto, que el ciberespacio constituye un nuevo dominio de operación, donde las operaciones militares de protección y de defensa siguen la misma lógica y principios que caracterizan la seguridad y defensa del Estado. Es significativa la importancia que tiene declarar que las misiones de las unidades cibernéticas de las Fuerzas Militares, dependen del uso del ciberespacio para llevar a cabo las operaciones cibernéticas.

Objetivo global

Proporcionar dirección, coherencia y lineamientos con un enfoque integral para el desarrollo de capacidades militares en el ciberespacio al 2022.

Objetivos estratégicos

a) Objetivo Estratégico 1 (OE1): Fortalecer el pie de fuerza requerido para dar respuesta a las amenazas cibernéticas.

b) Objetivo Estratégico 2 (OE2): Defender las infraestructuras críticas cibernéticas nacionales de la actividad cibernética maliciosa.

c) Objetivo Estratégico 3 (OE3): Desarrollar capacidades cibernéticas para mejorar las ventajas militares en Colombia.

d) Objetivo Estratégico 4 (OE4): Conformar ligas de ciberdefensa con los sectores públicos y privados.

e) Objetivo Estratégico 5 (OE5): Generar alianzas estratégicas a nivel nacional e internacional.

Supuestos

La mayor parte de los habitantes de la tierra, vive y usa el ciberespacio todos los días del año durante las 24 horas, ya sea en forma activa o pasiva. En general, los países desarrollados y con alta dependencia cibernética, tienen conocimiento de esta situación y, por lo tanto, son conscientes de los riesgos que corren en materia de seguridad y defensa nacional.

La capacidad de ciberdefensa en Colombia, debe estructurarse y desarrollarse para prevenir y retrasar o neutralizar la rápida progresión de los ataques cibernéticos, asegurando la detección temprana, implementando herramientas avanzadas de vigilancia y alerta, buscando así contener y limitar el daño potencial. Los ataques cibernéticos pueden resultar en una importante vida económica, humana o serias amenazas a la seguridad y defensa nacional. En este contexto, al

evaluar las consecuencias de la actividad cibernética hostil, debe existir la flexibilidad operativa necesaria para ajustar la respuesta a cada tipo de ataque y situación de forma proporcional.

Las actividades de ciberdefensa, que constituyen un área vinculada a las operaciones militares, también deben complementar la implementación de los requisitos para proteger la confidencialidad, integridad y disponibilidad de las tecnologías de información (TI) y las tecnologías de operación (TO).

Una capacidad operativa de ciberdefensa implica el conocimiento y los recursos necesarios para predecir, influir o bloquear las acciones que los posibles adversarios podrían tomar en el ciberespacio a través de operaciones militares.

Estrategia

Fortalecimiento del pie de Fuerza

a) Mantener la conformación de un Comando Conjunto, permitirá desarrollar capacidades y brindar directrices de forma articulada, de acuerdo con el rol funcional de cada Fuerza, al tiempo que se garantizará la interoperabilidad y el desarrollo de operaciones conjuntas, coordinadas, interinstitucionales y multinacionales.

b) Conformar comandos de ciberdefensa en cada Fuerza, para desarrollar capacidades cibernéticas y su interoperabilidad en el desarrollo de operaciones de tierra, mar, aire y espacio.

c) Considerar, para un futuro cercano, la creación de una nueva Fuerza, encargada de asumir todos los asuntos relacionados con el ciberespacio.

Defensa de las infraestructuras críticas cibernéticas

a) Apoyar el desarrollo y adopción de una Política y Ley para Protección y Defensa de las infraestructuras críticas con una visión de Colombia desde el componente de seguridad física y tecnológica, incluyendo planes de protección.

b) Definir y formalizar los sectores estratégicos para el país, desde una perspectiva integral de seguridad, es decir, evaluados desde el componente físico y tecnológico.

c) Identificar, clasificar, catalogar y priorizar los nodos estratégicos dependientes de tecnologías de información y comunicaciones que pertenecen a cada sector estratégico.

d) Desarrollar planes de protección y defensa para los nodos estratégicos dependientes de tecnologías de información y comunicaciones que pertenecen a cada sector estratégico

e) Gestionar la suscripción de acuerdos, convenios y protocolos, apoyos y cooperación mutua de ciberdefensa entre las Fuerzas Militares y los propietarios y operadores de infraestructura crítica, que permitan apoyar al fortalecimiento de la ciberdefensa y resiliencia cibernética nacional.

f) Realizar ejercicios y modelos de simulación de incidentes de ciberseguridad con la participación de los propietarios y/o operadores de infraestructura critica, que permitan analizar las dependencias e interdependencias entre las diferentes infraestructuras y los riesgos en su conjunto para mejorar continuamente la protección de la infraestructura crítica nacional de Colombia.

Desarrollo de capacidades cibernéticas

Las capacidades cibernéticas podrán ser empleadas en tiempos de paz o de guerra.

a) Capacidad de disuasión: cuando uno se prepara para defenderse, desestimula ataques de otros países que puedan, en alguna situación, creer que necesitan algo. La disuasión hará que antes de intentarlo alguien lo piense dos veces.

b) Capacidad de defensa: incluye las medidas para la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que manejan.

c) Capacidad de inteligencia: incluye actividades y operaciones para anular, neutralizar o contener cualquier tipo de amenaza cibernética.

d) Capacidad de ofensiva: incluye también las medidas y acciones a tomar ante amenazas o ataques.

e) Capacidad de diplomacia: conducir los asuntos exteriores de Colombia como un sujeto de derecho internacional, utilizando medios pacíficos y principalmente la negociación.

Conformar ligas de ciberdefensa con los sectores públicos y privados

Conformar ligas de ciberseguridad y ciberdefensa en apoyo a las Fuerzas Militares, definiendo estrategias para la adhesión de personal experto en los grupos de investigación y desarrollo de la industria cibernética.

Generar alianzas estratégicas a nivel nacional e internacional

a) Promover y articular la cooperación como una estrategia en o a través del ciberespacio, entre las entidades responsables de ciberseguridad y ciberdefensa en Colombia.

b) Establecer una red de alertas nacional que permita advertir sobre las nuevas amenazas a fin de contener cualquier incidente o minimizar los riesgos a través de la integración y complemento de las capacidades de los diferentes responsables de ciberdefensa a nivel Nación.

c) Instituir marcos de cooperación con la academia, el sector público y privado, la sociedad civil, los ciudadanos y los propietarios y/o operadores de infraestructura critica que permitan fortalecer la ciberdefensa nacional.

d) Firmar acuerdos, protocolos y convenios que permitan el intercambio de información bilateral o multilateral con Fuerzas Militares de otros países.

e) Coordinar con otros comandos, entidades del gobierno y empresas públicas y privadas, la integración de capacidades de defensa en el ciberespacio, en casos donde se requiera, bajo estrictas medidas de seguridad y de reserva de las capacidades.

f) Generar capacidades de respuesta a incidentes para el sector Defensa, para compartir información, herramientas, metodologías, procesos y mejores prácticas, que permitan en forma cooperativa mantener y prevenir en forma oportuna incidentes de seguridad informática.

g) Promover alianzas estratégicas del Sector Defensa con el Ministerio de Tecnologías de Información y Comunicaciones, con el Ministerio de Justicia y las instituciones de inteligencia del Estado, que lleven a mesas de trabajo nacionales permanentes.

h) Participar y desarrollar ejercicios de simulación de ciberguerra y eventos relacionados con ciberseguridad y ciberdefensa internacionales.

i) Promover la adhesión a organismo y/o redes 7x24 como apoyo a la gestión de incidentes, investigaciones y judicialización en el ámbito cibernético.

j) Fortalecer la influencia regional y la diplomacia pública internacional que permitan crear alianzas estratégicas y desarrollar estrategias para resolución de conflictos en el ciberespacio de manera pacífica.

Conclusión

La naturaleza de la estrategia propuesta es de tipo organizativo. Ayudará a establecer un sistema eficiente de ciberdefensa para Colombia. La información y la experiencia obtenidas se convertirán en la piedra angular de los planes de desarrollo cibernético futuro y orientación estratégica.

En definitiva, se propone avanzar en una dirección que permita a las Fuerzas Militares colombianas, a partir de sus competencias y responsabilidades, realizar la ciberdefensa, coordinando su accionar con instituciones del sector público y privado, a la vez que desarrollar y fortalecer las capacidades de ciberdefensa, a fin de estar en condiciones de desarrollar operaciones militares cibernéticas contra un agresor que pudiera atacar a Colombia.

En el siguiente capítulo, se presenta la metodología empleada en la investigación a fin de realizar una propuesta concreta de estrategia nacional de ciberdefensa para Colombia.

4. Metodología

4.1 Introducción

Este capítulo presenta la metodología de la investigación utilizada para la realización de este trabajo. En él se detallan los pasos desarrollados que permitieron la identificación de los tres elementos: ciberdefensa nacional, unidades militares de ciberdefensa y amenazas cibernéticas, los cuales se tomaron en cuenta para generar la propuesta de la estrategia militar de ciberdefensa para Colombia con base en el análisis de estrategias de ciberdefensa internacionales, las cuales fueron contrastadas con el modelo DOMPILEM, adoptado por las Fuerzas Militares colombianas para el desarrollo de capacidades. Este capítulo comienza describiendo cómo fue abordada la investigación, sus fundamentos y los pasos que se llevaron a cabo.

4.2 Descripción metodológica

La investigación obedece a un paradigma cualitativo[4] y el método utilizado es de tipo descriptivo, mediante el cual el investigador determinó entre las estrategias internacionales de ciberdefensa los elementos más relevantes, impacto o influencia en la ciberdefensa nacional. De igual manera, determinó los puntos u objetivos en los que son coincidentes entre ellas, con el propósito de determinar su aplicabilidad a la realidad nacional colombiana.

---

[4] El enfoque cualitativo es, entonces, un paradigma que descansa en la premisa de que "los significados son construidos socialmente por los individuos en su interacción con su mundo" (Merriam, 2002, p.3).

De otro lado, el alcance descriptivo permitió al investigador determinar y analizar cada una de las consecuencias directas e impacto colateral que se desprendía de las amenazas o ataques cibernéticos latentes y emergentes, así como las líneas de acción requeridas para el desarrollo de capacidades cibernéticas y los objetivos estratégicos a los que apuntan las estrategias revisadas en materia de ciberdefensa.

4.3 Técnicas de recolección

Para desarrollar la propuesta de la estrategia militar de ciberdefensa, se realizó la recolección de información de los tres componentes fundamentales, de acuerdo a los siguientes criterios.

4.3.1 Información de amenazas cibernéticas

La recolección de información de amenazas, se realizó tomando como referencia estudios del MIT y del Foro Económico Mundial, sin dejar de lado los pronósticos realizados por grandes fabricantes como el informe de amenazas 2019 de SophosLab (SophosLab, 2019), el informe de ciberamenazas 2019 de SonicWall, que desenmascara las amenazas dirigidas a empresas, gobiernos y pymes (SonicWall, 2019). El informe sobre las amenazas para la seguridad en Internet 2019 (ISTR), analiza en profundidad las últimas tendencias de los ataques contra la ciberseguridad, como el *ramsomware*, el *formjacking* y la seguridad en la nube, entre otros, a fin de analizar en prospectiva las amenazas latentes y emergentes en el componente cibernético (Symantec, 2019).

4.3.2 Información para la planeación por capacidades DOMPILEN

Para este propósito se hizo necesario abordar el modelo con base en las capacidades actuales de las unidades militares de ciberdefensa en Colombia, y a partir de ese análisis realizar la propuesta que permita desarrollar o fortalecer las capacidades en el componente cibernético.

4.3.3 Información de estrategias de ciberdefensa internacionales

Las estrategias estudiadas, Estados Unidos, Portugal, República Checa y Países Bajos, fueron seleccionadas de un total de estrategias de seguridad y defensa nacional de 81 países que se encuentran públicas en el portal de internet del CCDCOE, por sus siglas en inglés *Cooperative Cyber Defence Center of Excellence*, definido como el Centro de Defensa Cibernética acreditado por la OTAN, el cual se encarga de apoyar a sus países miembros en ciberdefensa y fomentar la cooperación de naciones amigas en materia cibernética. Los criterios de selección de los países estudiados fueron dos: influencia económica, política y militar a nivel global y el índice de desarrollo humano.

4.4 Estudio de caso múltiple

La selección de la muestra en un estudio de caso múltiple obliga al investigador a comprender el caso. Stake (1996, 2006) afirma que la investigación de los estudios de caso no es una investigación basada en muestras representativas porque no se estudia un caso para entender otros casos, sino que la obligación del investigador es entender ese caso por sí mismo. Asimismo, señala que en los estudios de caso múltiples se efectúa un esfuerzo particular de examinar algo que tiene muchos casos, partes o miembros de manera detallada para recopilar lo que cada caso tenga que comunicar con la intención de estudiar el fenómeno que exhiben esos casos (Stake, 2006). De

manera que la selección de la muestra para el estudio de caso es no probabilística sino intencionada, con un propósito. La muestra con un propósito se basa en el principio de que el investigador quiere descubrir, entender, ganar una visión profunda, por lo que selecciona la muestra de la que pueda aprender mejor (Merriam, 2002); por tanto, el investigador utiliza su juicio para determinar los segmentos de la población que participarán en su estudio (Charles, 1995).

Dicho lo anterior, el estudio se hizo con base en estrategias militares de ciberdefensa de Estados Unidos, Portugal, República Checa y Países Bajos, con el fin de analizar y aplicar el método de triangulación de puntos, elementos o componentes convergentes y divergentes presentes en las diferentes estrategias militares de ciberdefensa internacionales mencionadas usando el objetivo global, los objetivos específicos y los supuestos o principios para establecer los puntos en los que eran coincidentes, a fin de estudiarlos en la realidad colombiana y determinar su viabilidad de ejecución.

En definitiva, el presente estudio intenta contribuir al cambio de paradigma en el planeamiento y ejecución de operaciones militares en el nuevo dominio de guerra denominado ciberespacio.

4.5 Fases del proyecto

4.5.1 Instrumentalización

Conocer la problemática que gira en torno a las amenazas y ataques de tipo cibernético y su incidencia a la seguridad y defensa nacional a nivel nacional e internacional, permitió al investigador generar una conciencia situacional que lo llevó a indagar sobre las decisiones que

están tomando otras naciones en materia de ciberdefensa nacional con el propósito de efectuar la selección de los elementos más relevantes, que sirvieron de base para realizar el presente estudio de investigación y llegar a formular la propuesta de estrategia militar de ciberdefensa para Colombia.

Partiendo del hecho de que, en la actualidad, la ciberdefensa nacional corresponde a un eje estratégico para el cumplimiento de la misión de las Fuerzas Militares de Colombia, fue analizado desde diferentes perspectivas como la primera variable o elemento, toda vez que representa un pilar estratégico para la seguridad y defensa de la Nación en el ciberespacio.

Por su parte, las unidades militares de ciberdefensa nacionales, representan el segundo elemento de estudio, por ser las instituciones responsables de la ciberdefensa nacional. Dentro de ese marco, fue necesario estudiar sus capacidades actuales, componentes y organización a fin de realizar un análisis objetivo para el desarrollo de capacidades con base en el modelo DOMPILEM.

Complementando el estudio, las amenazas cibernéticas fueron estudiadas como el tercer elemento, considerando que son la razón que motiva la preocupación de las naciones para el desarrollo de capacidades cibernéticas.

Finalmente, se realizó la propuesta de la estrategia con base en el análisis integral de los elementos mencionados y tomando como referencia el esquema estructural de las estrategias militares de ciberdefensa internacionales estudiadas, en las cuales se evidencia el planteamiento de un objetivo global y los objetivos estratégicos que permiten alcanzarlo desde diferentes perspectivas. Sobre las bases de las ideas expuestas, se propondrá un esquema similar que presente un objetivo global

a alcanzar. Partiendo de unos supuestos nacionales en materia cibernética se propondrán unos objetivos estratégicos que permitirán cumplir el objetivo global consistente en fortalecer la ciberdefensa nacional.

4.5.2 Población y muestra

Dada la complejidad que se presenta para analizar y comparar todas las estrategias que se encuentran públicas en el Centro de Excelencia de la OTAN, el investigador recurrió a la selección de una muestra no probabilística (Hernández, Fernández y Baptista, 2010), (Hernandez, Fernandez, 2010)la cual representa un subconjunto de los elementos que pertenecen a la población que cumple con las características más representativas en términos de ciberdefensa y organización. Para ello, se tuvieron en cuenta los siguientes parámetros de selección: influencia económica, política y militar a nivel global y el índice de desarrollo humano.

- Estados Unidos: una de las principales potencias a nivel mundial, que ejerce una influencia económica, política y militar a nivel global. El poseer la economía nacional más grande del mundo, entre otros aspectos, le han facilitado realizar grandes desarrollos en todos los campos, como la ciberseguridad y ciberdefensa.

- Portugal: país miembro de la Unión Europea. De acuerdo con el Vison of Humanity es un país desarrollado, con un índice de desarrollo humano (IDH) considerado como "muy elevado" y con una alta tasa de alfabetización. El país está clasificado como el decimonoveno con mejor calidad de vida. Tiene uno de los mejores servicios sanitarios del planeta y es considerado una nación globalizada y pacífica.

- República Checa: país miembro de la Unión Europea. Posee una economía altamente desarrollada, se convirtió en el primer exmiembro del Comecon en alcanzar el estatus pleno de país desarrollado según el Banco Mundial. Además, según el Vision of Humanity (referencia), tiene el mayor índice de desarrollo humano de toda Europa Central y del Este y por ello está considerado como un Estado con "desarrollo humano muy alto".
- Países Bajos: los Países Bajos siempre se destacaron por estar a la delantera en materia de tecnología. La Comisión Europea ha publicado los resultados de la edición de 2016 del Índice de la Economía y la Sociedad Digitales en los que Dinamarca, los Países Bajos, Suecia y Finlandia siguen ocupando los primeros puestos de estos resultados.

4.5.3 Análisis de los datos

Los datos recolectados en el desarrollo de la investigación sirvieron de base para la identificación de la relación entre las variables identificadas así: la ciberdefensa nacional, las unidades militares de ciberdefensa nacionales y las amenazas cibernéticas, con el propósito de pronosticar los resultados.

Los datos obtenidos del análisis de las estrategias de ciberdefensa de Estados Unidos, Portugal, República Checa y Países Bajos, se cruzaron para determinar cuáles de los objetivos propuestos en las estrategias militares de ciberdefensa internacionales eran coincidentes. De esta manera, el investigador estuvo en la facultad de interconectar datos, correlativos a la generación de una estrategia que pudiese contrarrestar el impacto multidimensional derivado de los tres elementos

principales de la investigación, así: ciberdefensa nacional, unidades militares responsables de la ciberdefensa y las amenazas cibernéticas de cara a las tecnologías disruptivas.

En virtud de la información obtenida sobre las unidades militares responsables de la ciberdefensa (variable 2), se aplicará el modelo DOMPILEN sobre las bases de las ideas expuestas para dar cumplimiento a los objetivos identificados para la estrategia nacional colombiana y con ella contribuir a la neutralización, contención y respuesta frente a las amenazas cibernéticas que impacten a la seguridad y defensa nacional.

4.5.4 Interpretación de los datos

Los elementos analizados presentan un enfoque relacionado directamente con el componente económico, social y de seguridad nacional.

En primer lugar, la ciberdefensa nacional, impacta directamente sobre la seguridad nacional. Dicho de otra manera, según el Informe de Riesgos Mundiales 2019 (14ª edición), el Foro Económico Mundial señala:

> La tecnología sigue desempeñando una función profunda en la conformación del panorama de riesgos mundiales para individuos, gobiernos y compañías. En la GRPS, el "fraude y robo de datos masivo" se ubicó en el número cuatro de riesgo mundial por probabilidad, en un lapso de 10 años, con los "ataques cibernéticos" situados en el número cinco. Esto mantiene un patrón que se registró el año pasado, con la consolidación de la posición de los riesgos cibernéticos junto a los riesgos ambientales en el cuadrante de alto impacto y alta probabilidad del panorama de riesgos mundiales (Companies y Group, 2019).

Esto indica que cada vez más, la tecnología hace parte de la vida cotidiana, hasta el punto de impactar en cada uno de los habitantes colombianos; por lo tanto, la dependencia a esta lleva directamente a afectar en un momento dado la estabilidad nacional. Por tanto, su análisis permitirá forjar una visión estratégica para la nación, de tal manera que permita proyectar el desarrollo de capacidades cibernéticas a corto, mediano y largo plazo.

En segundo lugar, se encuentran las unidades militares por Fuerza y conjuntas, responsables de ciberdefensa nacional. Es por esto que contar con unidades fortalecidas, equipadas y entrenadas en el componente cibernético, permitirá a Colombia contener, neutralizar o contrarrestar amenazas cibernéticas que afecten la seguridad y defensa nacional para de esta manera incrementar la confianza cibernética de los ciudadanos nacionales y extranjeros en las Fuerzas Militares y con ellas, garantizar una prosperidad económica digital y social.

Con base en los anteriores argumentos, se concluye que las amenazas y ataques de carácter cibernético, impactan directamente en la economía digital del país. Es por esto que se hace necesario que las Unidades Militares cuenten con las capacidades de ciberdefensa que le permitan desarrollar operaciones militares en el ciberespacio, para afrontar los nuevos retos y hacer de Colombia una nación cada vez más resiliente en materia cibernética.

5. Resultados

5.1 Introducción

En el presente capítulo se presentan los resultados obtenidos al contrastar las estrategias militares de ciberdefensa a nivel internacional, así como el consolidado de amenazas latentes y emergentes definidas en prospectiva durante la investigación. Por último, se presenta la correlación de resultados del análisis de estrategias versus el modelo DOMPILEN para el desarrollo de capacidades de ciberdefensa para las unidades responsables de dicha función en las Fuerzas Militares de Colombia.

5.2 Resultado de análisis estrategias militares de ciberdefensa internacionales

A continuación, se presenta una tabla que sintetiza el resultado obtenido al comparar las estrategias de ciberdefensa de los cuatro países analizados, realizando un emparejamiento con los puntos donde son coincidentes las estrategias:

Tabla 4

Resultados análisis estrategias militares de ciberdefensa internacionales

Objetivo estratégico	Republica Checa	Países Bajos	Estados Unidos	Portugal	Resultados (match)
Capacidades militares cibernéticas (Op)	X	X	X	X	4 de 4
Cooperación	X	X	X	X	4 de 4
Infraestructura crítica	X	X	X	X	4 de 4
Educación	X	X	X		3 de 4
Disputa del ciberespacio	X		X	X	3 de 4
Protección y resistencia	X			X	2 de 4
Ciberseguridad militar	X		X		2 de 4
Innovación		X		X	1 de 4

Marco legal	X		1 de 4
Desarrollo infraestructura	X		1 de 4
Enfoque integral		X	1 de 4

Fuente: Elaboración propia.

Como se evidencia en esta síntesis, las cuatro estrategias militares de ciberdefensa internacionales presentan sus objetivos estratégicos dirigidos a un mismo enfoque, "Fortalecer la actuación de sus Fuerzas Armadas". En este sentido, los tres objetivos en los que coinciden las cuatro estrategias son el fortalecimiento de capacidades cibernéticas, la cooperación nacional e internacional y la protección de las infraestructuras críticas de la nación. Por su parte, la educación y disputar el poder del ciberespacio fueron consideradas por tres países. La protección y resistencia fueron avaladas por dos países.

Avanzando en este razonamiento, los puntos en que las estrategias son divergentes fueron cuatro: innovación, marco legal, desarrollo de infraestructura y marco integral, las cuales también fueron consideradas por el investigador, toda vez que representan puntos relevantes en la actualidad tecnológica nacional en materia de ciberseguridad y ciberdefensa.

Con base en este análisis, el investigador contrastó la realidad nacional y las capacidades actuales de las unidades militares responsables de la ciberdefensa nacional, se hizo una propuesta para Colombia.

5.3 Resultado del análisis de amenazas cibernéticas

A este respecto, es preciso afirmar que Colombia ha experimentado importantes avances en materia de conectividad a internet y uso del ciberespacio, y con ello la dependencia que la sociedad tiene de él, lo que puede contrastarse con el avance en materias de ciberseguridad y ciberdefensa. Dentro de este marco, el resultado obtenido de las amenazas es una vista sistémica de los riesgos claves latentes y emergentes a tener en cuenta (dos cuadrantes de la Ventana de AREM), enriquecida con la vista de los investigadores y los analistas de riesgos y amenazas en el contexto de la ciberdefensa nacional, donde se obtuvieron los resultados definidos en la siguiente tabla:

Tabla 5

Amenazas latentes y emergentes

Amenaza/riesgo latente	Amenaza/riesgo emergente
Ciberguerra	Guerra autónoma
LAWS Lethal Autonomous Weapons (robots militares, embarcaciones de superficie y submarinas, drones autónomos, sistemas satelitales autónomos)	Ciberarmas de destrucción masiva
Sistemas autónomos	

Fuente: Elaboración propia.

5.3.1 Amenazas/Riesgos latentes

Tres son las principales amenazas latentes en el ciberespacio, es decir, que se encuentran ocultas o aparentemente inactivas, que fueron identificadas y según el investigador, podrían poner en tensión la seguridad nacional de Colombia, afectando su prosperidad económica y social.

La primera es la ciberguerra que, sin duda, constituye el extremo más grave del espectro de los problemas de seguridad planteados en el ciberespacio, donde los actores son los Estados. La

ciberguerra puede permitir a los actores lograr sus objetivos políticos y estratégicos en menos tiempo, con mínimos riesgos y a bajo costo.

La guerra cibernética o ciberconflicto se configura en la actualidad como una posibilidad de intervención político-estratégica más eficiente, en la que habrá más posibilidades de que los daños provocados sean menores en comparación con las armas convencionales. Además de eso, será también más difícil de identificar/controlar el origen de los ataques. Por tantas ventajas, las actividades que se suceden en el ciberespacio atraen el interés de los Estados, con el objetivo de utilizarlas como instrumentos de política exterior. El conflicto sigue siendo una extensión de la voluntad política y ahora en el ciberespacio tiene un nuevo espacio en el que sus formas pueden participar. Colombia, no se encuentra ajena a esta amenaza.

La segunda, corresponde a las LAWS: "Las armas letales autónomas (LAWS, por sus siglas en inglés, *Lethal Autonomous Weapons*). La ONU define como arma autónoma una herramienta capaz de "localizar, seleccionar y eliminar objetivos humanos sin intervención humana" (Scharre, 2019, p. 3). Las armas letales autónomas son el resultado de la aplicar la inteligencia artificial a la búsqueda de soluciones en el ámbito del enfrentamiento militar, del combate.

Las verdaderas armas autónomas letales o LAW, se enfrentarán al enemigo sin órdenes humanas y decidirán qué hacer para evitar los obstáculos que pretendan impedir la ejecución de su misión. Por ejemplo, un pequeño tanque podría patrullar las calles de una ciudad y actuar sin un piloto que decidiera por él. Estas propuestas todavía no existen operacionalmente, pero ya han desatado una gran polémica y un debate internacional.

Hay LAW marinas o acuáticas (embarcaciones de superficie y submarinas), aéreas (drones autónomos que seleccionan por sí mismos los objetivos) y terrestres (algunos incluso con forma humana). El riesgo radica cuando sea la máquina mediante procedimientos autónomos la que elija los objetivos a abatir.

En tercer lugar, están los sistemas autónomos, considerados un grave problema de la inteligencia artificial. Un reconocido científico y académico de la Universidad de California, llamado Stuart Russell (2010), explica que los sistemas autónomos a su juicio es el problema actual de la inteligencia artificial, ahora presente en un sinnúmero de dispositivos que podrían ser manipulados para infiltrar sistemas informáticos de otros Estados, empresas o industrias nacionales críticos para la sociedad sin intervención humana (Rusell, 2000).

La posible existencia de robots, capaces de disparar las 24 horas del día de manera indiscriminada, es uno de los escenarios que han dejado de pertenecer exclusivamente a las películas y series de ciencia ficción y se ha convertido en una preocupación recurrente de organismos internacionales como la ONU o la Convención de Ciertas Armas Convencionales. En los próximos años cada arma tendrá la capacidad de decidir autónomamente a quién matar: uno de los grandes dilemas éticos de la inteligencia artificial aplicada a la guerra (Scharre, 2019).

5.3.2 Riesgos emergentes

Los resultados obtenidos dan cuenta de dos riesgos emergentes derivados de las tecnologías disruptivas, que retan las capacidades del sector militar para proteger la seguridad y defensa de la Nación. La primera amenaza es la guerra autónoma, definida en pocas palabras como el uso de la inteligencia artificial en la guerra. Dicho de otra forma, una guerra autónoma acaba por

transformarse en una guerra de recursos donde el humano no interfiere directamente. Simplemente es la interacción de sistemas autónomos entre sí; en este orden de ideas, se hace necesario establecer pautas para la innovación, que impidan emprender un viaje tecnológico sin retorno.

Por otra parte, están las ciberarmas de destrucción masiva. Si bien actualmente solo nueve Estados (supuestamente) poseen armas nucleares, las armas cibernéticas pueden ser obtenidas, desarrolladas o utilizadas por cualquier Estado o actor no estatal, son relativamente baratas, seguras y fáciles de operar. Esto tiene dos consecuencias. Primero, las armas cibernéticas pueden convertirse en un nuevo tipo de arma de destrucción en masa, o tal vez sería mejor llamarlas armas de destrucción masiva. Es de esperar que, dentro de unos años, gracias a la rápida y continua digitalización del mundo, los ciberataques puedan dañar a sociedades enteras. Es posible que las armas cibernéticas no puedan causar el mismo nivel de destrucción mortal que las armas nucleares, pero pueden ser muy eficaces. Al respecto de las nuevas capacidades de los agresores, Cano (2018, p.2) establece: "Si bien es claro que al final, el agresor digital doblegará las ´barreras` y superará las estrategias de protección definidas, para lo cual la empresa y las naciones deberán contar con procedimientos y prácticas de atención de incidentes", en donde los distintos actores de la dinámica de los ciberconflictos desarrollan una "tensión creativa" para sumergirse en el escenario de lo incierto y desconocido. Por ejemplo, se puede pensar en un sabotaje combinado y serio de la energía y los suministros de agua, así como en la comunicación (Van Der Meer, 2016).

Finalmente, y con base en los resultados obtenidos, se propone contar con una estrategia militar basada en objetivos que consideran como fundamento el desarrollo de capacidades y la aplicación

de medidas de contención y mitigación, los cuales sirvieron de base para la formulación de los objetivos estratégicos de la estrategia propuesta.

5.4 Objetivos propuestos para la estrategia nacional de Colombia

A continuación, se presentan los objetivos propuestos en la estrategia militar de ciberdefensa para Colombia, a fin de desarrollar capacidades que permitan dar respuesta a los ataques o amenazas de naturaleza cibernética. Esta propuesta se hizo con base en el análisis de los objetivos coincidentes, pero sin desconocer los divergentes que pudiesen aplicar de las estrategias militares de ciberdefensa internacionales contrastadas con la realidad nacional.

Objetivo Estratégico 1 (OE1):

Fortalecer el Pie de Fuerza requerido para dar respuesta a las amenazas cibernéticas.

Objetivo Estratégico 2 (OE2):

Defender las Infraestructuras Críticas Cibernéticas Nacionales de la actividad cibernética maliciosa.

Figura 6. Objetivos estratégicos ciberdefensa

Fuente: Elaboración propia.

5.5 Modelo DOMPILEN vs. los objetivos estratégicos propuestos

Para realizar este análisis, fue necesario efectuar un cruce de relaciones uno a uno, es decir, tomar cada uno de los objetivos estratégicos y estudiarlos frente a cada uno de los elementos del DOMPILEM (figura 6), para establecer las necesidades desde la óptica de la doctrina, organización, material, personas, instalaciones, liderazgo - educación, entrenamiento y mantenimiento.

Para este fin se realizó el análisis uno a uno, es decir, cada objetivo estratégico con cada uno de los componentes del DOMPILEM, de tal manera que se puedan establecer debilidades y

oportunidades para fortalecer las capacidades cibernéticas en Colombia, utilizando el siguiente modelo:

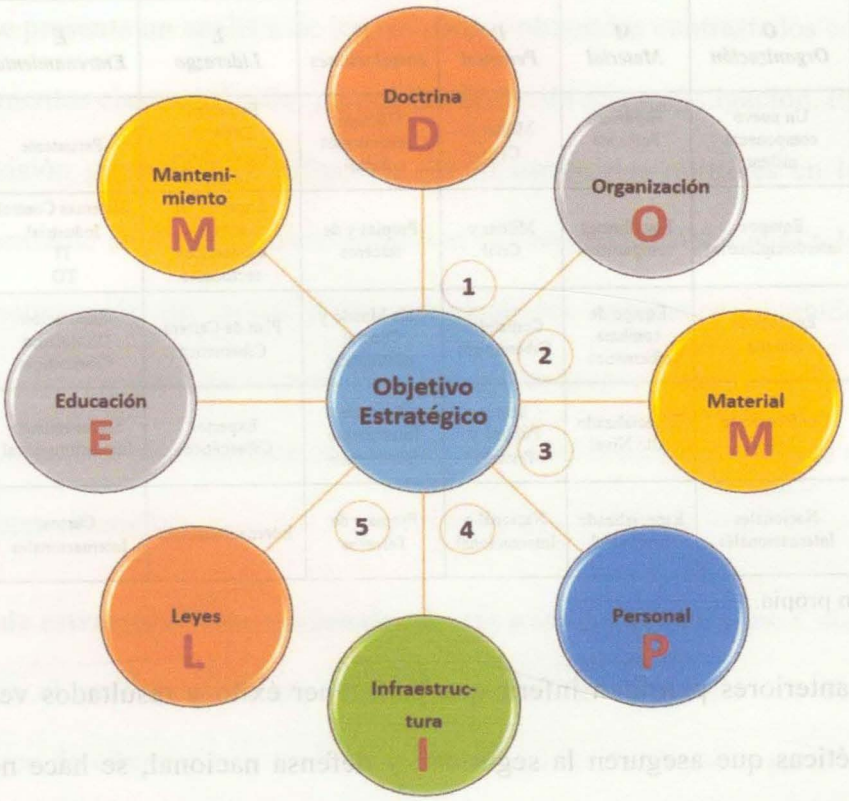

Figura 7. Modelo de análisis objetivos DOMPILEM

Fuente: Elaboración propia.

En síntesis, una vez realizado el cruce del modelo frente a los objetivos estratégicos propuestos, se obtuvo la siguiente tabla, la cual muestra un consolidado de los componentes clave de DOMPILEN, en contraste con cada uno de los objetivos estratégicos que plantea la estrategia nacional de ciberdefensa, los cuales deben desarrollarse en las unidades militares responsables de la ciberdefensa en Colombia, a fin de fortalecer las capacidades en materia cibernética que garanticen el desarrollo de operaciones militares en el ciberespacio.

Tabla 6

Resumen análisis objetivos vs. DOMPILEM

OBJ.	***D*** ***Doctrina***	***O*** ***Organización***	***M*** ***Material***	***P*** ***Personal***	***I*** ***Instalaciones***	***L*** ***Liderazgo***	***E*** ***Entrenamiento***	***M*** ***Mantenimiento***
OE1	Manuales conjuntos y por Fuerza	Un nuevo componente militar	Hardware Software	Militar y Civil	Oficinas Laboratorios Salas	Estrategas Expertos Especialistas Técnicos	Persistente	Plataformas Cibernéticas
OE2	Planes de Protección	Equipos interdisciplinarios	Plataformas compartidas	Militar y Civil	Propias y de terceros	Expertos en activos estratégicos sectoriales	Sistemas Control Industrial TI TO	Sistemas de Defensa Cibernética
OE3	Manual Operaciones Cibernéticas	Equipos de Batalla	Equipo de combate cibernético	Comandos Cibernéticos	Sala Mando y Control cibernético	Plan de Carrera Cibernética	Simulación Olimpiadas Cibernéticas	Plataformas de Operaciones Cibernéticas
OE4	Manual de Apoyo Cibernético	Conformación Ligas	Especializado Alto Nivel	Sector Público y Privado	Salas de Intercambio Cibernético	Expertos Cibernéticos	Entrenamiento Interinstitucional	Sistemas de Apoyo
OE5	Acuerdos, convenios	Nacionales Internacionales	Especializado Alto Nivel	Nacional e Internacional	Propia y de Terceros	Internacionalistas	Cursos Internacionales	Sistemas de Intercambio

Fuente: Elaboración propia.

Las evidencias anteriores permiten inferir que para tener éxito y resultados verificables en las misiones cibernéticas que aseguren la seguridad y defensa nacional, se hace necesario que las Fuerzas Militares realicen operaciones conjuntas entre las diferentes Fuerzas, coordinadas con la Policía Nacional, con organizaciones tanto del sector público como privado y con las naciones amigas, trabajando de la mano con los organismos binacionales y multilaterales, apoyados, siempre que se requiera, por las ligas de ciberdefensa.

6. Análisis de los resultados

6.1 Introducción

En este capítulo se presenta un análisis de los resultados obtenidos contrastados con cada una de las variables o elementos claves definidos para el desarrollo de esta investigación. En primer lugar, se presenta una visión general de la influencia de las estrategias militares en la ciberdefensa nacional, posteriormente se muestra cómo impactan los resultados obtenidos a la ciberdefensa nacional, y a continuación se indica cómo apoyarán los resultados obtenidos de cara al fortalecimiento de las capacidades cibernéticas de las unidades militares responsables de la ciberdefensa en Colombia, para finalizar con la influencia de los resultados frente a las amenazas o ataques de carácter cibernético.

6.2 Revisión de estrategias internacionales frente a la ciberdefensa en Colombia

Una vez realizado el análisis de la investigación, se puede evidenciar que el desarrollo de estrategias militares de ciberdefensa a nivel internacional se fortaleció a partir del año 2016, cuando el ciberespacio fue reconocido como un instrumento de defensa colectiva, un dominio de operaciones militares "... en el que la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar" (NATO, 2016, pp. 2-3).

Adicionalmente, en este mismo Comunicado de la Cumbre de Varsovia, emitido por los Jefes de Estado y de Gobierno que participan en la reunión del Consejo del Atlántico Norte en Varsovia del 8 al 9 de julio de 2016, en su numeral 71, señala:

> Cada aliado cumplirá con su responsabilidad de mejorar su capacidad de recuperación y su capacidad de responder de manera rápida y efectiva a los

> ciberataques, incluso en contextos híbridos. Junto con la adaptación continua de las capacidades de defensa cibernética de la OTAN, esto reforzará la defensa cibernética de la Alianza. Estamos ampliando las capacidades y el alcance de la OTAN Cyber Range, donde los Aliados pueden desarrollar habilidades, mejorar su experiencia e intercambiar mejores prácticas. Seguimos comprometidos con una estrecha cooperación bilateral y multilateral en defensa cibernética, incluido el intercambio de información y la conciencia situacional, la educación, la capacitación y los ejercicios. Las asociaciones sólidas desempeñan un papel clave para abordar eficazmente los desafíos cibernéticos. Continuaremos profundizando la cooperación con la UE, según lo acordado, incluso a través de la implementación continua del Acuerdo Técnico que contribuye a una mejor prevención y respuesta a los ataques cibernéticos. Mejoraremos aún más nuestras asociaciones con otras organizaciones internacionales y naciones asociadas, así como con la industria y la academia a través de la OTAN Industry Cyber Partnership (OTAN, 2016, pp. 2-3).

Estas afirmaciones, muy seguramente han influenciado en la toma de decisiones en materia cibernética para varias naciones. En lo que refiere a Colombia, es preciso afirmar que la OTAN ha servido de marco de referencia para el avance de la ciberdefensa nacional. Desde el 31 de mayo de 2018, Colombia formalizó su ingreso como socio global de la Organización del Tratado del Atlántico Norte (OTAN), convirtiéndose en el único país de América Latina con un estatus de mayor cooperación que comparte con otros países como Afganistán, Australia o Japón, pero que no implica su membresía a la Alianza Atlántica. Los socios globales de la OTAN "desarrollan

cooperación con la OTAN en áreas de interés mutuo, incluidos los desafíos de seguridad emergentes, y algunos contribuyen activamente a las operaciones de la OTAN, ya sea militarmente o de alguna otra manera" (OTAN, 2016, pp. 2-3). En particular para Colombia, se establecieron acuerdos en materia de cooperación en asuntos relacionados con ciberdefensa, la seguridad electrónica, marítima y la lucha contra el terrorismo y el crimen organizado.

6.3 Impacto a la luz de la ciberdefensa nacional

Contar con una estrategia militar de ciberdefensa, permitirá a las Fuerzas Militares de Colombia articular los esfuerzos hacia el cumplimiento de unos objetivos armonizados de manera conjunta, que ayuden a fortalecer la ciberdefensa, afrontando el ciberespacio como un dominio de guerra donde se desarrollan operaciones militares. Como lo afirma el autor Brad Bigelow en su artículo: "What are Military Cyberspace Operations Other Than War?", "Es útil considerar hacer un llamamiento para un papel militar más activo en el ciberespacio fuera de la guerra en el contexto del trabajo doctrinal sobre el papel de las operaciones militares distintas de la guerra en general" (Bigelow, 2019, p. 4). En este contexto, es el momento de hacer frente de manera organizada, articulada y bajo un modelo de desarrollo de capacidades a las amenazas y ataques cibernéticos que puedan afectar tanto a los intereses nacionales como a la seguridad y defensa nacional, porque no es un proceso sencillo y requiere disponer del tiempo y recursos humanos, técnicos y operativos, suficientes para alcanzar la efectividad. Disponer a plenitud de estos recursos solo es posible, si su planeamiento, alistamiento y pruebas se realiza en tiempos de paz; de lo contrario, en tiempos de guerra no existirá disponibilidad de recursos porque los esfuerzos estarán concentrados en responder ante el enemigo.

6.4 Resultados a la luz de las unidades militares de ciberdefensa en Colombia

A pesar de que existen unidades militares responsables de la ciberdefensa, el tipo de organización de algunas unidades no es apropiado para el desarrollo de operaciones militares en el ciberespacio. De acuerdo con las estrategias internacionales de ciberdefensa, se puede evidenciar que estas unidades requieren cumplir objetivos que obligan a contar con una organización militar tipo OTAN.

Por otra parte, contar con una estrategia militar de ciberdefensa, permitirá a las unidades militares responsables de la ciberdefensa nacional, contar con los lineamientos, políticas y ejes estratégicos sobre los cuales se debe trabajar para el desarrollo de capacidades cibernéticas para el desarrollo de operaciones militares en el ciberespacio. Así, cada Fuerza necesitará fortalecerse en cada una de las competencias que requiera para cumplir a cabalidad su rol funcional en el nuevo dominio de guerra, pero siempre trabajando articulada y colaborativamente entre el Ejército Nacional, la Fuerza Aérea Colombiana y la Armada Nacional, bajo el direccionamiento del Comando Conjunto Cibernético y la Junta Asesora de Ciberdefensa. El trabajo colaborativo y mancomunado representa un componente estratégico de cara a fortalecer las capacidades militares en el ciberespacio, como lo afirma el autor Brad Bigelow en su artículo: "What are Military Cyberspace Operations Other Than War?":

> Las Fuerzas Militares del ciberespacio que tienen la intención de aplicar la fuerza o la amenaza de la fuerza contra los sistemas adversarios deben trabajar muy de cerca, si no lado a lado, con los elementos autorizados para recopilar inteligencia y llevar a cabo el reconocimiento y la vigilancia de estos adversarios. Esta inteligencia es esencial para

> apoyar el desarrollo y las pruebas de armas, técnicas y tácticas en el ciberespacio, para apoyar la selección de objetivos y la evaluación de ganancias / pérdidas de inteligencia y, en la mayoría de los casos, para obtener acceso a los sistemas que pretenden afectar (Bigelow, 2019, p. 5).

La integración de capacidades cibernéticas entre las diferentes Fuerzas Militares de Colombia, representa varios aspectos significativos en términos de economía de escala, complemento de fortalezas interinstitucionales, aprovechamiento del recurso humano y efectividad en las operaciones. Es decir, cuanto se requiera, las Fuerzas podrán integrarse a través de un Centro de Operaciones Cibernético Conjunto, que permitirá que cada Fuerza aporte e integre sus componentes más sólidos y fortalecidos en aras de alcanzar resultados positivos en el desarrollo de operaciones militares cibernéticas.

6.5 Resultados a la luz de las amenazas cibernéticas

Después de hacer un análisis sobre las amenazas cibernéticas latentes y emergentes en el contexto nacional, haciendo uso del instrumento "ventana de AREM" (Cano, 2017), es preciso afirmar que este instrumento facilitó la obtención de resultados, a luz de una óptica prospectiva de la amenaza. De esta manera y de forma colaborativa, fue posible identificar cuáles fueron las amenazas de mayor impacto que podrían desestabilizar al país desde el componente cibernético.

Tomando como base los resultados obtenidos, se aplicó el modelo DOMPILEM, el cual arrojó la obtención de unos productos que una vez implementados permitirán a las unidades militares responsables de la ciberdefensa, fortalecer o desarrollar las capacidades disuasivas, defensivas, ofensivas, de inteligencia y diplomacia cibernética requeridas para alcanzar los objetivos

estratégicos propuestos. La integración de los efectos cibernéticos en las operaciones militares para operacionalizar completamente el dominio es un proceso continuo a nivel nacional, al igual que es un área de desarrollo para la OTAN (Thompson, 2019).

7. Conclusiones

7.0 Introducción

Las incertidumbres en el panorama internacional y los rápidos cambios que se están produciendo en todos los ámbitos están teniendo una gran repercusión en las políticas de seguridad y defensa, tanto nacionales como internacionales (Gil, 2017). Para tal efecto, el desarrollo de capacidades en el ciberespacio debe constituir una prioridad para la seguridad de cualquier país dependiente de tecnología, así como comprender la importancia que tiene en la actualidad poder desplegar operaciones militares en el ciberespacio.

Por su parte, los modelos de defensa para las nuevas guerras o en particular la ciberguerra, exige cambios relevantes, como nuevos campos de acción y nuevos tipos de operaciones militares que permitan actuar a cientos de kilómetros y usar un sin número de armas sofisticadas usando internet. Sin embargo, es preciso garantizar la lógica de los conflictos a través de la aplicación de teorías de los clásicos de la guerra, que permitan contar con una vista concreta y práctica para fundar una estrategia militar en el contexto cibernético

Los Estados, así como las organizaciones internacionales, están desarrollando sus capacidades para hacer frente a estas amenazas cibernéticas que, por su rápido desarrollo en los últimos años, constituyen un reto en todos los ámbitos como es en el caso de la defensa, lo que "supone el replanteamiento de algunas de las premisas más asentadas de cómo debe articularse la defensa nacional y hacer viable un sistema de seguridad global" (Torres, 2011, pp. 329-348).

Finalmente, para tener mejores resultados en las misiones cibernéticas que aseguren la seguridad y defensa nacional, se hace necesario que las Fuerzas Militares realicen operaciones conjuntas

entre las diferentes Fuerzas, coordinadas con la Policía Nacional, interinstitucionales con organizaciones tanto del sector público como privado y combinado con las naciones amigas, apoyados siempre que se requiera por las ligas de ciberdefensa. Estas novedades suponen cambios en las doctrinas militares, plantean nuevas cuestiones estratégicas, o generan nuevos conceptos, como el de ciberguerra o ciberarma (Torres, 2011).

De aquí en adelante, independientemente de los intentos de conceptualización, hay que tener presente que el ciberespacio es y será fundamental en el ámbito militar y que, a diferencia de los otros dominios, este es esencial para el funcionamiento de los otros cuatro dominios de guerra (tierra, mar, aire, espacio). Por ello no habría que subestimar las posibles consecuencias que puede tener un ataque cibernético o las implicaciones y los cambios que está produciendo en el ámbito militar, pero sin sobredimensionar las consecuencias que ha tenido hasta ahora (Torres, 2011).

7.1 Cumplimiento de los objetivos del estudio

Este trabajo de investigación da respuesta a la pregunta central de este estudio, a través del desarrollo de cada uno de los objetivos específicos planteados para esta monografía de maestría.

En primer lugar, respecto del objetivo "Analizar el contexto actual en materia de organización y estrategias de las Unidades Militares responsables de la ciberdefensa en Colombia", se estudiaron las unidades responsables de la ciberdefensa en Colombia que se encuentran activas y operativas y se determinaron sus capacidades actuales y las necesarias para desarrollar operaciones militares de ciberdefensa. Adicionalmente se analizaron estrategias militares de ciberdefensa internacionales para establecer los avances de países que revisten importancia a nivel nacional. Es importante resaltar que, el análisis de las unidades responsables de ciberdefensa de las Fuerzas

Militares de Colombia y la comparación con los avances internacionales en materia de defensa cibernética, permitió establecer que se requiere contar con al menos una unidad de ciberdefensa por Fuerza, con una organización tipo OTAN, debidamente entrenada y equipada para desarrollar operaciones militares cibernéticas de acuerdo con su rol funcional; así mismo, con capacidades para articularse e interoperar para el desarrollo de operaciones conjuntas, combinadas, interinstitucionales y multinacionales.

Prosiguiendo con el análisis, en lo que refiere al objetivo "Identificar y detallar las amenazas cibernéticas latentes y emergentes que imponen las tecnologías disruptivas a la Ciberdefensa Nacional en Colombia", se aplicó el instrumento "La Ventana de AREM", y se obtuvieron las amenazas que revisten mayor importancia a la seguridad y defensa nacional. Es decir, los resultados obtenidos en el análisis de las amenazas cibernéticas, aportaron para la elaboración de una propuesta de la estrategia militar de ciberdefensa, tomando como eje fundamental los principales riesgos a la seguridad y defensa de nuestro país de cara a las tecnologías disruptivas.

Finalmente, para dar cumplimiento al tercer objetivo, "Diseñar una propuesta militar estratégica operacionalizable basada en el planeamiento por capacidades DOMPILEM. (Doctrina, Organización, Material, Personal, Infraestructura, Liderazgo y Educación, Entrenamiento y Mantenimiento)", esta investigación permitió plantear un modelo estratégico basado en objetivos estratégicos analizados en cada uno de los componentes del Modelo DOMPILEM. Con esto fue preciso delimitar y definir prospectivamente hacia dónde deben ir las Fuerzas Militares, a fin de desarrollar capacidades militares para el desarrollo de operaciones cibernéticas, soportadas en un marco legal y constitucional.

Para concluir que el objetivo general planteado: "Diseñar una Estrategia Militar de Ciberdefensa que permita afrontar las amenazas cibernéticas que impone las tecnologías disruptivas a la Ciberdefensa Nacional al 2022", se cumplió satisfactoriamente, toda vez que la estrategia militar de ciberdefensa para Colombia se desarrolló con base en un análisis situacional del contexto actual en materia de ciberdefensa en Colombia. Posteriormente, se complementó el análisis con otras estrategias que ya han sido desarrollados por países miembros de la OTAN. De forma paralela, se realizó el estudio de las amenazas latentes y emergentes que demandan las tecnologías disruptivas, a fin de planear en una prospectiva a corto plazo, las posibles alternativas de solución basadas en el modelo de desarrollo de capacidades denominado DOMPILEM.

7.2 Contribuciones a la ciberdefensa

La estrategia militar de ciberdefensa propuesta, es el resultado de la combinación de varios elementos. En primer lugar, fue contrastada con las estrategias militares de ciberdefensa internacionales oficiales que se encuentran publicadas en el Centro de Excelencia de la OTAN, y analizada con base en la experiencia y vivencias propias del autor. Posteriormente, se analizaron los requerimientos con base en el modelo DOMPILEN para definir los requerimientos que la apalanquen y permitan que pueda cumplirse. Por lo expuesto anteriormente, se considera que la estrategia es una alternativa que proporciona dirección, coherencia y lineamientos con un enfoque integral para el desarrollo de capacidades militares en el ciberespacio en los próximos años en las unidades militares responsables de la ciberdefensa nacional en Colombia.

7.3 Contribuciones a la práctica

La presente investigación presenta una propuesta de estrategia militar de ciberdefensa realizada con base en modelos internacionales y de acuerdo con las necesidades nacionales, que permite dar un paso adelante en la búsqueda del fortalecimiento de las capacidades cibernéticas para adquirir superioridad militar en el ciberespacio. Esto representa un avance para repensar la doctrina en materia de operaciones militares cibernéticas.

Adicionalmente, otra contribución se ve reflejada en el método de estudio usado con las estrategias militares de ciberdefensa internacionales para proponer la estrategia contrastada con el modelo de capacidades de las Fuerzas Militares DOMPILEM, previo a un análisis de amenazas realizado con base en la Ventana de AREM, que permitió pensar en las amenazas que nos esperan en un futuro cercano.

7.4 Trabajos futuros

El desarrollo de esta investigación, presenta dos aristas sobre la cuales futuros investigadores podrían desarrollar proyectos, la primera son las tendencias y estrategias militares de ciberdefensa en Latinoamérica, que permite conocer el enfoque de las Fuerzas Armadas de la región. La segunda, corresponde a estudiar la viabilidad de desarrollar operaciones Multilaterales de Ciberdefensa, como respuesta a los ataques a la seguridad cibernética, que fue considerada por la Organización de Estados Americanos (OEA) como una amenaza transnacional (Organización de Estados Americanos, 2003).

Referencias

Accenture. (2015). *Guiding digital transformation*, Recuperado de: https://www.accenture.com/t00010101t000000__w__/au-en/_acnmedia/accenture/conversion-assets/dotcom/documents/local/au-en/pdf/1/accenture-insight-digital-density-index-guiding-digital-transformation.pdf 16.

Aguilar, J. (2017). *Industria 4.0*: *La cuarta revolución industrial.* Editorial Marcombo. Recuperado de https://www.casadellibro.com/libro-industria-40-la-cuarta-revolucion-industrial/9788426725684/5991036

Altmann, J. (2004). *Military Uses of Nanotechnology: Perspectives and Concerns., Security Dialogue*, 35(1), 61-79. Recuperado de https://doi.org/10.1177/0967010604042536

Amaral, A. C. (2013). *La amenaza cibernética para la Seguridad y Defensa de Brasil*, 19–22. Recuperado de http://190.12.101.91:80/jspui/handle/123456789/32

Ashmore y William, C. (s. f.). *Impact of Alleged Russian Cyber Attacks.* Recuperado de https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf

Bigelow, B. (2019). *What are Military Cyberspace Operations* Other Than War ?, 1-17.

Cano, J. (2017) *La ventana de AREM.* Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. Recuperado de www.isaca. org/journal.

Cano, J. (2018). *IT-Insecurity: Pronósticos de seguridad de la información 2018*. Recuperado de http://insecurityit.blogspot.com.co/2017/10/pronosticos-de-seguridad-de-la.html

Cano, J. (2018) *Ciberdefensa Empresarial*: U*n marco conceptual y práctico en un entorno digitalmente inestable.* En García, P., Barragán, R. y Fuentes, N. M. (2018), *Actas XV Reunión Española de Criptología y Seguridad de la Información* (pp. 96-101). Recuperado de: https://www.researchgate.net/publication/328191823_Ciberdefensa_empresarial_Un_marco_conceptual_y_practico_en_un_entorno_digitalmente_inestable de: https://www.researchgate.net/publication/328191823.

Cano, J. (2018). C*iberconflictos en la era digital: Ciber-axiomas y recomendaciones*.

Recuperado de http://insecurityit.blogspot.com/2018/03/

CESEDEN. (2015). *Tecnologías disruptivas y sus efectos sobre la seguridad* 1, 1-130. Recuperado de www.ieee.es/.../DIEEET12-2015_Tecnologias_Disruptivas_EfectosSeguridad.pdf.

Charles, C. (1995). *Introduction to educational research*. San Diego, Ca: Longman Publishers USA.

Christensen, C. M. *The innovator's dilemma : when new technologies cause great firms to fail* / Clayton M. Christensen. p. cm. — (The management of innovation and change series) Includes index. ISBN 0-87584-585-1 (alk. paper) 1. Creative ability in business. 2. Industrial management. 3. Customer services. 4. Success in business. I. Title. II. Series. HD53.C49 1997

Clarke, R., y Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do*. New York, USA: HarperCollins Publishers.

Clausewitz, K. (2010). *De la Guerra*, 239. Recuperado de http://www.biblioteca.org.ar/libros/153741.pdf

COGFM. (2012). Disposición 036-2012. Bogotá: COGFM.

COGFM. (2018). *Manual Fundamental Conjunto MFC 1.0*. Bogotá: COGFM.

Companies, M., y Group, Z. I. (2019). *Informe de riesgos mundiales 2019*. Retrieved from https://www.marsh.com/ar/es/insights/research/informe-riesgos-globales-2019.html

DoD. (2015). *Strategic Cyber Defense.* DoD.

DoD. (2018a). *National Cyber USA,* (September). DoD.

DoD. (2018b). *Summary Cyber Strategy US*, 10. Tomado de https://ccdcoe.org/library/strategy-and-governance/

Echevarría II, A. J. (2003). *Clausewitz's center of gravity*, *LVI*(1).

Eissa, S., Gastaldi, S., Poczynok, I. y Zacarias, M. E. (2012). *El Ciberespacio -Implicaciones a la Defensa Nacional.* Recuperado de http://sedici.unlp.edu.ar/handle/10915/40210

Ferreira, P. (2018). *Oportunidades y Desafíos de Tecnologías Emergentes* (pp. 36-48). Recuperado de https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume 1 Issue 2/Spanish/05-peterson_s.pdf

EJC. (2017). *Manual Fundamental Doctrina*. (Centro de Doctrina del Ejército - CEDOE, Ed.) (Vol. 1). Bogotá: Imprenta Militar del Ejército Restricciones. Tomado de www.cedoe.mil.co

FF.MM. (2016). *Ciberdefensa Conjunta para las Fuerzas Militares*. Bogotá.

Gaitán, A. (2012). *El Ciberespacio*. Bogotá: Escuela de Guerra Colombia.

Vergara, E. (2017). *Operaciones militares cibernéticas*. Buenos Aires.

Gil J. M. (2017). *La integración del ciberespacio en el ámbito militar.* Grupo de Estudios en Seguridad Internacional. Recuperado de http://www.seguridadinternacional.es

Gobierno de Colombia. (2011). *CONPES 3701*, 91. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf.

Green, J. A. (2015). *Cyber Warfare. A multidisciplinary analysis* (pp. 6861-72). New York, USA: Routledge.

Guerrero, J. (n.d.). *Armas autónomas, la amenaza fantasma*. Recuperado de https://www.muyinteresante.es/revista-muy/noticias-muy/articulo/armas-autonomas-la-amenaza-fantasma-461487840117

Hernandez, Fernandez, Baptista. (2010). *Metodología de la Investigación*. Bogotá: Panamericana Formas e Impresos.

Joyanes Aguilar, L. (2017). *Industria 4.0 : la cuarta revolución industrial*. Editorial Marcombo. Recuperado de https://www.casadellibro.com/libro-industria-40-la-cuarta-revolucion-industrial/9788426725684/5991036

Kanlli. (2015). *Industria 4.0: La cuarta revolución industrial es la transformación digital.* Blog Innovación y Nuevas Ideas de Kanlli. Retrieved from http://www.kanlli.com/estrategia-marketing-digital/industria-4-0-la-cuarta-revolucion-industrial-es-la-transformacion-digital/

Kirkpatrick, Klobentz, Palmer, Denton, T. (2018). *Biotechnology Governance*: *Landscape and Options*, 29.

Klaus S. (2018). *The Fourth Industrial Revolution, by Klaus Schwab*. World Economic Forum. Retrieved from https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

Marchant, G. E., Allenby, B., Arkin, R., Barrett, E. T., Borenstein, J., Gaudet, L. M., Meara, R. O. (2011). *Science and Technology Law*.

Merriam, S. (2002) S. *Qualitative research in practice.* San Francisco: Jossey Bass. Recuperado de https://www.academia.edu/7103948/La_investigaci%C3%B3n_cualitativa_y_el_estudio_de_casos_m%C3%BAltiples [Consulta: 10/07/2019]

MinDefensa. (2012). *Resolución 7436-2012*. Bogotá: Ministerio de Defensa.

MFC1.0. (2018). *Manual Fundamental Conjunto* 1.0. *Manual Reservado Comando General Fuerzas Militares*. Bogotá: MFC1.0.

MoD. (2012). T*he Netherlands - The Defence Cyber Strategy*, 20. Recuperado de http://www.defensie.nl

MoF, M. (2013). P*olitical Guidance for Cyber Defence*, 31976–31979. Tomado de https://ccdcoe.org/library/strategy-and-governance/?organisations=nato&region=europe

NATO. (2016, July 9). *Warsaw Summit Communiqué.* Retrieved from http://www.nato.int/cps/en/ natohq/official_texts_133169.htm

NCOC. (2018). *Cyber Defence Strategy of the Czech Republic*, 17. Recuperado de https://www.vzcr.cz/uploads/69-Cyber-Defence-Strategy-2018.pdf

Newmeyer, K. (2015). *Ciberespacio, Ciberseguridad y Ciberguerra*. pp. 88-89. Recuperado de http://virtual.esup.edu.pe/handle/ESUP/113 [Consulta: 20/07/2019).

Nye, J. S. (2017). *Deterrence and Dissuasion in Cyberspace, International Security*. 1(1), 44-71. Recuperado de https://doi.org/10.1162/ISEC.

Office of the Director of National Intelligence, 2014. Retrieved from https://www.dni.gov/index.php/who-we-are/leadership/director-of-national-intelligence

Organización de Estados Americanos. (2003). *Declaración Sobre Seguridad en las Américas* www.oas.org/juridico/spanish/decl_security_sp.pdf

Resolución Ministerial No. 7436 de 2012. Ministerio de Defensa de Colombia Documento Reservado.

Rui J. (2013). *Political Guidance for Cyber Defence Portuga*l (pp. 31976-31979).

Rusell, S. (2000). Inteligencia Artificial. *Revista Iberoamericana de Inteligencia Artificial* (Vol. 10). Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi-gb683ZHkAhUqqlkKHbLvAsAQFjAAegQIABAC&url=https%3A%2F%2Fluismejias21.files.wordpress.com%2F2017%2F09%2Finteligencia-artificial-un-enfoque-moderno-stuart-j-russell.pdf&usg=AOvVaw2e8_bmnkYRiI0QTVzWPSFa [Consulta: 10/06/2019]

Scharre, P. (2019). *Army of None: Autonomous Weapons and the Future of War*.

Schwab, K., & Botín, A. P. (2016). *La Cuarta revolución industrial. Debate*. Retrieved from https://www.casadellibro.com/libro-la-cuarta-revoluci0n-industrial/9788499926940/4073100

Schwab, K. (2018). *The Fourth Industrial Revolution.* World Economic Forum. Recuperado de https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

Sculpteo. (2018). The state of 3D printing. Retrieved from https://www.sculpteo.com › State_of_3DP_2018

Segars, A. H. (2018). S*even Technologies Remaking the World*. MIT Sloan Management Review.

Sgora, A., Vergados, D. D., & Chatzimisios, P. (2013). *A survey on security and privacy issues*

in Wireless Mesh Networks. Recuperado de https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.846

Stake, R. (1996). *The art of case study*. Thousand Oaks. Ca: Sage Publications

Stake, R. (2006). *Multiple case study analysis*. New York: The Guildford Press.

SonicWall. (2019). *Informe de Amenazas Cibernéticas de SonicWall 2019*. Recuperado de https://www.sonicwall.com/resources/white-papers/2019-cyber-threat-report-global-executive-summary-spanish/

SophosLab. (2019). *Informe de amenazas 2019*. Recuperado de https://www.sophos.com/es

SonyWall. (2019). *Informe de ciberamenazas 2019 de SonicWall.* Recuperado de https://www.sonicwall.com/resources/white-papers/2019-cyber-threat-report-europe-executive-summary-spanish/

SophosLab. (2019). *Informe de amenazas 2019*. Rceuperado de https://www.sophos.com/es-es/medialibrary/PDFs/.../sophoslabs-2019-threat-report.pd.

Strategy Department Defence. (2014). *Cyber Security Strategy for Defence* (pp. 1-18).

Symantec, 2019. *El Informe sobre las amenazas para la seguridad en Internet 2019 (ISTR).* Recuperado de https://www.symantec.com/es/es/security-center/threat-report

Theiler, O. (2011). "Nuevas amenazas: el ciberespacio". *Revista digital de la OTAN.* Recuperado de http://www.nato.int

Torres, M. R. (2011). "Los dilemas estratégicos de la ciberguerra". *Revista Ejército*, No. 839, 14-19.

Torres, M. R. (2013), "Ciberguerra". En Jordán Javier (Coord.), Manual de Estudios Estratégicos y Seguridad Internacional, Madrid: Plaza y Valdés, pp. 329-348.

Van Der Meer, S. (2016). *Cyber Warfare and Nuclear Weapons:* Game-changing Consequences?, (December), 36–38. Recuperado de http://www.techworld.com/news/security/cambridge-researchers-

Vergara, E. (n.d.). *Operaciones Militares Cibernéticas*.

William, C. (s.f.). *Impact of Alleged Russian Cyber Attacks.* Recuperado de https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf

World Economic Forum. (2012). *Asociación por la Resiliencia Cibernética.* Recuperado de http://www.innovacion.gob.pa/descargas/Asociacion%20por%20la%20Resiliencia%20cibernetica%20WEF.pdf.

Yampolskiy, R. V. (2017). *AI Is the Future of Cybersecurity, for Better and for Worse.* Recuperado de https://hbr.org/product/ai-is-the-future-of-cybersecurity-for-better-and-for-worse/H03NES-PDF-ENG