Cooperación internacional y ciberdiplomacia como mecanismo para mitigar las ciberamenazas en Colombia

Fernando Andrés Ramos 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

COOPERACIÓN INTERNACIONAL Y CIBERDIPLOMACIA COMO MECANISMO PARA MITIGAR LAS CIBERAMENAZAS EN COLOMBIA.

ALUMNO:

FERNANDO ANDRES RAMOS DIAZ

DIRECTOR:

Pedro Aníbal Buitrago Rincón

GRUPO DE INVESTIGACION

MASA CRÍTICA

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO

BOGOTA – COLOMBIA

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

COOPERACIÓN INTERNACIONAL Y CIBERDIPLOMACIA COMO MECANISMO PARA MITIGAR LAS CIBERAMENAZAS EN COLOMBIA.

FERNANDO ANDRES RAMOS DIAZ

DIRECTOR:

Pedro Aníbal Buitrago Rincón

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTA – COLOMBIA

2019

TABLA DE CONTENIDO

	Pág.
INTRODUCCIÓN	1
I. ENTENDIENDO EL CIBERESPACIO Y SUS AMENAZAS	3
1.1. La naturaleza del ciberespacio y sus amenazas	3
II. CIBERAMENZAS: UN PROBLEMA DEL ORDEN TRANSNACIONAL	22
2.1. Medidas de contención para las ciberamenazas en la agenda internacional.	22
2.2. Ciberseguridad: Estrategias para combatir las ciberamenazas.	27
2.3. Agenda Internacional para asuntos de ciberdefensa y ciberseguridad.	30
III. LA COOPERACIÓN DIPLOMÁTICA COMO COROLARIO EN LA GESTIÓN DE LAS CIBERAMENAZAS	35
3.1 Nuevas perspectivas frente a la lógica diplomática en relación con la ciberseguridad	35
3.2 La experiencia europea frente a la de la ciberdiplomacia	39
3.3 Transformaciones pendientes para Colombia en la gestión de las ciberamenazas.	44
CONCLUSIONES	53

INTRODUCCIÓN

El mundo actual expone un gran desarrollo, las fronteras y los límites tradicionales se han borrado por cuenta de la globalización por la globalización, la tecnología, las telecomunicaciones y con ello generación de relaciones de interdependencia entre los diferentes actores estatales y no-estatales, que inciden en las dinámicas de seguridad.

Considerando la dimensión trasnacional de las amenazas que afectan el ciberespacio, mitigar los factores de riesgo constituye una tarea inherente a los Estados y los diferentes actores que tengan relación con él, toda vez, que asumir posturas no colaborativas corresponde a una visión anacrónica frente a la gestión compartida de los riesgos. Bajo esta perspectiva, la cooperación internacional frente a la gestión compartida de riesgos en el ciberespacio constituye una tarea imprescindible al momento de pensar en la consolidación de las condiciones de seguridad de dicho entorno.

En este contexto, el presente documento tendrá como pregunta de investigación: ¿Cuál es el impacto de la cooperación internacional frente a la gestión de riesgos y amenazas en el ciberespacio? En dicho orden de ideas se plantea la presente investigación, en aras de aportar una perspectiva crítica que permita establecer las vías más eficaces que puedan considerarse al momento de mitigar los riesgos y amenazas propios del ciberespacio.

Para desarrollar el propósito de la investigación, el documento se encuentra dividido en tres capítulos cada uno de los cuales busca desarrollar los objetivos específicos de la investigación. El primer capítulo caracteriza y ahonda en la naturaleza del ciberespacio. En el segundo capítulo se presentan los mecanismos de cooperación internacional, como una

herramienta imprescindible en la mitigación de los riesgos y amenazas del ciberespacio, adoptando la postura de la gestión compartida del riesgo. En el tercer capítulo, se expone una hoja de ruta que pueda ser seguida por Colombia para la mitigación exitosa de los riesgos y amenazas propias del ciberespacio, para dichos efectos se establece un inventario de las capacidades requeridas desde un enfoque integral, en relación con las condiciones requeridas para garantizar entornos seguros.

La investigación aquí presentada fue diseñada como un estudio de caso de orden cualitativo para lo cual se abordó la revisión sistemática de literatura especializada, priorizando fuentes secundarias a partir de las cuales pudieran ser desarrolladas las variables de estudio seleccionadas.

I. ENTENDIENDO EL CIBERESPACIO Y SUS AMENAZAS

1.1. La naturaleza del ciberespacio y sus amenazas

El mundo actual expone un gran desarrollo, las fronteras entre los países han sido borradas por la globalización, la tecnología, las telecomunicaciones tiene múltiples canales por los que transitan millones de datos, en este mundo avanzado las amenazas a la defensa se han multiplicado por la dependencia que tanto el sector público como privado tienen por el internet. El país hoy en día traslada su defensa a un nuevo escenario, que se caracteriza principalmente por el manejo de información que corre a una gran velocidad, este escenario es el ciberespacio.

El ciberespacio como nuevo escenario de la guerra, requiere de operaciones de defensa de las distintas naciones que pasaron del campo físico al campo virtual, generando un cambio en las políticas y estrategias, obligándolas a estar actualizando permanentemente, buscando tener personal especializado, mejorar y optimizar los recursos para poder tener una estructura sólida, que construya barreras adecuadas para contrarrestar los ciberataques sin importar su origen.

La ciberdefensa es real, es un aspecto muy importante que requiere ser analizado para determinar las amenazas que se pueden presentar y las implicaciones que generarían dichas amenazas, especialmente si tenemos en cuenta que toda la infraestructura crítica del país, en la actualidad, se maneja a través de una red de sistemas que funcionan sobre una gran red. Uno de los principios de la guerra nos dice que hay que derrotar al enemigo sin combatir,

seguramente cuando Sun Tsu escribió esto, no llegó a concebir que ello se podría llegar a dar en gran medida mediante las estrategias cibernéticas, pues el combate ya no se desarrolla mediante los medios tradicionales, contacto físico o el uso de armas como tanques, aviones, buques o la misma infantería, ya en los grandes conflictos las guerras se desarrollan desde oficinas, lejos del área de combate a cientos o miles de kilómetros del enemigo y con un poder de ataque que podría ser virtualmente mayor que las armas convencionales.

El ciberespacio es un escenario que debe ser tomado como un pilar de la defensa de Colombia, se debe modernizar constantemente en material, equipos tecnológicos, también diseñar estrategias de ciberdefensa, igualmente el personal encargado de ciberdefensa y ciberseguridad se debe preparar en este campo. Con esto poder tener una organización capaz de enfrentar los retos que se presentan en la defensa del ciberespacio.

La incorporación paulatina de sistemas tecnológicos, para el desarrollo de operaciones militares facilitó las coordinaciones entre las diferentes unidades a través del uso de sistemas de comunicación, y el interés de las fuerzas enemigas para negar esta capacidad, permitieron el surgimiento de la Guerra Electrónica.

El primer evento en el que se empleó esta capacidad, y del que se tenga conocimiento, se presentó en la batalla de Tsushima, durante la guerra rusojaponesa en el mes de mayo de 1905 (Thurbon, 1977); tal ha sido la relevancia obtenida, que, actualmente, se cataloga como un elemento estratégico multiplicador del poder de combate (Gordon, 2014).

La investigación y desarrollo tecnológico al servicio de la seguridad nacional permitió

que, en 1957, se lanzara el satélite Sputnik, convirtiendo el espacio en el cuarto dominio de la guerra. Más adelante, en este mismo año, gracias a un proyecto militar estadounidense, en el que se buscaba crear una red de equipos de cómputo que uniera los centros de investigación de defensa de los Estados Unidos, que presentara altos niveles de resiliencia, y que permitiera una conexión constante, a pesar de verse afectados por un ataque nuclear, dio origen al ciberespacio (Melamud, 2005).

El ciberespacio es definido como una red interdependiente de infraestructuras tecnológicas, donde se incluye: el internet, las redes de telecomunicaciones, los sistemas de cómputo, los controladores y los procesadores de las industrias críticas de los Estados. (Spade, 2012).

Desde que se incorporaron los equipos de cómputo en las operaciones militares y se dio la transmisión de datos a través de redes de información, los comandantes cuentan con información en tiempo real acerca de la ubicación de sus unidades y la situación en el campo de batalla; facilitándoles el proceso de toma de decisiones. Esto, complementado con la capacidad de realizar la entrega de armamento de una forma más precisa.

Hoy en día, podemos afirmar que la tecnología ha generado un sin número de ventajas a las Fuerzas Militares permitiéndoles ser más efectivas y eficaces en el cumplimiento de su misión; no obstante y de forma paralela, ha generado una alta dependencia de estos sistemas, y a su vez grandes vulnerabilidades, las cuales pueden llegar a ser explotadas por las fuerzas enemigas, poniendo en riesgo la seguridad nacional.

1.2. Antecedentes

1.2.1 Ciberguerra

En el mes de agosto de 2006, ataques cibernéticos realizados desde la República Popular China infiltraron los sistemas de información que eran utilizados por miembros del Congreso y del Comité de Asuntos Exteriores de la Cámara de los Estados Unidos de Norteamérica. El congresista Frank Wolf (R-VA) sostiene que "la información era crítica y sensible sobre la política exterior estadounidense y el trabajo del Congreso" (Wolf, 2008).

En el mes de abril de 2007, las cuentas de correo electrónico del Secretario de Defensa de los Estados Unidos, Robert Gates fueron vulneradas, al igual que los sistemas de información de varias otras agencias y departamentos Gubernamentales a causa de una serie de Ciberataques. (Instituto español de estudios estratégicos, 2010, p. 95).

Posteriormente en el año 2007, Estonia experimento un bloqueo general de sus instituciones Gubernamentales entre las cuales se encontraban el parlamento, ministerios, medios de Comunicación y el sistema financiero a causa de una serie de ataques de denegación de servicio, lo cual requirió de la intervención de la comunidad internacional y de la Organización del Tratado del Atlántico Norte.

En el año 2008, durante el conflicto entre la Federación Rusa y Georgia, por Osetia del Sur, se presentaron acciones militares entre ambos países; sin embargo, Rusia lanzó una seria de ataques cibernéticos, entre los que se detectaron ataques de defacement, dirigidos hacia sitios

web de instituciones gubernamentales, políticas y financieras; ataques de denegación de servicio hacia las páginas de la presidencia, del parlamento y varios ministerios; asimismo insertaron un código malicioso en otros portales gubernamentales. Estos ataques causaron un gran impacto a nivel gubernamental, lo que sumado a la falta de disponibilidad de los sitios web de las instituciones centrales del Estado causó un efecto desalentador en los ciudadanos de la República de Georgia. (Organización del Tratado Atlántico Norte, 2008)

En el mes de julio de 2009, Nuevamente instituciones Gubernamentales Estadounidenses fueron blanco de una serie de ciberataques que afectaron la Comisión Federal de Comercio, el Departamento de Defensa, la Casa Blanca, entre otros (DNP, 2011, p. 6)

Entre el 2007 y el 2009, personal de la República Popular China logró la exfiltración de datos sobre el programa de diseño del avión de combate F-35, desarrollado por la compañía Lockheed Martin. Los investigadores forenses encontraron que los intrusos obtuvieron datos sobre el diseño del avión, las estadísticas de rendimiento y sistemas electrónicos. A su vez, rastrearon que las actividades maliciosas se originaban desde direcciones de protocolo de Internet chinos, usados en intrusiones de red anteriores. (Spade, 2012)

En Colombia se han presentado un sin número de ataques, entre los cuales se encuentran ataques de DDos contra páginas de entidades gubernamentales. El día 11 de abril de 2011 fue atacada la página web del Ministerio del Interior y de Justicia de Colombia, como protesta por el proyecto de ley que impulsó este ministerio, proyecto que buscaba penalizar la piratería informática; dicha iniciativa era conocida en la red como ley Lleras (por el entonces ministro Germán Vargas lleras). Tres días después fue atacada la página del Senado de Colombia y el

programa Gobierno en línea. Posteriormente, el 15 de abril de 2011 el objetivo fue la página web de la presidencia de república. (Reuters, 29 de febrero de 2012).

1.2.2 Marco Teórico Contextual

Durante este siglo, organizaciones internacionales como la Organización de las Naciones Unidas (ONU), la Organización de Estados Americanos (OEA) y sus estados miembros comenzaron a preocuparse por los nuevos desafíos y amenazas que atentan contra la estabilidad y la seguridad mundial. (Niño, 2014).

Así mismo, a principios del año 2002, en el marco de la Asamblea General de las Naciones Unidas, en la "Resolución No 57-53", los Estados miembros manifestaron su preocupación por la utilización de medios y tecnologías de información en contra de la estabilidad y seguridad internacional; puesto que la infraestructura de los Estados se afecta negativamente y, por ende, la seguridad civil y militar. A su vez, se invitó a los Estados miembros a determinar los criterios básicos en cuanto a la seguridad de la información, especialmente, con el uso apropiado e ilícito de las tecnologías de la información y las telecomunicaciones. (Organización de las Naciones Unidas [ONU], 2002).

Posteriormente, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), en el marco del cuarto periodo de sesiones, celebrado en la ciudad de Montevideo, Uruguay, del 29 al 30 de enero de 2004, estableció el compromiso, por parte de los Estados miembros, para identificar y combatir las amenazas emergentes, tales como las amenazas a la seguridad cibernética. (Organización de los Estados Americanos [OEA], 2004).

Teniendo en cuenta que la dinámica de la sociedad moderna y la interconectividad requerida para el funcionamiento de los diferentes sistemas (los cuales permiten su normal desarrollo) hacen que estos sean altamente vulnerables ante ataques electrónicos y cibernéticos, las principales amenazas se ven representadas por algunos Estados Nación, actores trasnacionales y organizaciones criminales, las cuales buscan explotar las vulnerabilidades propias de la infraestructura de las tecnologías de la información (TI) y de su interacción a través del ciberespacio (Ver tabla 1).

Tabla 1. *Adaptación de las amenazas a la seguridad nacional.*

AMENAZA	METODOLOGÍA	OBJETIVO CIBER	OBJETIVO G.E
Hackers	Ingreso a sistemas y redes privadas, vulnerando los sistemas.	Robo, fraude, denegación de servicio y extorsión.	Espionaje, robo de información, extorsión.
Crimen Organizado	Aprovechar actividades online. Descifrar códigos.	Interés económico.	Interés económico.
Terroristas	Atacar sistemas interconectados a la red.	Adquirir información para el planeamiento de ataques físicos o cibernéticos.	Adquirir información de agencias gubernamentales y de las Fuerzas Militares.
Estados Nación	Desarrollo de ciber-capacidades ofensivas, técnicas y operativas.	Espionaje y ciberataques en el marco de una ciberguerra.	Negar el uso del espectro electromagnético a las Fuerzas Militares y bloquear los sistemas de vigilancia y alerta temprana, Comando y Control y Comunicaciones

Fuente: Office of the Homeland Security, National Strategy for Homeland Security.

Con el fin de ejercer control e influencia, los Estados-Nación han desarrollado capacidades militares en cada uno de los dominios naturales: poder naval (buques) para proteger sus costas, controlar las líneas marítimas y atacar a otros Estados; poder terrestre (ejércitos y vehículos) para controlar, defender y extender sus fronteras; el poder aéreo (aeronaves y sistemas de

defensa antiaérea) y espacial (naves espaciales y satélites) para atacar a otros por medio del cielo, defenderse de otros ataques y conducir la observación; sin embargo hoy en día enfocan el desarrollo de capacidades en materia de Guerra Electrónica y Ciberoperaciones (Spade, 2012).

Ante esto, Colombia, con el Plan Nacional de Desarrollo 2014-2018, establece dentro de los objetivos, estrategias y metas (Departamento Nacional de Planeación [DNP], 2015b, p. 6 y 474), los siguientes:

> **OBJETIVOS**
>
> **A. Fortalecimiento de los roles del Estado para el goce efectivo de derechos de todos los habitantes del territorio**
>
> • **Objetivo 1.** Proveer seguridad y defensa en el territorio nacional. [...]
>
> **C. Asegurar el respeto de la soberanía nacional y la protección de los intereses nacionales**. Como garantes de la soberanía y de la integridad territorial, las Fuerzas Militares tienen la obligación constitucional de emprender todas las acciones encaminadas a proteger, frente a cualquier tipo de agresión externa o interna, estos dos valores, en los dominios terrestre, marítimo, fluvial, aéreo, espacial y ciberespacial. Ello supone impedir la ocurrencia de eventos relacionados con ataques contra la infraestructura crítica de la nación, todo tipo de acciones ilegales tendientes a obtener control sobre el territorio nacional o ataques cibernéticos contra los intereses nacionales. [...]:

Mantenimiento de las capacidades disuasivas para la seguridad y defensa nacional: en línea con la tradición de respeto por el derecho internacional, los principios de no agresión y de cooperación internacional, el Gobierno nacional mantendrá una capacidad disuasiva creíble dentro de una postura estratégica defensiva que le permita cumplir tanto con su mandato constitucional, como responder a potenciales amenazas. [...]

Fortalecimiento de las capacidades en ciberdefensa: Colombia deberá desarrollar capacidades que permitan atender las amenazas cibernéticas y sus riesgos asociados, así como fortalecer las capacidades de neutralización y reacción ante incidentes o ataques informáticos que atenten contra la infraestructura crítica digital y la soberanía nacional. Para ello, se desarrollará, entre otras la siguiente línea de acción:

[...]

- Fortalecimiento de las capacidades disuasivas del país en el ciberespacio y posicionamiento de Colombia en la región como referente en Ciberdefensa.

Con el panorama internacional y de acuerdo con las directrices planteadas por el Departamento Nacional de Planeación [DNP] en el Plan Nacional de Desarrollo 2014-2018 [PND 2014-2018], y en el documento CONPES 3854 de 2016 titulado "Política Nacional de Seguridad Digital" donde se establecen unos nuevos objetivos dirigidos a la defensa y seguridad nacional en el entorno digital.

Allí se establece que la Política Nacional de Seguridad Digital adoptará una visión

holística con gestión sistemática y cíclica del riesgo, será liderada desde el alto nivel del gobierno y asegurará la defensa y seguridad nacional en el ámbito digital.; así mismo, con el objetivo de que el País tenga una visión estratégica en seguridad digital; se creará la figura de coordinador nacional de seguridad digital, quien tendrá las herramientas jurídicas que le permitirán desempeñar sus funciones con la mayor efectividad. Dicha figura será un funcionario dependiente del Departamento Nacional de Planeación, el cual tendrá entre otras funciones las de dirigir la implementación de la Política Nacional de Seguridad Digital y hacer seguimiento continuo de la misma, Garantizar que el alcance de la seguridad digital en el País este enfocada a enfrentar nuevos tipos de crimen, delincuencia, y otros fenómenos que afecten la seguridad. Así mismo, este objetivo se desglosó en 4 objetivos estratégicos entre los cuales se busca "fortalecer la Capacidad operacional, para Ejercer y mantener el dominio del espacio aéreo, disuadir la amenaza, derrotar el enemigo y contribuir a los logros de los fines del Estado." (2015b, p. 16). Igualmente, este objetivo establece dos objetivos específicos, a saber:

A. Objetivo específico No. 1 fortalecer la capacidad Operacional

Tener la superioridad y capacidad para enfrentar la amenaza contando con la estandarización operacional, infraestructura, equipos, armamento, el despliegue operacional, talento humano adecuado. Entrenando e incrementando la proeficencia operacional del personal de vuelo de acuerdo a los estándares establecidos, que configure el tamaño de fuerza requerido para brindar sostenibilidad en el desarrollo de operaciones aéreas.

B. Objetivo No 2 Liderar la Seguridad y Defensa del Poder Aéreo y Espacial del País Se pretende ir a la vanguardia, innovar, orientar y tener iniciativa en medidas de prevención, disuasión y reacción, para proteger al personal, aeronaves e infraestructura del poder aeroespacial del país buscando un posicionamiento regional.

1.2.3 La capacidad de guerra electrónica

La guerra electrónica es una capacidad ineludible para las fuerzas armadas actuales. Cuando, en términos generales, se habla de guerra electrónica, nos estamos refiriendo al conjunto de acciones militares encaminadas al control y utilización del espectro electromagnético en beneficio de las fuerzas propias, tanto para acciones defensivas, como de explotación o de ataque. En la doctrina militar, esto se define como la acción militar para explotar el espectro ElectroMagnético (EM), el cual comprende la interceptación e identificación de las emisiones electromagnéticas, el empleo de la energía electromagnética, incluyendo la energía dirigida, para reducir o prevenir el uso hostil del EM y acciones para asegurar su uso efectivo por las fuerzas propias.

Colombia que no es ajena a esta realidad mundial, identificó la necesidad de adquirir las capacidades de guerra electrónica en la década de los 90, inicialmente con la adquisición e implementación de sistemas de autoprotección electrónica abordo de aeronaves de superioridad aérea, y ataque; así como también de los sistemas de vigilancia y alerta temprana.

Posteriormente, se reconoció la importancia de contar con la capacidad de interceptar, interferir y negarle la capacidad de utilización del espectro electromagnético al enemigo, para tal fin, se creó el año 2010 una estructura organizacional para el desarrollo de capacidades de Guerra electrónica.

De la misma forma, se establecieron, doctrinariamente, las operaciones de Guerra Electrónica dentro de la Función de multiplicar las Fuerzas y la define como "actividad militar que se apoya en el empleo de la energía electromagnética para destruir, neutralizar o reducir la capacidad de combate enemiga, sacar provecho del uso del espectro electromagnético del oponente y asegurar el empleo eficiente de las emisiones electromagnéticas propias" (p. 115).

FUNCIÓN	MISIÓN TÍPICA	OPERACIÓN TIPO
Multiplicar las Fuerzas	Guerra Electrónica	Ataque electrónico
		Protección electrónica
		Apoyo a la guerra electrónica

Fuente: Manual de Doctrina Básica Aérea y Espacial.

En el año 2010 se publicó el primer manual de doctrina de Guerra Electrónica y se inició a desarrollar y socializar como concepto en las diferentes unidades. Para el año 2014, se implementó el Centro de Guerra Electrónica, con el fin de desarrollar las capacidades operativas en este ambiente operacional" (Fuerza Aérea Colombiana, 2015); además, establece las tres áreas operacionales:

a. Protección electronica (DOD, 2014)

La protección electrónica corresponde a todas aquellas acciones encaminadas a proteger al personal, las facilidades y los sistemas de cualquier uso del espectro electromagnético amigo o enemigo que pueda degradar, neutralizar, o destruir nuestra capacidad de combate.

Para proteger las capacidades de combate propias y amigas, se debe:

- Realizar una actualización constante del orden de batalla electrónico (OBE) amigo y enemigo.
- Realizar ejercicios que permitan coordinar el uso de las capacidades para asegurar los sistemas.
- Coordinar el uso del espectro electromagnético con las demás fuerzas.
- Realizar un entrenamiento utilizando las medidas pasivas y activas, bajo condiciones normales, condiciones de alerta o amenaza de ataque electrónico, donde se logre identificar cuando un sistema está siendo degradado.

b. Actividades de protección electrónica

Las actividades que se deben desarrollar para que haya protección electrónica son:

- Fortalecimiento electrónico.
- Enmascaramiento electrónico.
- Control de emisión.
- Administración del espectro electromagnético.
- Modos de reserva para tiempos de guerra.

- Compatibilidad electromagnética.

c. Soporte Electrónico

El soporte electrónico corresponde a la división de la guerra electrónica (GE) donde se involucran capacidades que están bajo el control directo del comandante operacional, con el fin de interceptar, identificar, ubicar o localizar la energía electromagnética irradiada intencional o fortuitamente, con miras a identificar, analizar, planear y realizar operaciones.

Para proporcionar soporte electrónico, se debe:

- Corroborar otras fuentes de información o inteligencia.
- Conducir y realizar operaciones de ataque electrónico.
- Ejecutar las medidas de autoprotección.
- Asignar sistemas de armas.
- Crear o actualizar las bibliotecas de misión.

i. Actividades de soporte electrónico

Las actividades desarrolladas para dar soporte electrónico son:

- Reconocimiento electrónico.
- Inteligencia electrónica.
- Seguridad electrónica.

ii. Ataque Electrónico

El ataque electrónico corresponde a la división de la Guerra Electrónica que involucra el uso de energía electromagnética, energía dirigida o armamento anti-radiación, con el propósito de atacar personal, facilidades o equipo, con la intención de degradar, neutralizar, o destruir la capacidad de combate del enemigo.

iii. Actividades de ataque electrónico

Las actividades desarrolladas durante un ataque electrónico son:

La capacidad de ciberoperaciones

Hoy, gracias a la evolución tecnológica, la doctrina básica de la USAF, lo define como "la capacidad de proyectar el poder militar o influencia a través del control del aire, espacio y ciberespacio para lograr los objetivos estratégicos, operacionales y tácticos" (Fuerza Aérea de los Estados Unidos, 2011, p. 12).

El General de la Fuerza Aérea Norteamericana, Henry Arnold, afirma que la Fuerza Aérea debía pensarse en términos del mañana, puesto que la evolución tecnológica continuará a un ritmo sin precedentes; de manera tal que el poder aéreo del mañana estará en el ciberespacio. El rápido adelanto de las tecnologías de la información y las telecomunicaciones, y su vínculo con las operaciones físicas hacen que el ciberespacio sea cada vez más importante para el éxito militar. (Fadok & Raines, 2012).

Como resultado del trabajo realizado por las dependencias involucradas en el desarrollo de la iniciativa estratégica en el mes de agosto del 2014, la creación de la Dirección de Cibernética Aeroespacial, la cual dependerá directamente de la Jefatura de Inteligencia Aérea (JIN) y tendrá como misión: "Planear, coordinar y defender la infraestructura crítica de la Fuerza Aérea Colombiana; además de ejecutar acciones en el ciberespacio que fortalezcan las capacidades institucionales en apoyo al cumplimiento de la misión; dicha dirección tendrá la siguiente estructura organizacional.

Es de vital importancia recalcar que la Fuerza Aérea ya se encuentra trabajando en la implementación y uso de las ciberoperaciones dentro de un terreno defensivo; no obstante, el desarrollo y evolución de las ciberoperaciones ofensivas a nivel mundial toman mayor importancia con el trascurrir del tiempo y el avance en la tecnología de la información; lo que ha reflejado un nuevo espacio, donde se librarán las batallas del futuro. Claro está, estas capacidades, que desarrollen los países en la parte de las ciberoperaciones, serán muchos más efectivas si tienen la capacidad de trabajar en conjunto con las operaciones aéreas, Guerra Electrónica y las realizadas en el ciberespacio. Esta combinación será exitosa solamente si la Fuerza Aérea reconoce la necesidad de apoyar la implementación, dentro de su doctrina, de las nuevas capacidades que la tecnología nos brinda dentro y fuera del campo de combate.

De acuerdo con lo anterior, el Manual de Doctrina Básica Aérea y Espacial (MABDA), en su cuarta edición, establece que, para la FAC, controlar el ciberespacio es:

> (...) alcanzar la superioridad ciberespacial, la cual consiste en lograr ventajas operacionales en cualquier momento, a través del empleo del ciberespacio, sin ningún

tipo de interferencia. La superioridad ciberespacial permite tener libertad de acción y alcanzar los efectos deseados en los diferentes ambientes de empleo, contribuyendo en el desarrollo de las operaciones Aéreas y Espaciales. (Fuerza Aérea Colombiana, 2013); Así mismo establece las misiones típicas y operaciones tipo como se relaciona en la tabla No 3.

Tabla 3. *Función*

FUNCIÓN	MISIÓN TÍPICA	OPERACIÓN TIPO
Controlar el aire, el espacio y el ciberespacio	Operaciones ciberespaciales	Ciber-Inteligencia.
		Ciber-Defensa.
		Ciber-Operaciones.

Fuente: Manual de Doctrina Básica Aérea y Espacial.

Es importante tener claro que el ciberespacio está compuesto por una capa física y una virtual. La capa física está compuesta por computadoras, servidores, routers, procesadores, satélites, interruptores y cables. La parte virtual está formada por conexiones electrónicas y por los datos enviados entre y almacenados en las piezas de su infraestructura física. (Spade, 2012).

Si bien es cierto que controlar el ciberespacio es un reto sumamente ambicioso de lograr, como lo es el de controlar el espacio se debe lograr, por lo menos, el control de la infraestructura física propia y las redes de información que le permiten el flujo de datos entre los diferentes sistemas; en pocas palabras, debe controlar la infraestructura crítica de la Fuerza y, en un futuro, lograr desarrollar sus propias aplicaciones e implementar redes propias, buscando una reducción paulatina de la dependencia de proveedores de tecnología y de servicios.

Las operaciones tipo establecidas en materia de ciberoperaciones se relacionan a continuación;

a. **Ciberinteligencia.** Corresponde a las operaciones realizadas en el ciberespacio, encaminadas a recolectar, procesar, explotar y difundir información para el planeamiento y ejecución de operaciones aéreas, espaciales y ciberespaciales; también, se realizan actividades de contrainteligencia para detectar y combatir las intrusiones avanzadas.

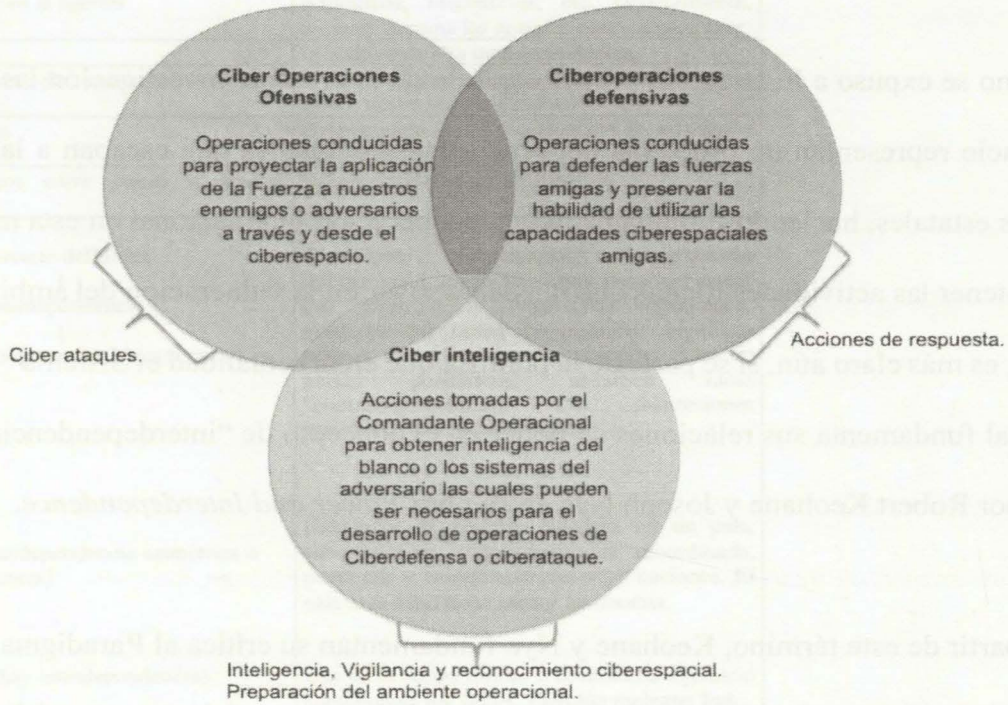
b. **Ciberdefensa.** Corresponde a las operaciones que se realizan en el ámbito militar o no y las cuales buscan contribuir al logro de los objetivos nacionales. Este tipo de operaciones busca proteger y defender la infraestructura crítica, la cual le permite a las Fuerzas Militares cumplir con su misión. A diferencia de las operaciones ofensivas, las operaciones de defensa no requieren el alto nivel de coordinación ni de autorización.

Los cuatro objetivos de la ciberdefensa son:

- Proteger la infraestructura crítica operacional.
- Detectar cualquier ciberataque.
- Recuperar los sistemas que hayan sido comprometidos durante el ataque.
- Responder al ciberataque mediante la ejecución de operaciones ofensivas.

c. **Ciberataque.** Corresponde a las operaciones activas, cuyo objetivo es contrarrestar la acción del adversario. Por ejemplo, un ciberataque permite degradar el comando, control y comunicaciones; suprimir las defensas antiaéreas, degradar los sistemas de a

bordo de plataformas y el armamento inteligente; asimismo, puede ser utilizado para aumentar o para incrementar las posibilidades de éxito de un ataque cinético. (Owens, Dam & Lin, 2009).



II. CIBERAMENAZAS: UN PROBLEMA DEL ORDEN TRASNACIONAL

2.1. Medidas de contención para las ciberamenazas en la agenda internacional.

Como se expuso a lo largo del primer capítulo de la presente investigación las amenazas al ciberespacio representan un problema del orden transnacional ya que escapan a las capacidades estatales, haciéndose fundamental, la cooperación internacional en esta materia con miras a contener las actividades ilícitas que pueden derivar en la vulneración del ámbito virtual. Lo anterior, es más claro aún, si se parte de la premisa que en la actualidad el Sistema Internacional fundamenta sus relaciones de poder en el concepto de "interdependencia" planteado por Robert Keohane y Joseph Nye en su obra *Power and Interdependence*.

A partir de este término, Keohane y Nye fundamentan su crítica al Paradigma Realista de las Relaciones Internacionales estableciendo un verdadero reto teórico y pragmático a esta doctrina y a cada uno de sus postulados (Tabla 1). De este modo, para estos autores existe un tipo de interdependencia que es *compleja* y que se caracteriza por un mundo en el que *otros actores*, además de los Estados participan directamente en la política mundial, en la cual no existe una clara jerarquía de asuntos y en el que la fuerza sea un instrumento ineficaz de la política (Borja, 2005, p.127).

Tabla 1. Explicación del concepto de Interdependencia a la luz de los postulados de R. Keohane, J. Nye, R. Cox y A. Gramsci.

Interdependencia	
Ausencia del uso de la fuerza	Militar
Falta de jerarquía en la agenda	Las agendas incluyen temas de seguridad, económicos, sociales, políticos, culturales, ecológicos, migratorios, etc. Generalmente, ninguno domina las agendas permanentemente.
Agenda amplia	Indicativo de alta interdependencia
Múltiples canales de contacto entre las sociedades	A nivel gubernamental, institucional, entre ONG, nexos sociales, culturales, etc.
Contexto histórico	Determinante en la construcción de relaciones simétricas, asimétricas, etc.
Efectos recíprocos entre países o actores internacionales	Vulnerabilidades, sensibilidades
Ejercicio del poder ↓ Interdependencia ↓ Por consenso: hegemonía. Mecanismos →	Dimensión institucional, organización internacional: las instituciones encarnan reglas que facilitan la expansión hegemónica; producto del orden hegemónico; legitiman normas del orden mundial; cooptan élites en países periféricos; absorben ideas "contrahegemónicas." Las instituciones minimizan el uso de la fuerza.
Por coerción: Dependencia (interdependencia asimétrica o baja interdependencia) →	Influencia de poderes externos en un país, subordinación, vida económica subordinada, penetrada y entrelazada con otras naciones. El país más débil tiene menos autonomía.
Dominación (no hay interdependencia) →	Uso de la fuerza militar o económica. Ejercicio contundente del poder. Ejemplo reciente: Irak.
Tipos de interdependencia: Simétrica; compleja; asimétrica; bilateral; sensible; multilateral	Canadá-Estados Unidos: compleja (ausencia del uso de la fuerza; múltiples canales de contacto entre las sociedades; falta de jerarquía en los asuntos de la agenda bilateral). México-Estados Unidos: asimétrica (dependencia en áreas como la económica; vulnerabilidades recíprocas en narcotráfico, migración y **recursos de aguas transfronterizas**).

Fuente: http://catarina.udlap.mx/u_dl_a/tales/documentos/mes/rivera_l_mg/capitulo1.pdf

La respuesta del realismo no se haría esperar y en 1979 Kenneth Waltz publicó *Theory*

of International Politics, que posteriormente condujó al surgimiento del "neorrealismo" o "realismo estructural" de la Relaciones Internacionales. Asó, Keohane, en *Neorealism and its Critics*, dirigirió una fuerte crítica a los neorrealistas "por tener una visión unidimensional del poder (...). [Considerando] que el neorrealismo es incapaz de explicar fenómenos fundamentales; por ejemplo, que una *gran potencia* como Estados Unidos sea derrotada por un pequeño país como Vietnam, o que una organización como Al Qaeda sea capaz de realizar un ataque directo a la seguridad interna de los Estados Unidos" (Ortega 2007, p.560).

Como se expuso, la interdependencia compleja se caracteriza por la multiplicidad de canales que conectan a las sociedades desde las élites gubernamentales hasta las no gubernamentales, los bancos, las corporaciones, etc.; la ausencia de una jerarquía en la agenda interestatal, y el hecho que la fuerza militar no sea utilizada por los gobiernos para resolver problemas. De este modo, el concepto resulta de gran utilidad para analizar las relaciones de poder en un mundo cada vez más complejo y el cual, como lo explican los autores en cuestión, "está conformado por Estados soberanos que buscan maximizar sus intereses y poder" (Keohane & Nye, 1989, p.165).

Más allá de las críticas a la obra de Keohane y Nye, así como a los demás teóricos de la interdependencia compleja, lo cierto, en todo caso, es que la visión multidimensional del poder, totalmente desligada del dogma realista, resultaría ser un acierto de los institucionalistas liberales para la comprensión de fenómenos que con el pasar de los años comenzarían a tener lugar en el Sistema Internacional. Ejemplo de estos fenómenos es el surgimiento de los denominados "conflictos de cuarta generación", los cuales aparecieron en el plano internacional como una combinación de estrategias *no convencionales* de combate, y dentro de las que se

incluyen las amenazas cibernéticas.

A partir de lo anterior, la obra de Keohane y Nye sirve para caracterizar la imposibilidad de comprender el asunto del ciberespacio desde una óptica unidimensional que sólo deba abordarse desde una perspectiva de Defensa y Seguridad estatal, pues desde la argumentación de estos autores, el Estado es un actor más involucrado en la contención de las amenazas cibernéticas. Además, en un mundo globalizado, y por ende cada más interdependiente, resulta fundamental apelar a la teorización de Keohane y Nye para comprender la necesidad de defender el ciberespacio por medio de la sinergia de capacidades entre actores estatales y transnacionales. Los Estados deben por tanto concebir que en un mundo interconectado e interdependiente, una amenaza para uno de sus miembros representa un riesgo para los demás actores del Sistema Internacional y, por ende, la cooperación internacional resulta ser la alternativa de la solución más coherente para enfrentar las ciberamenazas.

Vale la pena mencionar, que a diferencia de otras dimensiones de la guerra, "el ciberespacio no es un ámbito análogo al de la tierra, mar, aire o estratósfera, no tiene distancias, posiciones ni territorios que puedan ocuparse; el ciberespacio no puede ser conquistado" (Borg, 2015, p.65), por lo cual más allá de identificar potenciales amenazas a este ámbito virtual y posibles magnitudes de estas, se debe considerar que el dominio cibernético trasnacional plantea nuevas preguntas sobre el sentido de la seguridad nacional. Algunas de las respuestas más importantes deben ser nacionales y unilaterales, con énfasis en la profilaxis, la redundancia y capacidad de recuperación. Sin embargo, es probable que los principales Gobiernos no tarden en descubrir que la inseguridad creada por los actores cibernéticos no estatales requerirá una cooperación más estrecha entre los países. (Nye, 2013)

Lo anterior, demuestra la importancia que tiene para el Sistema Internacional contener y confrontar la inseguridad cibernética por medio de alianzas estratégicas con actores que trasciendan las fronteras territoriales. En este punto, dicha situación se podría analizar a la luz de la conceptualización presentada hasta aquí sobre la interdependencia compleja, pues en el contexto mundial de las últimas décadas, con la aparición de este tipo de fenómenos, es cada vez más evidente cómo los Estados no son independientes unos de otros, sino interdependientes, lo que significa "situaciones caracterizadas por efectos recíprocos entre países o entre actores de diferentes países" (Keohane & Nye, 1989, p.8). Almagro (2016) lo plantea de la siguiente manera:

A pesar de los avances prometedores que hemos logrado hasta el momento, la necesidad de continuar con cooperación multilateral y la creación de capacidad sigue siendo igual de urgente. Las tecnologías de la información y las innumerables formas en que las utilizamos siguen evolucionando a un ritmo acelerado, al igual que las vulnerabilidades que traen consigo y los actores y las amenazas que buscan aprovecharse de estas. Solo trabajando juntos podemos seguir el ritmo y asegurar que los beneficios de este dominio digital nuevo y en expansión superen los riesgos y los costos. (p. XII)

Con base en lo argumentado dentro del presente contenido, vale la pena abordar algunos escenarios específicos de cooperación internacional, en materia de ciberdefensa y ciberseguridad, con miras a la consiga de un ciberespacio libre y seguro que garantice el Estado de Derecho, la democracia y los Derechos Humanos en el Sistema Internacional. Dichos escenarios serán desarrollados en el siguiente apartado y reforzarán el análisis proyectado hasta

aquí en torno a la necesaria consolidación de alianzas estratégicas entre actores estatales y transnacionales, en un mundo globalizado y cada vez más interdependiente, con miras a prevenir y combatir las amenazas cibernéticas.

2.2. Ciberseguridad: Estrategias para combatir las ciberamenazas.

Como se ha planteado a lo largo de la presente investigación, la globalización es un factor determinante en lo que respecta a los ciberdelitos, ya que la tecnología en un escenario globalizado que ha facilitado el accionar de la delincuencia organizada, generando un fenómeno transnacional que es cada vez más complejo de combatir para los Estados, dada la alta porosidad de sus fronteras y la existencia de actores con ánimo de un lucro proveniente de actividades ilegales. Por esta razón, los Estados ven en la necesidad de crear nuevas estrategias para combatir estas amenazas trasnacionales, implicando un abordaje multidimensional y multilateral que requiere de cooperación.

En consideración de lo anterior, se evidencia que las organizaciones internacionales han abordado y priorizado el tema de ciberseguridad, ello bajo la comprensión de que esta concierne a todos los Estados miembros, y que por tanto es necesario generar estrategias para combatir las ciberamenazas, ejemplo de esto se encuentran organizaciones como:

> (...) las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)

Como se mencionó anteriormente, la ciberseguridad escaló en la agenda desde los atentados del 11S, materializándose en principio en la firma del Convenio de Budapest el 23 de noviembre del 2001 siendo este promovido por el Consejo de Europa, y caracterizándose por ser "un acuerdo nacido con vocación universal y transatlántica, que supuso y es el máximo referente para la lucha contra la ciberdelincuencia, y sigue siendo el único tratado que tiene por objeto la armonización normativa del derecho penal de las naciones o estados que lo ratifican" (Hernandez, s.f, pág. 13).

En el caso de Estados Unidos se crea la Estrategia Nacional para asegurar el Ciberespacio, la cual fue promulgada en el año 2003 y se ratificó en el Plan Nacional de Protección de Infraestructuras en el 2006, esta estrategia prioriza 18 sectores que requieren planes de protección específicos de infraestructura. Posteriormente en el 2008 se crea la Iniciativa Integral de Ciberseguridad. Durante la administración de Barack Obama se realiza un estudio sobre los esfuerzos en Ciberseguridad y se presenta una visión sobre las principales recomendaciones para que el presidente consolide un plan de Ciberseguridad a nivel nacional (Maciel, Foditsch, Belli & Castellón, 2016).

Por lo anterior, este plan de Ciberseguridad replanteó la estructura de las instituciones encargadas de la seguridad del país inaugurando el Departamento Especializado en la Ciberguerra, así como el Cibermando de Estados Unidos en el 2009 (Clarke, 2011).

En este sentido, como lo argumenta Javier Candau (2011), Estados Unidos centra sus esfuerzos en 5 aspectos principales a saber: 1. Sistema de respuesta nacional de seguridad en el

ciberespacio. 2. Programa de reducción de amenazas y vulnerabilidades. 3. Formación y concienciación en el ciberespacio. 4. Asegurar el ciberespacio gubernamental. 5. Cooperación nacional e internacional.

Para el año 2013, en el marco de una de las organizaciones encargadas de la seguridad en el territorio europeo bajo una noción de cooperación policial como lo es EUROPOL se creó el Centro Europeo de la Lucha contra la Ciberdelincuencia o EC3, como estrategia para el tratamiento de ciberamenazas y ciberataques, creando dentro de esta misma organización el Centro de respuesta ante incidentes cibernéticos del ámbito europeo (CERT-EU). (Hernández, s.f)

En cuanto a la región de América Latina, se encuentra que el 70% de los países de la región cuentan con algún tipo de protección de datos en sus constituciones. Así mismo, países como Argentina, Colombia, Costa Rica, México, Perú y Uruguay han promulgado leyes de protección de datos. A pesar de esto "la retención de los datos obligatorios es una práctica cada vez más utilizada en la región y, en muchos casos, se pueden obtener datos almacenados sin una orden judicial" (Maciel, Foditsch, Belli & Castellon, 2016, pág. 9).

Ahora bien, pese a que en el marco de organizaciones internacionales, así como en escenarios de cooperación multilateral y bilateral entre los Estados se promulga por la creación de Ciberseguridad para combatir las amenazas en el ciberespacio la cooperación sigue siendo precaria, esto ante la dificultad derivada de cuestiones de orden legislativo, político e incluso cultural, las cuales derivan en situaciones de la incapacidad de confiar totalmente en otros Estados, así como en el temor de permitir que sus vulnerabilidades sean expuestas.

A pesar de esto, la mayoría de los casos de cooperación entre los Estados están en cabeza de organizaciones internacionales que se constituyen con diferentes objetivos tales como economía, el desarrollo, la seguridad, donde pese a los intereses particulares de cada organización, el tema de la ciberseguridad se prioriza ante la amenaza que representa para cada sector de interés a nivel internacional.

2.3. Agenda Internacional para asuntos de ciberdefensa y ciberseguridad.

Como se examinó en el anterior capítulo, la agenda internacional ha incluido dentro de sus prioridades la defensa del ciberespacio, ello bajo el supuesto de un Sistema Internacional cada vez más consciente de las amenazas cibernéticas que lo rodean. En este sentido, y como se analizó en el primer capítulo de la investigación, Colombia ha decidió alinear sus prioridades en materia de Defensa y Seguridad con esta agenda internacional, fortaleciendo la infraestructura institucional y normativa pertinente para enfrentar este serio desafío.

De igual forma, de acuerdo con el concepto de interdependencia compleja desarrollado por Keohane y Nye, quedó claro que la cooperación internacional es un factor fundamental para prevenir y combatir las amenazas cibernéticas en un mundo cada vez más interconectado. Por lo anterior, en este apartado, se analizará la participación de Colombia en el plano internacional en materia de ciberdefensa y ciberseguridad.

Se podría decir que en los últimos años Colombia ha adelantado esfuerzos en materia de cooperación internacional con países como Estonia, España, Estados Unidos, Israel, Brasil,

Chile, México, Corea del Sur. En el caso particular de asistencia bilateral con Corea del Sur, Colombia firmó un acuerdo de transferencia de conocimiento en Tecnologías de Información y Comunicación en temáticas como ciberseguridad, seguridad de la información y gobierno electrónico (Anderson, 2015).

De igual manera, se destacan algunos acercamientos con diversos organismos internacionales como: Naciones Unidas (ONU), OTAN, Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), Foro Económico Mundial (OECD) e Interpol. "Dentro de los logros de política internacional más destacables, Colombia fue invitada por el Consejo de Europa en el año 2011 a adherirse a la Convención sobre Delito Cibernético, conocido también como *Convenio de Budapest*, lo que le convierte en una de las pocas excepciones de países no miembros en formar parte de esta herramienta de política internacional (i.e. Estados Unidos, Japón, Canadá y República Dominicana)" (Sánchez & Jones, 2016, p.87).

Adicionalmente, y como se destaca en el CONPES 3854 de 2016

> el país ha suscrito acuerdos con organizaciones internacionales como el *Antiphishing Working Group* (...) con el fin de acceder a recursos y programas específicos en ciberseguridad y ciberdefensa, y hacer parte de esta coalición con empresas de la industria, autoridades legales y entidades de gobierno, que colaboran en función de contar con mejores mecanismos de alarma y respuesta frente a ataques cibernéticos. Estas alianzas también se han fortalecido en el contexto local con actores de la industria nacional (págs. 15-16)

Por otra parte, vale la pena resaltar que el COLCERT se vinculó en noviembre de 2013 al *Forum of Incident Response and Security Teams* (*FIRST*), importante espacio para el intercambio de información y cooperación en asuntos de interés común frente a la seguridad cibernética (Forum, 2015). De igual manera, y tras haberse analizado a lo largo de la presente investigación que la defensa del ciberespacio no debe entenderse como un fenómeno que se deba enfrentar de manera unidemensional, pues en un Sistema Internacional interdependiente deben intervenir más actores aparte de los Estados, Colombia también ha adelantado acercamientos con firmas multinacionales. En este sentido se destaca el caso de *Microsoft*, con la cual se firmó un memorando de entendimiento para programas como: Cybercrime Center, Cyber Threat Intelligence Program (CTIP), Security Cooperation Program (SCP) (Colombia, 2013).

Por otro lado, el país se ha posicionado a nivel regional con un liderazgo notable en temas de ciberdefensa y ciberseguridad, ostentando una posición ventajosa respecto al promedio mundial y de las Américas, ejemoplo de ello, algunos indicadores de eficiencia comparativa como el *Global Cibersecurity Index* de la Unión Internacional de Telecomunicaciones (UIT). Según éste, en 2014 el país se ubicaba en el quinto lugar del ranking a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay; mientras que en el plano mundial comparte la novena posición, junto a países como Dinamarca, Egipto, Francia y España (Consejo, 2016). Vale la pena mencionar, que este Índice se calcula con base en cinco variables: legislación, cooperación, construcción de capacidades, organización, y conocimiento técnico.

Cabe señalar que debido a los avances generados a partir de la implementación del

CONPES 3701, Colombia ganó la confianza del Sistema Internacional en materia cibernética, al ser un Estado que aprendió a implementar "buenas prácticas" en su defensa al ciberespacio y en un período de tiempo muy corto se consiguieron grandes resultados. Sin embargo, más allá de los avances significativos en materia de ciberdefensa y ciberseguridad, los logros de Colombia siguen siendo insuficientes para cerrar la brecha existente entre capacidades y el contexto estratégico cibernético, y de allí que el país haya desarrollado y aprobado el CONPES 3854. Como ya se explicó en el capítulo anterior, este nuevo documento trae una serie de novedades, alineando los retos nacionales sobre el ciberespacio con las recomendaciones de organismos internacionales como la OECD.

A propósito de la consolidación de las relaciones de Colombia con el resto del mundo en materia de cooperación en temas de ciberdefensa y ciberseguridad, se debe decir que la OECD ofrece un foro donde los gobiernos de los países miembros trabajan conjuntamente para la solución de problemas comunes que afectan el bienestar económico y social de las personas (Organization, 2015). En la actualidad, Colombia se encuentra en proceso de adhesión a esta organización, para lo cual viene consolidando esfuerzos para ajustarse a los derroteros que ha sugerido, haciéndose énfasis en la gestión del riesgo, y vinculando elementos socioeconómicos en la planificación de la Defensa y Seguridad del Estado.

Finalmente, en materia de cooperación nacional, vale la pena agregar que el CCOC viene adelantando el proceso de elaboración del catálogo de infraestructuras críticas cibernéticas nacionales en el país. "El catálogo en mención permitirá, a futuro, coordinar y gestionar los planes y programas de protección y defensa a infraestructuras críticas cibernéticas nacionales" (Consejo, 2016, p.16). Lo anterior, también posibilita identificar la sinergia de

esfuerzos a nivel nacional para combatir las ciberamenazas.

Para finalizar, se debe establecer que la búsqueda de logros contundentes en materia de ciberdefensa y ciberseguridad, la implementación del CONPES 3854 es fundamental en la actual coyuntura nacional, en la cual toda la institucionalidad centra sus esfuerzos en la construcción de una paz estable y duradera tras el fin del conflicto con la guerrilla de las FARC. Dentro de este nuevo contexto estratégico, se visualiza un aumento de las nuevas amenazas y una mutación de las antiguas; principalmente, la criminalización de las disidencias del grupo insurgente FARC, por ejemplo, las *bandas criminales* (*Bacrim*) (Sánchez & Jones, 2016, p.91). Considerar que las Bacrim son ajenas a las Tecnologías de la Información y Comunicación para el desarrollo de actividades ilícitas es ingenuo, estas les usan en detrimento de la confianza de los usuarios del ambiente digital (Chambers; Etges; Sutcliffe, 2008).

En este orden de ideas, se hace esencial el mantenimiento de alianzas estratégicas con actores transnacionales, así como la búsqueda de nuevos aliados, pues, entre todas las razones expuestas en la presente investigación, la ciberdefensa y la ciberseguridad se vuelven elementos indispensables para fortalecer el escenario propicio que garantice la transición de Colombia hacia la paz.

III. LA COOPERACIÓN DIPLOMÁTICA COMO COROLARIO EN LA GESTIÓN DE LAS CIBERAMENAZAS

3.1 Nuevas perspectivas frente a la lógica diplomática en relación con la ciberseguridad.

Como se estableció en los anteriores capítulos, la revolución de la información ha generado grandes cambios en las interacciones sociales, así mismo, esta ha trasformado la forma tradicional de concebir el Estado y el Sistema Internacional, pues a partir de este fenómeno conceptos como la soberanía y la gestión pública han tomado un nuevo rumbo ante la incidencia de diferentes actores y medios que intervienen.

En este orden de ideas, la revolución de la información también ha impactado ámbitos como la diplomacia, la cual desde una perspectiva tradicional aboga por la búsqueda de un relacionamiento optimo entre los Estados, no obstante, dicha comprensión se transforma en el Sistema Internacional actual, en el cual se reconoce la importante incidencia de nuevos actores no estatales, la facilidad de las comunicaciones y la porosidad de las fronteras estatales (Rubio, 2011).

Por lo anterior, el desarrollo de diferentes estrategias desde la ciberdiplomacia o la diplomacia digital también hacen parte de las dinámicas y estrategias de los Estados en el Sistema Internacional, entiendo ello como como mecanismo de posicionamiento ante una época de revolución informática donde:

> La difusión de la información significará que el poder estará más

> distribuido y las redes extraoficiales disminuirán el monopolio de la burocracia tradicional. Los gobiernos tendrán un menor control de sus estrategias, también de las de comunicación. Tendrán un menor grado de libertad al tener que responder de los hechos y tendrán que compartir escenario con más actores. Aumentarán las sociedades público-privadas y la 'privatización' de funciones (Nye, 2003, pág.85).

Este tipo de cambios, generaron además que se buscaran formas nuevas de cooperación internacional, así, la política exterior de los Estados se ha redefinido y se ha instrumentalizado en las relaciones diplomáticas desde un enfoque digital.

En este sentido a partir de los postulados de Nye (2003), en el ámbito de la diplomacia se reconocen acciones propias del softpower (poder blando) del Estado, el cual, se entiende "como un concepto intangible, vinculado a la imagen del país, formada por la ideología, la percepción internacional de su estabilidad institucional, su imagen acogedora, rentable para invertir, culturalmente interesante, turísticamente atractivo, tecnológicamente avanzado, etc" (Rubio, 2011, pág. 30).

Así, en lo que respecta a la utilización del ciberespacio, aparece en el fin de la Guerra Fría el concepto de Netpolitik como un nuevo estilo de diplomacia que buscaba utilizar las capacidades generadas por la invención del Internet, siendo un mecanismo para que los Estados presenten su organización política, cultural, identidad, valores, etc. En síntesis, la Netpolitik suponía la utilización del poder blando con el fin de lograr proyección estatal, siendo el Internet la herramienta por excelencia sobre la cual se cimienta su gestión (Terrés, 2011).

Ahora bien, a pesar que estos cambios se consideraban un desarrollo positivo para las interacciones sociales y la gestión estatal, la utilización masiva del Internet también generaría nuevas amenazas para las personas y los Estados ante la falta de privacidad, el flujo de información, la transmisión en tiempo real y la facilidad en cuanto a la accesibilidad, de grupos terroristas, grupos o personas dedicadas a perpetrar acciones delincuenciales (Bollier, 2003).

Por lo anterior, ante la multiplicidad de actores, las nuevas amenazas creadas por la utilización del ciberespacio y la vulnerabilidad creciente en el Sistema Internacional, los Estados empiezan a entender la importancia de la cooperación internacional entre actores estatales como no estatales, que cumplan con ciertos parámetros de compatibilidad con las ideologías política, económicas y sociales, para la creación de estrategias mancomunadas en contra de las ciberamenzas (Fisher, 2009).

En este orden de ideas, la lógica tradicional del manejo de la información de los Estados también cambia ante la aparición del ciberespacio y las ciberamenzas. En este sentido, los Estados al ver la necesidad de cooperar deben renunciar en cierta medida a lo que por excelencia han cuidado desde su creación, parte de su soberanía., pues la cooperación implica que los Estados deben compartir temas como la información, los recursos, el conocimiento, por lo tanto, descubren que para poder desempeñar un papel trascendental en el Sistema Internacional "tienen que prescindir de las barreras que impedían el intercambio de información, renunciando a la trampa tradicional de mantener la información oculta en una caja fuerte, algo que en la nueva situación resulta suicida" (Rubio, 2011, pág.36).

En este orden de ideas, la cooperación internacional en temas de ciberseguridad cada vez cobra mayor sentido, en la medida que proporcionalmente aumentan las ciberamenazas. De esta manera, la ciberdiplomacia se convierte en la herramienta para crear dicha cooperación internacional, propendiendo por el mantenimiento de un ciberespacio seguro, ya que como lo afirma Terrés (2011) al entender que:

> El libre flujo de información multimediática continuará acelerándose, abriéndose paso y evolucionando. Ningún actor tiene ya el monopolio de la generación y transmisión de datos, imágenes, video y audio. Las nuevas herramientas han abierto a todos los sectores la posibilidad de ser fuente y destino de información(pag.26)

Bajo la comprensión de la existencia continua de amenazas (estado latente) y la incapacidad de acabar con estas de manera inmediata, la ciberdiplomacia se presenta como una posible la respuesta de los Estados para combatir las ciberamenzas, generando una cooperación internacional que permita reducir los riesgos a los que se enfrentan ante las herramientas tecnológicas creadas por la globalización.

En este contexto, la ciberdiplomacia se materializa en la media que las cancillerías ya no solo se relacionan con sus interlocutores tradicionales, sino además reconoce la multiplicidad de actores que inciden en la seguridad del ciberespacio (Lichtenstein, 2010).

Así mismo, la ciberdiplomacia se caracteriza por ser en la práctica una herramienta

esencial para las cancillerías que busquen enfrentar los retos del siglo XXI "los diplomáticos están obligados a adoptar estas herramientas para hacer mejor su trabajo, para llegar a más gente, para obtener más y mejor información y, sobre todo, para dialogar e interactuar con nuevos públicos" (Terrés, 2011, pag.126).

Lo anterior, permitirá entender a cabalidad el funcionamiento, las nuevas invenciones, las tendencias de todos los actores del Sistema Internacional, generando un sistema de información que permita a los Estados estar mejor preparados ante nuevas amenazas, así como combatir las ya existentes a partir de la cooperación internacional de diferentes actores que compartan sus mismos intereses. En resumen, la ciberdiplomacia se constituye en el siglo XXI como la herramienta para combatir las amenazas generadas por la globalización, entendiendo que, ante el ambiente coyuntural, la diplomacia tradicional es obsoleta ante la nueva lógica de las relaciones sociales y estatales. Por esta razón, es importante entender que a pesar que ha sido una transformación lenta y compleja para los Estados, durante los últimos años se han creado diferentes estrategias desde este margen que permiten observar el cambio de la lógica tradicional, ejemplo de esto se encuentra con la Unión Europea y los diferentes esfuerzos por consolidar alianzas en temas de ciberdiplomacia, ciberseguridad y ciberdefensa.

3.2 La experiencia europea frente a la ciberdiplomacia

La Unión Europea se ha caracterizado durante los últimos años por ser un ejemplo de cooperación internacional en temas de ciberseguridad y ciberdefensa, así mismo, desde su lógica de cooperación estatal se han creado una serie de estrategias que buscan consolidar una

política de seguridad digital no solo dentro del territorio europeo, sino además influir a nivel internacional, siendo uno de los bloques con mayores estudios y alianzas en pro de la ciberseguridad y la ciberdefensa, constituyéndose como uno de los pioneros en lo que respecta a la ciberdiplomacia.

En este sentido, es importante caracterizar algunas de las ultimas estrategias que han significado el posicionamiento en ciberdiplomacia del bloque europeo, siendo ejemplo de ello la presentación de la nueva estrategia de seguridad (junio 2016) denominada "visión compartida, acción común: Una Europa más fuerte". En esta estrategia se describe el conjunto de acciones articuladas y sinérgicas que deben efectuar los Estados europeos con el fin de brindar una solución efectiva a las amenazas comunes de seguridad (Izquierdo, 2016).

Como consecuencia de lo anterior, se plantea un escenario de acción conjunta, en el cual cada uno de los Estados miembros debe ser protagonista en el fomento de la cooperación y de la ejecución de una política exterior en red. En este sentido, y teniendo en cuenta la multiplicidad de actores europeos se hizo necesario implementar un modelo diplomático que contribuyera a promover un orden europeo multilateral capaz de garantizar la seguridad de los ciudadanos y orientar el avance hacia una mayor integración en seguridad y defensa.

En relación con lo anterior, y teniendo en cuenta que la Unión Europea debe abordar asuntos de seguridad de forma transversal mediante una política internacional coherente, ha cobrado gran importancia el diseño de una política, -entre otras- frente a: i) la ciberseguridad, ii) la promoción y protección de derechos en el ciberespacio, iii) la economía digital, iv) el desarrollo de cibercapacidad, y v) la ciberdelincuencia – entre otros –

En este sentido, Federica Mogherini (2016), en prólogo de "hacia una estrategia global de la UE" indicó:

> Participaremos en acciones de ciberdiplomacia y de capacitación con nuestros socios y trataremos de celebrar acuerdos de comportamiento responsable en el ciberespacio basados en el Derecho internacional existente. Apoyaremos la gobernanza digital multilateral y un marco de cooperación mundial en materia de ciberseguridad, respetando la libre circulación de la información. En el ámbito espacial, promoveremos la autonomía y la seguridad de nuestros servicios espaciales y trabajaremos en la formulación de principios de comportamiento espacial responsable, que podría dar lugar a la adopción de un código de conducta internacional de carácter voluntario (pág.33-34).

Por tanto, en el escenario europeo se ha acelerado la reflexión sobre nuevas prácticas de diplomacia y se ha reconocido la necesidad de establecer un enfoque global en lucha contra el terrorismo que instrumentaliza las tecnologías de la información. De esta forma el 11 de febrero de 2015 el Consejo de la Unión Europea, a través del documento denominado "Conclusiones del consejo sobre la ciberdiplomacia", invitó a los estados miembros a "abordar estas cuestiones transversales y polifacéticas mediante una política internacional coherente para el ciberespacio que promueva los intereses políticos, económicos y estratégicos de la UE, y deben asimismo seguir colaborando con los socios y organizaciones internacionales clave, así como con la sociedad civil y el sector privado" (Secretaria General

del Consejo, 2015).

Esta realidad del sistema digital global ha implicado el surgimiento de una nueva agenda de seguridad europea que demanda soluciones articuladas que precisan la negociación y creación de vínculos entre diversos actores para promover acciones efectivas que permitan prevenir, investigar y sancionar punitivamente cualquier ciberataque. Esto implica una estrategia ciberdiplomática robusta que cree un entorno político favorable para expedir leyes y movilizar la estructura administrativa para luchar eficazmente contra estos delitos facilitando su detección, investigación y sanción.

Al respecto, el convenio sobre la Ciberdelincuencia de Budapest del año 2001 fue el primer tratado sobre delitos informáticos que tuvo como objetivo aplicar una política penal común encaminada a salvaguardar los bienes jurídicos penales vulnerados por medio del cibercrimen. Los principales objetivos del tratado fueron: i) armonizar las legislaciones penales, y ii) el establecimiento de un esquema de cooperación internacional eficaz en la investigación y persecución (Jefatura del Estado, 2010).

En consecuencia, es claro que la Unión Europea ha liderado en el contexto internacional la reflexión sobre los nuevos modelos de ciberdiplomacia y ha contribuido en la reestructuración legislativa y administrativa de sus estados. Este desarrollo refleja un esfuerzo articulado respecto de las urgencias del mundo digital y contribuye a reafirmar la idea de que es preciso implementar una "gestión coordinada no sólo en el campo de lo real, sino también en el de lo virtual. Es decir, es necesaria una gestión de la reputación, de información, de transparencia y de cercanía al ciudadano y a los demás actores de las relaciones

internacionales" (Rodríguez, 2015, pág. 933).

En este contexto, el avance de las tecnologías de la información y la complejidad técnica a través de la cual los ciberdelincuentes ponen en riesgo los derechos humanos de los asociados ha obligado a los estados a cambiar la forma de relacionarse entre ellos. Es necesario contar con espacios de discusión y articulación permanentes que protejan los intereses legítimos en la utilización y en el desarrollo de las nuevas tecnologías.

Por tanto, podemos concluir que, en este nuevo contexto diplomático de la Unión Europea, se afrontan de manera articulada los riesgos inherentes a la multiplicidad de herramientas virtuales que ponen en riesgo la seguridad de los estados y los derechos subjetivos de los asociados.

> La irrupción de nuevos actores afecta también a las relaciones internacionales y a la forma en que los estados se enfrentan a ellos a través de su labor diplomática. Cambian las funciones y cambian los actores, que se amplían más allá de la frontera de lo estatal y cambian sobre todo las formas de ejercer esas funciones y las herramientas con las que se cuenta para ello. (Rubio, 2011, pág. 54)

En este sentido puede establecerse que la Unión Europea ha buscado generar una serie de mecanismos enfocados en la ciberdiplomacia, reconociendo una multiplicidad de actores en el Sistema Internacional, aquellos que buscan cooperar y aquellos que son una amenaza directa, estableciendo alianzas con otros Estados y recalcando la importancia en la actualidad de

estudios en tema de ciberseguridad y la ciberdefensa para adelantarse a cualquier ciberamenazas, generando un enfoque desde la prevención de riesgos informáticos.

3.3 Transformaciones pendientes para Colombia en la gestión de las ciberamenazas.

Como se ha desarrollado a lo largo de este trabajo, la materialización de los aspectos teóricos y conceptuales se ven reflejados en las estrategias de políticas públicas en materia de ciberdefensa y ciberseguridad al interior de cada Estado. Sin embargo, es importante recalcar que para combatir las ciberamenazas en la actualidad la cooperación internacional se convierte en la visión multidimensional del fenómeno y por lo tanto es esencial para cumplir los objetivos.

En este orden de ideas, específicamente para el caso colombiano se encuentran una serie de esfuerzos que como se describieron en el primer capítulo han buscado mitigar las amenazas ya existentes, así como adelantarse a las venideras. Este tipo de esfuerzos han sido influenciados por diferentes normativas internacionales donde Colombia ha ratificado su interés por unir esfuerzos para combatir las ciberamenazas.

En este sentido, dentro de los esfuerzos vigentes en estos temas en Colombia se encuentra el Conpes 3854 (2016), el cual describe los diferentes instrumentos utilizados en el país para crear una política nacional de seguridad digital:

- En primer lugar, se referencia el Convenio sobre Cibercriminalidad de Budapest mediante la cual se enmarca la importancia de crear una legislación

robusta que permita la prevención de conductas delictivas, así como la necesidad de un sistema penal fuerte que permita detectar, investigar y sancionar los delitos cibernéticos a cabalidad.

- En segunda instancia, se tiene en cuenta la Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la OEA donde se recalca la importancia de analizar y materializar la seguridad cibernética de manera multidimensional y multidisciplinaria.
- En tercer lugar, se encuentra la Decisión 587 de la Comunidad Andina en la cual se establecen los parámetros para la creación de la Política de Seguridad Externa Común Andina.
- Así mismo, en lo que compete a la ciberdefensa se tiene como referencia la Declaración de la Cumbre de Gales de la OTAN en 2014, donde se abordan temas de ciberseguridad y se establecen alianzas entre los países miembros
- De igual manera, se destaca la Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes de la OEA en el 2015, donde se desarrolla un proyecto de asistencia técnica a los Estados americanos miembros, para la elaboración de un listado de infraestructura critica, clasificando activos, redes, sistemas y funciones, buscando evaluar las diferentes vulnerabilidades, riesgos, amenazas e interdependencias.

En este orden ideas, bajo estos parámetros internacionales, la política de seguridad cibernética en Colombia tiende a ser insuficiente en la medida que a pesar que busca abordar el tema desde el enfoque jurídico, técnico, penal, etc, su materialización no se basa en un enfoque multidimensional y multidisciplinario en realidad, ya que, a pesar de ser abordado

desde los temas de la Defensa y Seguridad Nacional, no se concibe desde un enfoque preventivo de análisis de riesgos, donde más sectores que comparten intereses estén involucrados en la consecución de objetivos, distinguiendo así los objetivos económicos, sociales de ciberseguridad y ciberdefensa.

Muestra de lo anterior, se plasma en los organismos encargados de estos temas, actualmente "el colCERT es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, el cual presta su apoyo y colaboración a las instancias nacionales tales como el CCP y el CCOC" (Conpes 3854, 2016, pág. 33). Este grupo coordina las acciones necesarias para la protección de la infraestructura critica del Estado frente a posibles riesgos de ciberseguridad que afecten directamente la Seguridad y Defensa Nacional. Sin embargo, no existe un trabajo interdisciplinario o interinstitucional a nivel nacional que permita establecer una visión global de la ciberseguridad (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015).

En este sentido, como lo establece un estudio realizada por la OEA en el 2014, al ser Colombia un país con un entorno digital cada vez más activo, el enfoque manejado durante los últimos años de seguridad digital que no se basa en la gestión de riesgos, de carácter preventivo y no reactivo, así como el no involucramiento de diferentes instituciones interesadas en el tema, será cada vez más insostenible y costosa la gestión en este tema.

De esta manera, puede establecerse que la creación de una cultura de seguridad digital se convierte en algo fundamental, en la medida que las amenazas y la incertidumbre digital afecta diferentes sectores y agentes, por lo que sus consecuencias pueden desencadenar una

desestabilización estatal o afectaciones económicas y sociales sin precedentes (Azócar & Lavín, 2017).

Por lo tanto, como lo establece la OCDE (2015) el entendimiento de los riesgos en materia de seguridad digital debe ser formulado en términos económicos y sociales como, por ejemplo: pérdidas financieras, pérdidas en competitividad, pérdidas de oportunidad, daños a la reputación, a la imagen o a la confianza; y debe ser gestionado debidamente por todos los interesados o posibles afectados.

En este orden ideas, el Estado colombiano al desarrollar su política de seguridad digital o ciberseguridad de manera sectorial, pues en la actualidad se reconoce una dificultad para vincular diferentes actores y por lo tanto no existe un enfoque multidimensional y multidisciplinario.

En este orden de ideas, el ejercicio de la ciberdiplomacia en Colombia se muestra de manera precaria, ya que, si bien existe influencia de diferentes actores internacionales en lo que respecta a la creación de políticas de ciberseguridad y ciberdefensa, no se generan alianzas de cooperación internacional que permitan mitigar efectivamente las ciberamenazas, abordándose el tema como una cuestión de orden interno, lo cual imposibilita la cooperación con otros Estados o actores internacionales interesados en el tema.

Por lo anterior, puede establecerse que en temas de diplomacia Colombia sigue enfocada en la diplomacia tradicional, en la medida que concibe la cooperación internacional como un riesgo en si mismo para su Defensa y Seguridad Nacional, pues hasta el momento no

se han creado alianzas robustas que permitan encontrar la voluntad política y en el caso internacional diplomática en lo que respecta a la ciberseguridad y ciberdefensa regional e internacional.

Finalmente, también se encuentra que la mayor debilidad en combatir el fenómeno de las ciberamenzas en Colombia tiene que ver con que las estrategias se han desarrollado desde la ofensiva y no desde la prevención, lo que muestra la deficiencia en adelantarse al fenómeno, en gran medida a causa de la utilización de un enfoque tanto interno como externo de la política tradicional que no prever las amenazas.

Según el coronel Alberto González en la revista SISTEMA "para el Ejército de Colombia el ciberespacio juega un papel muy importante dentro del desarrollo de las operaciones militares. Quien maneje el ciberespacio y tenga el dominio de la información y de ese escenario lleva la delantera respecto a las intenciones de los enemigos del Estado" (edición 130).

La importancia que toman las amenazas cibernéticas cada día es mayor, sobre todo las que están dirigidas contra el Ejército Nacional. Por esto la implementación de un plan que contemple la creación de una unidad de ciberdefensa cobra mayor valor ante los posibles sucesos que se puedan presentar en el ciberespacio.

En el componente de ciberdefensa y ciberseguridad, debe ser primordial para el manejo de todo el ciberespacio por parte del Ejercito Nacional. Negarle la importancia que se merece puede conllevar a obtener fracasos y poner en riesgo no solo la seguridad del

Ejercito sino también la de todo el Estado.

Con todo esto se denota la importancia que genera garantizar la defensa del dominio cibernético dentro de la institución ofreciendo al mando herramientas interactivas; mediante el uso adecuado de la tecnología de punta obteniendo como resultado un completo panorama del desarrollo de la guerra en un teatro de operaciones cibernético; acorde a la normatividad de seguridad en comunicaciones y ciberdefensa.

Una vez que el ciberespacio sea tomado como un dominio esto implica tener una doctrina bien definida con normas tanto nacionales como internacionales para poder realizar operaciones. Con la experiencia de las operaciones irregulares donde un juez o un fiscal pueden controvertir nuestras actuaciones en operaciones y convertirnos de héroes a tiranos, se debe ajustar muy bien la reglamentación con las normas vigentes logrando tener una doctrina bien sustentada.

Conocer las amenazas al ciberespacio es una estrategia fundamental a pesar de que muchos de los individuos que realizan ataques son difíciles de detectar y capturar, esto implica tener una evaluación equilibrada de la amenaza según la revista de la OTAN, nuevas amenazas al ciberespacio dicen que se deben tener en cuenta dos aspectos:

Hasta ahora, los estados siguen siendo los actores más peligrosos en el ciberespacio. A pesar de la creciente disponibilidad de capacidades ofensivas por parte de redes criminales que podrían ser utilizadas en el futuro por actores no estatales como los grupos terroristas, lo cierto es que el espionaje y sabotaje digitales de alto nivel aún necesitan las capacidades, resolución

y análisis de la relación coste-beneficio de un estado.

Aún no ha habido un acto de ciberterrorismo con daños físicos y efectos materiales, pero la tecnología de los ciberataques está evolucionando claramente desde una simple molestia a una amenaza seria contra la seguridad de la información e incluso contra infraestructuras nacionales esenciales, (edición digital).

La consecución de material, equipo tecnológico de punta, capacitación de personal e instalaciones, sugiere para el Ejército Nacional destinar un presupuesto para la adquisición de dicho material, como no se puede escatimar esfuerzos ni recurso para este fin. Esto implica la planeación, la organización y la ejecución de un plan bien detallado que contemple costos y beneficios de todo lo que se piense adquirir, para que pueda ser aprobado por el Comando General.

Colombia a pesar de todos sus esfuerzos por proteger el ciberespacio está muy lejoseste fin. Por esta razón para cumplir con la tercera estrategia implica mejorar las relaciones con los ejércitos más desarrollados como el de Estados Unidos, tener comunicación constante con el personal encargado de ciberdefensa y ciberseguridad de este país, también implica realizar acercamientos con las grandes empresas proveedoras de tecnología, buscando tanto apoyo tecnológico como apoyo en desarrollo de proyectos tecnológicos propios.

La tercera estrategia es muy importante ya que en ella se estipula la capacitación, los convenios, las alianzas con otros países que nos generen nuevos conocimientos, experiencias.

Esto implica también tener un archivo donde se lleve los registros de actividades del ciberespacio con el fin de retroalimentarse y buscar soluciones a futuras acciones.

La organización y puesta en marcha de la brigada de ciberdefensa del Ejército es de vital importancia ya que es el paso inicial para fortalecer la ciberdefensa y ciberseguridad tanto en el Ejército como en todas las instituciones, que una vez terminada y organizada la pueden tomar como ejemplo, para su desarrollo en cada institución y de esta forma trabajar en una sola dirección, para la protección de todo el ciberespacio de Colombia, mejorando en 100% las fortalezas actuales y tratando de corregir las debilidades que se tienen en este campo.

La puesta en marcha de este ambicioso proyecto implica la participación activa del personal que integran tanto el arma de comunicaciones como el personal del arma de inteligencia, deben dejar de lado los celos de trabajo para poder formar un equipo, que generé resultados y que brinde la seguridad necesaria a todo el ciberespacio del Ejercito Nacional.

Una implicación que tiene que surgir de este proyecto es la concientización de acuerdo a la Escuela de altos Estudios en su monografía 137 nos dice:

aspectos de los sistemas informáticos y de las comunicaciones, empezando por el eslabón débil en todos ellos: el ser humano que los construye los mantiene y los usa (p,15)

Todos los integrantes del Ejército, desde el soldado regular pasando por el personal civil hasta llegar a los generales deben ser conscientes de las amenazas que se pueden presentar en el ciberespacio, en este momento la seguridad y defensa es un tema que solo lo

conocen en comando Ejercito, pero es ajeno para las unidades de provincia, la implicación más importante es que todos y cada uno de los miembros de la Fuerza conozcan las amenazas que acechan en el ciberespacio, como también las formas de prevenir un posible ataque.

CONCLUSIONES

La comprensión de la Seguridad Nacional en el actual escenario internacional pasa por reconocer la ampliación y profundización del concepto de seguridad, lo cual implica el reconocimiento tanto de nuevos temas que se vinculan en la agenda de seguridad como de nuevos actores que intervienen e impactan directamente en ella. En este sentido, el ciberespacio constituye aquel espacio por excelencia en el que se materializa la ampliación y profundización del concepto de seguridad, así como las dinámicas de un Sistema Internacional altamente interdependiente, de cuya articulación surge la posibilidad de construir entornos libres de amenazas o con posibilidades de mitigación efectiva.

En concordancia con lo anterior, la importancia de reconocer el ciberespacio como un bien público mundial, en el cual convergen multiplicidad de actores y fenómenos, haciendo necesario propulsar medidas tendientes a garantizar su seguridad, entendiéndole como un elemento central en la Defensa y Seguridad tanto de los Estados como del Sistema Internacional, pues su desatención puede derivar en la materialización de riesgos y amenazas para diferentes actores.

En este punto, es importante mencionar que la consolidación de un ciberespacio seguro requiere sinergia de esfuerzos entre diferentes actores estatales y transnacionales con miras a prevenir y combatir las diversas amenazas que se pueden llegar a gestar en este ámbito virtual. Por tanto, es prioritario el desarrollo de escenarios de cooperación que ralenticen y/o contengan los efectos devastadores que suponen un ciberespacio sin control. En este punto, se

debe clarificar que las amenazas trascienden a los Estados, toda vez que estas pueden repercutir en términos sociales, políticos, económicos, entre otros.

Por tanto, uno de los principales supuestos de la presente investigación refiere a la comprensión del ciberespacio como un escenario multidimensional, en el cual no es sólo la seguridad de los Estados es la que se puede ver vulnerada en términos tradicionales, sino que, por el contrario, es la seguridad de éstos y de diferentes actores como la población civil, empresas, organizaciones internacionales, entre otros la que puede verse allí vulnerada, para lo cual es imprescindible el reconocimiento a las manifestaciones no ortodoxas que puedan representar riesgos o amenazas y en consecuencia la necesidad entorno a encontrar mecanismos de mitigación eficiente en relación con la construcción de capacidades por parte de los Estados.

En consecuencia, y como segundo hallazgo de la investigación se destaca la construcción de un ciberespacio seguro desde diversos ámbitos y a partir de una asociación de esfuerzos entre actores estatales y no estatales, ello con el fin de con el fin de proteger la vida de las personas, la integridad, la estabilidad, el *statu quo* y funcionamiento de los Estados, así como su estabilidad económica. En este sentido, un ciberespacio seguro supone acciones no sólo de orden ofensivo, sino defensivo, lo cual requiere de la construcción e implementación de buenas prácticas tanto en la esfera domestica como internacional.

Llegados a este punto, la ciberdiplomacia constituye una herramienta para combatir las amenazas generadas por la globalización, así como aquellas propias del ciberespacio, entendiendo que en las actuales dinámicas del Sistema Internacional, la efectividad de la diplomacia tradicional es cada vez más reducida. Si bien, como se expuso en el tercer capítulo del presente trabajo, la Unión Europea ha avanzado significativamente ejerciendo como líder en

escenarios de cooperación en temas de ciberseguridad y ciberdefensa (ciberdiplomacia), el caso colombiano dista parcialmente de dicha realidad.

Y es justamente en este punto en donde se ubica uno de los principales retos de evidencia una dificultad al momento de materializar esfuerzos de cooperación internacional en el marco de la ciberdiplomacia. En este sentido, es prioritario que en principio se trabaje en pro de la creación e implementación de una cultura de ciberseguridad, la cual termine por insertase tanto en la institucionalidad domestica como en términos de política exterior.

Para esto último, y bajo la comprensión de la ciberseguridad y de la ciberdiplomacia como un asunto intermestico, se propone la creación de un Comité Intersectorial, en cual incluso puedan converger actores privados que participen o se vean impactados por los asuntos de seguridad librados en el denominado quinto dominio. Lo anterior, si bien es tan sólo una acción puntual, si supone el reconocimiento y comprensión del ciberespacio y de la ciberseguridad como un asunto multidimensional que requiere un abordaje multilateral (tanto desde diferentes ámbitos como de diferentes actores). En seguimiento de lo anterior, la ciberdiplomacia se entiende como una estrategia defensiva, que busca anticiparse a ataque alguno, protegiendo así, entre otros la infraestructura critica de los actores.

Ahora bien, en atención al actual contexto regional en cual se encuentra insertado América Latina, Colombia debe promulgar por escenarios de cooperación e intercambio constante con Fuerzas e Instituciones de otros países, ello con el fin de adquirir experiencia y evitar que los lazos de cooperación queden reducidos a situaciones críticas. Es igualmente importante, que la estrategia de ciberdiplomacia colombiana se encuentre soportada en la

institucionalidad nacional, pues si bien el Conpes 3864 plantea y establece herramientas importantes, es determinante soportales con una normatividad integral y multidimensional que contemple la persecución del cibercrimen en diferentes escenarios.

REFERENCIAS

Baker, E. (2014). "A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. Information Technology for Development". [S.l], v. 20, n. 2, págs. 122-139.

Bejarano, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio". En: Cuaderno de Estrategia, No. 149, IEEE, febrero de 2011.

Camps, P. (2016). "Ciberdefensa y ciberseguridad: Nuevas amenazas a la Seguridad Nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito". Consulta realizada el 25 de mayo de 2017. Disponible en:

www.calen.gub.uy/pdf/investigacion/2016-1-Ciberseguridad-Camps.pdf

Cancelado, H. (2010). "La seguridad internacional frente a las amenazas globales contemporáneas".

En: *Análisis Político*, Nº 68, Bogotá, enero-abril, 2010, págs. 91-100.

Clarke, R. & Knake, R. (2011). *Guerra en la red, los nuevos campos de batalla.* Barcelona: Editorial Planeta.

Colombia, Consejo Nacional de Política Económica y Social (2016). "Política Nacional de Seguridad Digital". Bogotá, D.C., 2016. (Documento CONPES 3854). Consulta realizada

en diciembre de 2016. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

"Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá, D.C., 2011. (Documento CONPES 3701). Consulta realizada en marzo de 2015. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Colombia, Departamento Nacional de Planeación (2014). "Bases del Plan Nacional de Desarrollo 2014-2018: todos por un nuevo país". Bogotá, D.C., 2014. Consulta realizada en febrero de 2016. Disponible en: https://colaboracion.dnp.gov.co

"Política Nacional de Seguridad Digital. Bogotá, DC, 2016 (Documento CONPES 0000)". Consulta realizada el 22 de abril de 2017. Disponible en: http://www.mintic.gov.co

Cubeiro, E. (2016). "Ciberdefensa". En: Díaz, A. (Ed.). *Conceptos fundamentales de inteligencia*. Valencia: Tirant lo Blanch.

Kissinger, H. (2016). "Orden mundial: Reflexiones sobre el carácter de las naciones y el curso de la historia". [S.l.]: Debate. 2016

Laqueur, W. (2015). "La guerra cibernética". Vanguardia Dossier, [S.l.], No. 54.

Lewis, J. (2002). "Assessing the risks of cyber terrorism, cyber war and other cyber threats". Center for Strategic and International Studies, diciembre de 2002.

Llongueras, A. (2013). *La guerra inexistente, la ciberguerra*. Madrid: Eae Editorial Acad MIA Espa Ola.

McAfee Labs (2011). "McAfee threats report: fourth quarter 2011". Santa Clara, CA, 2012. Consulta realizada en marzo de 2016. Disponible en: http://www.intel.com

Organisation for Economic Co-operation and Development (2015). "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document". Paris: OECD. Consulta realizada el 24 de mayo de 2016. Disponible en: http://www.oecd.org/sti/ieconomy/digital-security-riskmanagement.pdf

"Para el país, la seguridad digital es una política nacional". (2016). En: *Portafolio.com*. Consulta realizada en julio de 2017. Disponible en: http://www.portafolio.co/economia/gobierno/conpes-aprobo-nueva-politica-seguridad-digital-colombia-494057

Sánchez, M. & Jones, S. (2016). "Lineamientos de Política en ciberseguridad y ciberdefensa: Logrando la Seguridad y Defensa de Colombia en un Mundo Digital". En: J. Rodrigues (Ed.), *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional* (págs. 81-94). Rio de Janerio: ESG.

Sancho, C. (2016). "Ciberespacio bien público mundial en tiempos de globalización: Política Pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafío del siglo XXI". En: J. Rodrigues (Ed.), *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional* (págs. 42-74). Rio de Janerio: ESG.

Superintendencia Financiera de Colombia (2015). "Informe de operaciones: Primer semestre de 2015". [S.l.]. Consulta realizada el 25 de abril de 2017. Disponible en: https://www.superfinanciera.gov.co

Theiler, O. (2011). "Nuevas amenazas: el ciberespacio". *Revista de la OTAN* (edición digital). Consulta realizada el 27 de julio de 2017. Disponible en: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

Torres, A. (2011). *Cooperación Policial en la Unión Europea: la necesidad de un modelo de inteligencia criminal eficiente*. [S.l.]: Editorial Dikinson.

Vargas, E. (2014). *Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la Seguridad Nacional?* (Tesis de pregrado). Universidad Militar Nueva Granada. Bogotá.

Vásquez. E. (2016). "Proteger la infraestructura crítica, una tarea fundamental en ciberseguridad nacional". Consulta realizada el 21 de julio de 2017. Disponible en: https://securingtomorrow.mcafee.com

Almagro, L. (2016). "Mensaje del Secretario General de la OEA". En: Organization of American States; Inter-American Development Bank. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Washington, DC. Consulta realizada en enero de 2017. Disponible en: https://publications.iadb.org.

Anderson, G. (2015). "South Korea and Colombia agree to enhance defence ties". En: IHS Jane's 360. Consulta realizada el 15 de febrero de 2017. Disponible en: http://www.janes.com/article/49907/southkorea-and-colombia-agree-to-enhance-defence- ties.

Borg, S. (2005). "No es una guerra fría". En: Vanguardia Dossier, [S.l.], No. 54,

enero/marzo2015. Borja, A. (2005). Ensayos escogidos de Robert O. Keohane y Joseph S. Nye. México: CIDE, Colección Estudios Internacionales.

Candau, J. (2011). Estrategias Nacionales de Ciberseguridad. Ciberterrorismo. Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Chambers-Jones, Clare (2013). "Virtual world financial crime: legally flawed". En: Law and Financial Markets Review [S.l.], v. 7, n. 1, p. 48-56.

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones (2013). "Colombia firma un memorando de entendimiento con Microsoft en temas de ciberseguridad, educación e innovación". Consulta realizada en enero de 2017. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-5037.html.

Comisión Europea (1999). "La transnationalité! Une démarche qui marche!". En: Communautés

européennes sur ec.europa.eu. Consulta realizada en agosto de 2016. Disponible en:

http://ec.europa.eu/employment_social/equal/data/document/i8-fr.pdf.

Colombia, Consejo Nacional de Política Económica y Social (2016). "Política Nacional de Seguridad Digital". Bogotá, D.C., 2016. (Documento CONPES 3854). Consulta realizada en diciembre de 2016. Disponible en:

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Forum of Incident Response and Security Teams (2015). [n/a]. En: About First. [S.l.]. Consulta realizada en julio de 2017. Disponible en: https://www.first.org/about.

Keohane, R. & Nye, J. (1989). Power and Interdependence. Harvard: Harper Collins Publishers.

Maciel, M; Foditsch, N; Belli L; Castellón, N. (2016). "Seguridad Cibernetica, privacidad y

confianza: tendencias en America Latina y el Caribe. El camino a seguir" En: Ciberseguridad

¿Estamos preparads

Nye, J. (2013). "El rugido del clic del ratón". En: El País, [S.l.]. Consulta realizada en junio de

2017. Disponible en:

http://elpais.com/elpais/2013/09/13/opinion/1379069360_411737.html.

Organisation for Economic Co-operation and Development. "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document". Paris: OECD. Consulta realizada en agosto de 2017. Disponible en: http://www.oecd.org/sti/ieconomy/digital-security-riskmanagement.pdf.

Ortega, R. (2007). [Reseña sobre Ensayos escogidos de Robert O. Keohane y Joseph S. Nye]. En Política y Gobierno Política, ISSN: 1665-2037, Vol. XIV, No. 2, 2007, México, págs. 559-562.

Sánchez, M. & Jones, S. (2016). "Lineamientos de Política en ciberseguridad y ciberdefensa: Logrando la Seguridad y Defensa de Colombia en un Mundo Digital". En: J. Rodrigues (Ed.), Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional (págs. 81-94). Rio de Janerio: ESG.

Azócar, D; Lavín, J. (2017). "El desarrollo global del ciberespacio: nuevos desafíos para los Estados y la sociedad civil". *InterNaciones*, *4*(10).

Bollier, D. "The Rise of Netpolitik. How the Internet is Changing International Politics and Diplomacy". The Aspen Institute. Disponible en: http://www.ucm.es/info/sdrelint/ficheros_materiales/ materiales0415.pdf.

Conpes 3854. (2016). "Política Nacional de Seguridad Digital. Bogotá, DC, 2016 (Documento CONPES 3854)". Consulta realizada el 22 de abril de 2017. Disponible en:

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Fisher, A. (2009). "Gov 2.0, a New Year, and a New Approach to Public Diplomacy? Or what does

'Many to Many' Actually Mean?". Disponible en:
http://www.wandrenpd.com/wp-content/uploads/2009/12/ Gov-2-0-What-does-many-to- many-

mean.pdf.

Izquierdo, J. (2016). "La nueva estrategia de seguridad europea 2016". Instituto Español de Estudios

Estratégicos. Documento Marco.

Jefatura del Estado. (2010). "Instrumento de ratificación del convenio sobre la ciberdelincuencia,

hecho en Budapest el 23 de noviembre de 2001. Gobierno de España.

Lichtenstein, J. (2010). "Digital Diplomacy". The New York Times Magazine. Disponible en:

http://www.nytimes.com/2010/07/18/magazine/ 18web2-0-t.html.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). "Estudio sobre el

estado de apropiación de la seguridad de la información en entidades del Estado". Bogotá.

Colombia.

Mogherini, F. (2016). "Una visión común, una actuación conjunta: una Europa más fuerte".

Estrategia global para la política exterior y de seguridad de la Unión Europea.

Nye, J. (2003). "La paradoja del poder norteamericano". Madrid. Taurus.

OCDE. (2015). "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity in Digital Security Risk Management for Economic and Social Prosperity" OCDE Publishing, Paris, Francia. Disponible en: http://www.OCDE.org/sti/ieconomy/digital-security-risk-management.pdf

OEA. (2014). "Recomendaciones y Observaciones - Misión Internacional de Asistencia Técnica en Seguridad Cibernética Colombia Abril de 2014". Publicaciones de la OEA, Washington D.C., Estados Unidos de América.

Rodríguez, A. (2015). "Diplomacia digital, ¿Adaptación al mundo digital o nuevo modelo de diplomacia? Universidad Camilo José Cela. España.

Rubio, R. (2011). "Diplomacia Digital. Una introducción". Universidad Complutense de Madrid.

Terrés, G. (2011). "Diplomacia pública 2.0: una propuesta virtual para un mundo real". Secretaria de relaciones exteriores. Revista Mexicana de Política Exterior.

Secretaria General del Consejo. (2015). "Conclusiones del Consejo sobre la ciberdiplomacia". Consejo de la Unión Europea. Bruselas 11 de febrero 2015.