La ciberdiplomacia como una herramienta de cooperación internacional en pro de un ciberespacio seguro en Colombia

Yubelly Astrid Monroy Álvarez

Trabajo de grado para optar al título profesional:

Maestría en Seguridad y Defensa Nacionales

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

2017

ESCUELA SUPERIOR DE GUERRA

"GENERAL RAFAEL REYES PRIETO"

YUBELLY ASTRID MONROY ÁLVAREZ

DEPARTAMENTO MAESTRÍA EN SEGURIDAD Y DEFENSA NACIONALES

ESCUELA SUPERIOR DE GUERRA
"GENERAL RAFAEL REYES PRIETO"
BOGOTÁ D.C.
NOVIEMBRE- 2017

LA CIBERDIPLOMACIA COMO UNA HERRAMIENTA DE COOPERACIÓN INTERNACIONAL EN PRO DE UN CIBERESPACIO SEGURO EN COLOMBIA.

YUBELLY ASTRID MONROY ÁLVAREZ

Trabajo de grado presentado para optar por el título de:

Magister en Seguridad y Defensa Nacionales

Dirigido por:

Daniela Sánchez Duque

ESCUELA SUPERIOR DE GUERRA

"GENERAL RAFAEL REYES PRIETO"

BOGOTÁ D.C.

NOVIEMBRE- 2017

TABLA DE CONTENIDO

	Pág.
Introducción	1
I.CIBERESPACIO: EL QUINTO DOMINIO DE LA INTERACCIÓN HUMANA.	3
1.1. El ciberespacio como un bien público mundial: Una breve revisión conceptual.	3
1.2. Ciberespacio seguro: El nuevo paradigma de la Seguridad Estatal	9
1.3. La Defensa y Seguridad de Colombia en un mundo digital	13
II. CIBERAMENZAS: UN PROBLEMA DEL ORDEN TRANSNACIONAL	21
2.1. La Cooperación Internacional como medida de contención para las ciber amenazas.	21
2.2. Cooperación internacional en el marco de la lógica de ciberseguridad.	25
2.3. Colombia y su posicionamiento en los escenarios de Cooperación Internacional para asuntos de ciberdefensa y ciberseguridad.	28
III. LA CIBERDIPLOMACIA COMO HERRAMIENTA DE COOPERACIÓN INTERNACIONAL	33
3.1 El cambio de lógica de la diplomacia tradicional a la ciberdiplomacia	33
3.2 La Unión Europea como configurador de la ciberdiplomacia	37
3.3 La ciberdiplomacia: Una tarea pendiente para Colombia	41
CONCLUSIONES	45

ANEXOS

Anexo 1	Resumen de Estado de Riesgo del Ciberespacio.
Anexo 2	Total de suscriptores de Internet.
Anexo 3	Episodios destacados de Ciberguerra en el Sistema Internacional.
Anexo 4	Marco normativo colombiano en materia de ciberdefensa y ciberseguridad.
Anexo 5	Iniciativas de ciberseguridad según Bases del PND.

INTRODUCCIÓN

El desarrollo de fenómenos como la globalización y con ello la construcción de un Sistema Internacional altamente interdependiente ha impactado las dinámicas de seguridad, toda vez que se reconocen nuevos escenarios y actores que intervienen en ella. Así pues, la seguridad y defensa se desliga de escenarios tradicionales, para dar paso a un nuevo escenario siendo este el ciberespacio.

En la actualidad, las características del ciberespacio han conducido a catalogarlo como un "bien público mundial"[1], y la importancia que ocupa en la actual agenda internacional es innegable teniendo en cuenta los riesgos que diariamente lo amenazan. En este sentido, este ámbito virtual representa un factor de vital importancia para la Seguridad Nacional de los Estados, pues un ataque cibernético podría afectar tanto a los clientes de un banco, como a los habitantes de una ciudad, y dependiendo del caso, la estabilidad entera de todo un país, siendo así un escenario no tradicional en el cual convergen intereses tanto estatales como de naturaleza disímil.

Considerando la dimensión trasnacional del ciberespacio y las múltiples amenazas a su seguridad, promulgar por un ciber espacio seguro supone un trabajo mancomunado entre los Estados y diferentes actores del Sistema Internacional, ya que una confrontación aislacionista de dicho fenómeno es obsoleta, pues éste exige un accionar coordinado. Desde esta perspectiva herramientas como la ciberdiplomacia son de gran importancia, pues permite consolidar esfuerzos colectivos en pro de un mismo objetivo.

En este contexto, y teniendo a Colombia como estudio de caso surge la pregunta rectora de la presente investigación siendo esta ¿Cómo la ciberdiplomacia constituye una herramienta de cooperación internacional en pro de un ciber espacio en Colombia? Frente al anterior cuestionamiento, se plantea la ciberdiplomacia como una herramienta de cooperación internacional que podrá ayudar a Colombia a consolidar un ciberespacio seguro, ello, bajo la comprensión del ciberespacio como un escenario multidimensional y cuya protección requiere medidas de orden domestico acompañadas por la inserción de Colombia en las dinámicas de cooperación internacional en pro de un ciberespacio seguro.

---

[1] Bien colectivo de dimensión universal del que se benefician todos los países y sus habitantes tanto de hoy como del futuro (SKOS).

Con el fin de sustentar y desarrollar el anterior planteamiento, el presente documento se encuentra dividido en tres capítulos cada uno de los cuales busca desarrollar los objetivos específicos de la investigación. El primer capítulo explica el proceso de securitización del ciberespacio, determinando este último como un escenario en el que participan múltiples actores no tradicionales y en cuya agenda se deben considerar temas no convencionales que escapan a la lógica tradicional de seguridad. En este sentido, la hipótesis de trabajo de la presente investigación es es sostenible desde una perspectiva de seguridad no tradicional, resultado de la ampliación y profundización frente a los actores y los fenómenos, así como bajo el reconocimiento de un Sistema Internacional globalizado y altamente interdependiente.

A lo largo del segundo capítulo, se presenta la cooperación internacional como un mecanismo efectivo en la contención de problemas de seguridad asociados al ciberespacio, ello bajo la comprensión de las amenazas al ciberespacio como problemas de orden trasnacional que escapa las capacidades estatales, haciendo necesario la cooperación internacional en un escenario de interdependencia compleja. Así mismo, se revisa la participación de Colombia en diferentes instancias internacionales, analizando brevemente si en Colombia existen políticas públicas o estrategias tendientes a materializar de manera efectiva lo pactado o acordado a nivel internacional.

Finalmente, el tercer capítulo y tras desarrollar conceptualmente las dos variables de la presente investigación[2], se expone la ciberdiplomacia como una herramienta de cooperación internacional viable para lograr un ciber espacio seguro. Para ello, y frente al caso colombiano, se enfatiza en la necesidad de un enfoque integral en la construcción de capacidades de seguridad cibernética, así como en la protección de la infraestructura critica desde una perspectiva preventiva y defensiva más que ofensiva, en la comprensión de la ciberdiplomacia como una herramienta abierta que vincule a múltiples actores no sólo de orden estatal.

Cabe señalar que el mayor aporte de la presente investigación se refleja en el segundo capítulo, pues es en este justamente donde se expone la ciberdiplomacia y algunos escenarios

[2] Variable dependiente: Ciberespacio seguro + Variable independiente: Ciberdiplomacia como herramienta de cooperación internacional

puntuales en los que Colombia debe trabajar para consolidar y articular la estrategia domestica de ciberseguridad en el escenario internacional.

Ahora bien, frente a los aspectos frente a los aspectos metodológicos, se debe señalar que la investigación se enmarca en un estudio de caso, el cual aborda como objeto de estudio la consolidación de un espacio ciberespacio seguro en Colombia. Así mismo, el trabajo es de tipo descriptivo, ya que se presentan los principales avances y escenarios de cooperación internacional en pro de un ciberespacio seguro, a la vez que se conceptualiza extensamente el ciberespacio, en este sentido, la investigación interrelaciona dos variables: ciberespacio seguro y ciberdiplomacia como herramienta de cooperación internacional.

Así mismo, el trabajo se realiza desde un enfoque metodológico cualitativo, al utilizar herramientas de orden narrativo, priorizando fuentes secundarias, al acudir a textos académicos, artículos, revistas indexadas, memorias, CONPES, entre otros recursos bibliográficos como herramienta para aproximarse al caso de estudio.

Por otro lado, se afirma que la investigación presenta visos de una investigación bajo el enfoque institucionalista, pues las organizaciones e instituciones internacionales constituyen el medio mediante el cual los diferentes actores interactúan entre sí en pro de la consolidación de un espacio ciberespacio seguro. (Sánchez, 2015, pág., 14). Por último, se debe señalar que hasta el momento se desconoce investigación alguna que relacione las dos variables, y que en especial proponga la ciberdiplomacia como una herramienta para fortalecer el actual escenario colombiano, lo cual ya convierte esta investigación en innovadora desde la perspectiva académica.

I. CIBERESPACIO: EL QUINTO DOMINIO DE LA INTERACCIÓN HUMANA

1.1. El ciberespacio como un bien público mundial: Una breve revisión conceptual

Las guerras han sido un factor inherente a la historia de la humanidad, lo que ha significado que su evolución implique procesos de adaptación ante las diferentes herramientas y estrategias tanto en los campos tradicionales de batalla como en otros.

En este sentido, los conflictos han evolucionado hasta llegar a las denominadas *guerras híbridas*, caracterizadas por el empleo de estrategias militares no convencionales, como el despliegue de militares sin identificación en un territorio, las acciones de inteligencia, la *ciberguerra* se ha consolidado como un ambiente cotidiano donde diferentes actores como personas, organizaciones y gobiernos interactúan, con el fin de comunicarse y realizar ''transacciones económicas e inclusive gestionar diversas actividades grupales a nivel nacional e internacional" (Sancho, 2016, p.41).

En este sentido, Clarke y Knake (2011) lo definen de la siguiente manera:

> El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de Internet. Es importante dejar claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de Internet podemos comunicarnos con cualquier ordenador conectado y con cualquiera otra de las redes de Internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde Internet. Algunas de esas redes privadas son muy semejantes a Internet, pero, al menos teóricamente, se encuentran separadas de ella. (p. 104)

En la actualidad, las características del ciberespacio han conducido a catalogarlo como un "bien público mundial"[3], y la importancia que ocupa en la actual agenda internacional es innegable teniendo en cuenta los riesgos que diariamente lo amenazan. En este sentido, este ámbito virtual representa un factor de vital importancia para la Seguridad Nacional de los

[3] Bien colectivo de dimensión universal del que se benefician todos los países y sus habitantes tanto de hoy como del futuro (SKOS).

Estados, pues un ataque cibernético podría afectar tanto a los clientes de un banco, como a los habitantes de una ciudad, y dependiendo del caso, la estabilidad entera de todo un país, siendo así un escenario no tradicional en el cual convergen intereses tanto estatales como de naturaleza disímil.

Por lo anterior, Llongueras Vicente (2013) realiza un análisis sobre lo que el ciberespacio representa para la Seguridad Nacional de un Estado:

> El ciberespacio es un elemento de poder dentro la Seguridad Nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias, forjándose y desarrollándose el concepto de las operaciones militares centradas en redes (p.19)

En este contexto, surgen dos conceptos claves para referirse a las acciones del Sector Defensa y Seguridad, así como a la actuación de los actores del Sistema Internacional en el ciberespacio, siendo estos *ciberdefensa* y la *ciberseguridad*. Estos dos conceptos se han convertido en pilares fundamentales de la Seguridad Nacional de los Estados, y aunque muchas veces son utilizados como sinónimos, es importante diferenciarles. En este sentido, mientras la ciberseguridad

> tiene una connotación eminentemente de protección, la ciberdefensa engloba otras acciones más allá de las puramente defensivas; entre ellas, la denominada ciberdefensa activa, la ciberinteligencia, y todo un abanico de acciones ofensivas: la intrusión, la infección, la denegación de servicios o la alteración de la información, que puede llevar aparejada incluso la destrucción física. (Cubeiro, 2016, p.45).

A partir de lo anterior, se considera la existencia de una relación de complementariedad entre los dos conceptos, por lo cual su aprehensión por parte de los gobiernos nacionales al momento de realizar la planificación de las políticas de Defensa y Seguridad cibernética es determinante. Así como la ciberseguridad se encuentra vinculada estrechamente a la Estrategia de Seguridad Nacional, la ciberdefensa no puede ser un caso aislado, por el

contrario, debe estar incluida en la Defensa Nacional, en la Defensa Militar y en la Defensa Civil. También en temas como, la protección de *infraestructuras críticas* y la lucha contra organizaciones criminales y terroristas (Feliu, 2012).

En este sentido, existen países como Estados Unidos que han decidido privilegiar con vehemencia la consolidación de una política de ciberdefensa seria y agresiva. Según Laqueur (2015), el Pentágono "dispone de una lista de armas cibernéticas destinadas al espionaje y sabotaje propios de la ciberguerra. En todas las principales operaciones ofensivas tales como la de introducir un virus en las redes de países extranjeros, se precisa la aprobación del Presidente" (p.13). Respecto a lo anterior, Kissinger (2016) plantea que el mundo debe comenzar a preguntarse si la "tecnología de Internet ha superado la estrategia y la doctrina, al menos por ahora, [particularmente cuando es] más fácil emprender ciberataques que defenderse de ellos, lo que posiblemente estimulará una propensión ofensiva en la construcción de nuevas capacidades" (p.345).

Ahora bien, respecto a la infraestructura crítica, ésta se puede definir en el ámbito de la cibernética como "instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad, el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos" (Torres, 2011, p.347). De este modo, la protección de este tipo de infraestructura es una tarea fundamental para la ciberdefensa y la ciberseguridad de todo país, pues aunque en un principio, por ejemplo, se consideraba que un *malware*[4] solo tenía capacidad de generar daños en los "archivos" de un equipo, en la actualidad es posible que pueda llegar a destruir su *hardware*.

[4] Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento (InfoSpyware).

Por lo anterior, se destaca otra caracterización de la infraestructura crítica tomada de las disposiciones para la *Estrategia Digital Nacional en Materia de Tecnologías de la Información y Comunicaciones de México*, en donde se define como aquellas "infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional" (Vásquez, 2016, párr.4). En este punto, una realidad que se debe tener en cuenta es que los logros de la ciberdelincuencia y el ciberespionaje combatidos mediante la ley y la contrainteligencia, han encontrado pocos obstáculos en este tipo de estrategias, lo que indica, que es cuestión de tiempo para que ciberataques cada vez mayores comiencen a atentar contra las infraestructuras críticas y de manera más eficaz (Bejarano, 2011).

Así, la estrategia de Defensa y Seguridad de todo Estado deberá ser implacable en la prevención de posibles ataques, en la protección para disminuir la vulnerabilidad y, en caso de crisis, en minimizar daños y acelerar el período de recuperación. Las amenazas a la infraestructura crítica siempre han existido en tiempos de guerra o conflicto, pero en la actualidad los escenarios de amenaza incluyen también ataques en tiempos de paz por medio de ciberataques (Feliu, 2012).

Adicionalmente, y como lo plantea Lewis (2002), si se tiene en cuenta que un ciberataque resulta más fácil y barato que uno físico (así los niveles y duración de los primeros sean comparativamente menores), se hace fundamental proteger este tipo de infraestructura mediante las siguientes recomendaciones:

> (...) servicios y organizaciones estratégicas, lo cual obliga a convocar a actores de diversa naturaleza, provenientes de la administración civil del Estado y a las Fuerzas Armadas y de Orden y Seguridad, junto a variados estamentos dentro de la sociedad civil, quienes deben garantizar que esa información cumpla con las siguientes características: disponibilidad,

> integridad, oportunidad, confiabilidad, interoperabilidad, seguridad. (Sancho, 2016, págs.57-58)

Por lo anterior, este concepto toma gran relevancia en la presente investigación, pues todo ataque contra el ciberespacio se perpetrará contra la infraestructura crítica, lo que pondría en juego la estabilidad de un determinado Estado, así como la confianza de la ciudadanía en tal territorio para enfrentarse a estas amenazas. En este orden de ideas, se debe realizar otra diferenciación conceptual entre dos nociones que se usan indistintamente en el ámbito de la defensa y la seguridad cibernética: el *cibercrimen* y la *ciberamenaza*. Los anteriores términos no pueden catalogarse como categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la Seguridad Nacional, ni todas las amenazas a la Seguridad Nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos de terrorismo y criminalidad organizada, determinadas formas de cibercriminalidad sí representan verdaderas amenazas a la Seguridad Nacional (Feliu, 2012). Para efectos de la investigación, se tendrá en cuenta esta categorización a la hora de utilizar un término u otro.

Con la evolución de los conflictos armados fue mutando el concepto de seguridad tradicional "para dar paso a una nueva función del Estado que es la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos frente a las amenazas emergentes en el escenario de una vida más digital y gobernada por la información" (Sánchez 2011, párr.3). De allí, y como se analizará más adelante, la importancia que tiene la consolidación de estrategias contundentes y multidimensionales para prevenir y combatir los ataques al ciberespacio, comprendido como un bien público mundial, y orientadas, por ende, a garantizar la Seguridad Nacional de los actores internacionales.

Como pudo examinarse en este primer apartado, los conceptos de Defensa y Seguridad han evolucionado en atención a la aparición de nuevas y cada vez más sofisticadas amenazas a los Estados.

1.2. Ciberespacio seguro: El nuevo paradigma de la Seguridad Estatal

Las organizaciones políticas humanas, desde la antigüedad, han sufrido serios desafíos a su Defensa y Seguridad, pues de forma continua las estrategias de guerra y las amenazas a estas variables han cambiado y generado nuevos retos, pasado así por en un principio a las tribus, luego a los imperios, más tarde a las naciones y posteriormente a los Estados modernos (Cancelado, 2010, p.92). En este sentido, tras el final de la Guerra Fría y los atentados del 11 de septiembre de 2001 (11-S), el Orden Mundial se redefinió especialmente en materia de seguridad, configurando nuevas prioridades en la agenda política de los diferentes actores del Sistema Internacional.

Las fronteras territoriales empezaron a perder poder, al igual que el dominio militar del espacio y el tiempo. El uso de aviones civiles en un atentado terrorista demostró que todo podía llegar a convertirse en un arma, en cualquier momento, por tanto nada comenzó a parecer imposible o impensable en el reinventado Orden Mundial del siglo XXI (Theiler, 2011, párr.2).

Como se explicó en el anterior apartado, con la evolución de Internet y la llegada de las nuevas Tecnologías de la Información y las Comunicaciones (TIC) se dio origen a un nuevo espacio para el desarrollo de las actividades humanas: el ciberespacio. Éste se constituyó, de acuerdo con la revista *The Economist*, en el *quinto dominio de interacción humana*, luego del terrestre, el marítimo, el aéreo y el espacial (Camps, 2016). De este modo,

el ciberespacio comenzó a posicionarse progresivamente como un campo que debía ser atendido desde la perspectiva de Seguridad de los Estados.

En un comienzo el ciberespacio parecía ser el escenario virtual e ideal para facilitar la vida de millones de personas alrededor del mundo, poniendo a su disposición información, nuevas posibilidades y servicios para los usuarios, convirtiéndose en un instrumento estratégico para la industria, la administración y las Fuerzas Militares. Sin embargo, a partir del 11-S, esta herramienta comenzaría a convertirse en un serio riesgo para todo el Sistema Internacional, mutando en un campo fértil para amenazas de diversa índole en un mundo globalizado y, por ende, cada vez más interconectado.

Así, las amenazas tradicionales transformaron su forma y ámbito de actuación, pasando ahora a accionar en este ciberespacio, dando lugar a la aparición de términos como ciberdelito, cibercrimen, ciberactivismo, ciberterrorismo, ciberespionaje, ciberataque, ciberseguridad, los cuales se constituyeron como nuevos riesgos en el ámbito cibernético. A partir del surgimiento de este tipo de amenazas (ciberamenazas), los Estados empezarían a dirigir sus esfuerzos hacia la creación de infraestructuras institucionales y normativas para contener cualquier ataque cibernético, pues la salvaguarda de la soberanía y la integridad del espacio geográfico ya no podía asegurarse únicamente por medio de la defensa militar, dada la complejidad de un nuevo tipo de amenazas que comenzarían a exigir una visión mucho más amplia e integral de los gobiernos durante la planificación de su Defensa y Seguridad (Camps, 2016).

La importancia de un ciberespacio seguro y blindado es innegable en un mundo cada vez más interconectado, pues cada día se hace más extenso, alberga más información y aumenta su oferta de servicios para los usuarios. El denominado quinto dominio de la interacción humana es susceptible a amenazas que pueden ocasionar daños complejos para

las víctimas y otorgar grandes réditos a los victimarios, quienes muchas veces, incluso, no pueden ser identificados. En este medio, los ataques pueden ser patrocinados por Estados o empresas privadas, pueden venir de grupos organizados con fines terroristas o activistas, de organizaciones delictivas o de simples individuos, así como pueden ser dirigidos o genéricos y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso (Camps, 2016).

En este sentido, salvaguardar el ciberespacio se ha posicionado como un elemento central en la planificación de la Defensa y Seguridad de los Estados, pues debido a los riesgos y amenazas que lo pueden vulnerar, se hace necesario garantizar una serie de estándares mínimos de seguridad en su uso, lo cual implica enfrentar desafíos importantes a nivel nacional e internacional. De esta manera, Sancho (2016) destaca algunos de los derroteros que deben tener en cuenta los Estados al momento de diseñar y estructurar su estrategia para prevenir actividades ilícitas en el ciberespacio:

> En el nivel nacional, la formulación de una política pública de ciberseguridad que contemple e integre los diferentes aspectos involucrados en este tema con la finalidad de evitar que un ciberincidente ponga en riesgo la vida de las personas, su patrimonio y/o la seguridad nacional. A nivel internacional cobra relevancia la necesidad de participar en instancias de diálogo multilaterales, donde sean abordados temas como: la gobernanza en internet; estándares mínimos de seguridad en el ciberespacio y la participación en convenios o resoluciones internacionales sobre situaciones que afectan la ciberseguridad y que involucran a diferentes países del mundo. (p.49)

A partir de lo anterior, se evidencia cómo la búsqueda de un ciberespacio seguro demanda la 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, las cuales pueden traer consigo efectos devastadores[5]. Al respecto, el *Informe de Riesgos*

[5] Ver Anexo 1

Mundiales (2013), elaborado por el Foro Económico Mundial (FEM), advirtió sobre el peligro de los "incendios digitales en un mundo hiperconectado". Con ello, se refería a las consecuencias sociales e inclusive políticas que puede generar la información falsa difundida en Internet, resultado de un error humano o una acción deliberada, siendo esta última la que genera mayores desafíos desde la perspectiva de la seguridad de la información en el ciberespacio (Sancho, 2016).

Como se analizó en este apartado, el ciberespacio, además de representar las ventajas de la evolución informática y digital, como la economía en las comunicaciones y demás, se ha convertido en un bien público de carácter global constantemente amenazado por actividades ilícitas que se pueden perpetrar en él con inconmensurables secuelas para sus víctimas. En consecuencia, cada vez son más los Estados que han asumido dentro de sus prioridades en materia de Defensa y Seguridad la vinculación de una nueva necesidad: "la defensa del quinto dominio".

Para alcanzar este objetivo, se ha hecho necesario comprender que esta defensa debe realizarse desde diversos ámbitos y a partir de una asociación de esfuerzos entre actores estatales y no estatales, alineándose con los estándares internacionales en esta materia, 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. De este modo, es fundamental que los gobiernos implementen buenas prácticas en materia de ciberdefensa y ciberseguridad para evitar el cibercrimen, el ciberespionaje, el ciberhacktivismo, e incluso, la ciberguerra y, en caso de producirse alguno de ellos, contar con un plan de contingencia que contemple acciones de prevención, respuesta, mitigación y resiliencia, con la finalidad de enfrentar de la mejor forma posible el ciberincidente manifestado (Sancho, 2016).

Con base en lo argumentado, es claro cómo la evolución de las tecnologías de la información y las comunicaciones no solo se ha puesto a disposición de millones de personas un ámbito virtual que facilita sus vidas de distintas maneras, sino además, un reto a la Seguridad Nacional de los actores que conforman el Sistema Internacional. El anterior desafío, sin duda alguna, representa un nuevo paradigma en la planificación de la Defensa y Seguridad de los Estados que es la búsqueda de un ciberespacio seguro.

1.3. La Defensa y Seguridad de Colombia en un mundo digital

Colombia ha presentado una tendencia creciente en los niveles digitales desde hace varios años, lo cual ha traído grandes oportunidades y amenazas para el país. El número de suscriptores a Internet (fijo dedicado y móvil) en Colombia pasó de 687.637 en el 2005 a casi 11'000.000 en el primer trimestre del 2015 (Consejo, 2016, p.27; Colombia, 2015, p.9)[6]. Asimismo, el sector que más se vio favorecido con el aumento de los niveles de conectividad en los últimos años ha sido el financiero, toda vez que el número de operaciones monetarias usando Internet como canal pasó de 31.66% en el 2012 a 42.62% en el 2015, lo cual significó un 35% más de transacciones (Superintendencia, 2015).

Los altos niveles de conectividad incrementan la dependencia de los diferentes actores (individuos, empresas, instituciones públicas y privadas, etc.) a las Tecnologías de la Información y las Comunicaciones, lo que significa mayor riesgo proveniente de las amenazas que rondan en el ambiente digital (Sánchez & Jones, 2016). Teniendo en cuenta los acontecimientos de los últimos años en el mundo generados por ataques al ciberespacio,

[6] Cfr. Estadísticas del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (Ver Anexo 2).

Colombia se ha volcado, cada vez más, a fortalecer sus capacidades en materia de ciberdefensa y ciberseguridad para contrarrestar eventuales riesgos.

En 2011, el país realizó un primer gran esfuerzo desplegando su primera política pública en la materia mediante la formulación del "CONPES 3701: *Lineamientos de Política para ciberdefensa y ciberseguridad*", documento desarrollado por el Consejo Nacional de Política Económica y Social, siendo un hito que permitió al país iniciar un camino con grandes logros operativos, legislativos, estratégicos y diplomático (Sánchez & Jones, 2016, p.81).

Como se ha analizado hasta aquí, "no es un misterio que las Tecnologías de la Información y Comunicación, al igual que los mayores niveles de conectividad, traen grandes beneficios y oportunidades para los diferentes usuarios" (Baker, 2014, págs.122-123), de lo anterior que Colombia ha dirigido sus esfuerzos en materia de Defensa y Seguridad al mantenimiento de un ciberespacio[7] seguro y que le permitiera potenciar las capacidades económicas y sociales del país con la ayuda de este ámbito virtual.

Además de las experiencias negativas de los últimos veinte años en el mundo [8]vale la pena mencionar algunos incidentes cibernéticos que tuvieron lugar, no hace mucho tiempo, en la región y en el país. Dichos eventos, también impulsarían la consolidación del CONPES 3701, ya que a partir de éstos quedaron expuestas algunas debilidades de Colombia en materia cibernética:

> El 23 de diciembre de 2009 se desmanteló, en una operación conjunta entre Panda Security, FBI y la Guardia Civil Española, una de las más grandes Botnets para cyberscamming y DDoS conocidas hasta la fecha: Botnet "Mariposa". En la cuenta de afectación de Mariposa- 13 millones de

[7] La legislación Colombiana entiende el término "ciberespacio" de la siguiente manera: "Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios" (Resolución 2258 de 2009, Comisión de Regulación de Comunicaciones de la República de Colombia).
[8] (Ver Anexo 3),

> computadores, 190 países y 31.901 ciudades – Colombia se encontró en la quinta posición con 4.94% de las infecciones, dos de sus ciudades principales también lograron la lista de mayor número de IP comprometidas (i.e. Bogotá, D.C, 2.68% y Medellín 0.65%). Ese mismo año, McAfee Labs ya había identificado a Colombia como el origen de 1.9% del Spam mundial, por encima de países con mayor nivel de conectividad y población como Rusia. (Sánchez & Jones, 2016, p.82)

En esta misma línea, durante el año 2009 se presentaron una gran cantidad de delitos informáticos que tuvieron lugar en Colombia. Mención aparte se debe hacer a las filtraciones de los cables secretos de los Estados Unidos publicados por *WikiLeaks* entre 2010-2011, las cuales tuvieron un impacto importante en las relaciones diplomáticas entre Colombia y sus vecinos, particularmente con Venezuela y Ecuador (Sánchez & Jones, 2016).

Por otra parte, el 15 de abril del año 2011, las páginas web de Presidencia, Senado, Ministerio del Interior y la plataforma de trámites "Gobierno en Línea", fueron víctimas de ataques DDoS[9] que las inhabilitaron por varias horas. Estos ataques fueron atribuidos al grupo hacktivista *Anonymous*, y se replicarían el 20 de julio del mismo año en el marco de lo que este grupo denominó "Operación Independencia", continuando hasta 2012 mediante una arremetida exacerbada por la presentación de una nueva versión de la Ley Lleras (Ley 201 de 2012) y la Cumbre de las Américas (Sánchez y Jones, 2016).

Adicionalmente, según el *McAfee Threats Report*, Colombia presentó en el año 2011 un aumento significativo de computadores *Zombie* utilizados como remitentes de Malware para la creación de botnets, superando a países como Japón, España, Australia, Portugal, Reino Unido y Venezuela (McAfee Labs, 2011, p. 11-13). Vale la pena mencionar, que esta

[9] Los ataques DDoS (Distributed Denial of Service) son los ataques más comunes que puede tener una página web, que consiste en saturar los servidores web de una institución hasta el punto que esta misma colapse, para esto se utilizan computadoras que se encuentren infectadas por virus (botnets) haciendo que se cree una red, en esta red de computadoras infectadas, los usuarios no se dan cuenta que hacen parte del ataque (Vargas, 2014, p.6).

estadística negativa que ostentaba el país fue decreciendo con la implementación del CONPES 3701.

Hechos como los expuestos, serían el punto de partida para incentivar la creación del referenciado documento, el cual establecería los derroteros del país para contener este tipo de amenazas en el ciberespacio. En este sentido, esta política fue explícita en su introducción: "*El Gobierno Nacional requiere conocer y actuar de forma integral frente amenazas informáticas (...) que puedan comprometer información, afectar infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado*" (Consejo, 2011, págs.4-5).

Para alcanzar el anterior objetivo, dentro del documento se establecieron tres ejes estratégicos: Desarrollo de capacidades de ciberseguridad y ciberdefensa, fortalecimiento del cuerpo normativo, y capacitación especializada. Adicionalmente, para apoyar el objetivo de esta política se constituyeron cuatro instancias: Comisión Intersectorial[10], Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT)[11], Comando Conjunto Cibernético de las Fuerzas Militares (CCOC)[12], Centro Cibernético Policial (CCP)[13].

Los resultados del CONPES 3701 fueron más que satisfactorios para Colombia, pues al año 2015 se había cumplido en un 90% lo planteado por el Consejo Nacional. Los logros más representativos con la implementación del CCOC, por ejemplo, serían: "La creación de un comité de ciberdefensa de las Fuerzas Militares; adquisición de la plataforma de entrenamiento y ciberdefensa; cooperación internacional con Estados Unidos, OEA, y

---

[10] La Comisión Intersectorial se planteó como el cuerpo de direccionamiento estratégico de carácter interagencial encargado de fijar lineamientos para política.

[11] El ColCERT se diseñó como el grupo que da forma a los lineamientos estratégicos, coordinando las acciones necesarias para proteger al Estado colombiano frente a amenazas cibernéticas que atenten o comprometan su Defensa y Seguridad Nacional.

[12] El CCOC se estableció para prevenir y contrarrestar amenazas o ataques cibernéticos que afecten los valores e intereses nacionales (Consejo, 2011, págs. 20-24).

[13] El CCP se diseñó para el apoyo y protección ante delitos cibernéticos.

España; 38 cursos de capacitación y 340 servidores entrenados; adquisición de plataformas operacionales en ciberdefensa; identificación de infraestructuras críticas cibernéticas nacionales; elaboración del manual de ciberdefensa conjunta" (Sánchez & Jones, 2016, p.86).

De igual forma, con la implementación del CONPES 3701 se atendieron muchos más incidentes digitales en Colombia. "El CCP agenció 2.652 incidentes en el año 2013, mientras que para el año 2015 el CCP y CSIRT de la Policía Nacional atendieron 6.366 incidentes, incrementando la cobertura de capacidades operativas en un 140%" (Sánchez & Jones, 2016, p.86).

En materia de infraestructura normativa para la ciberdefensa y la ciberseguridad, el Consejo determinó una falencia dentro del Ordenamiento Jurídico colombiano al respecto. Por esta razón, se recomendó fortalecer el cuerpo legal y la *cooperación internacional* en asuntos cibernéticos. "Desde julio del año 2011, Colombia desarrolló 11 herramientas jurídicas (4 leyes y 7 decretos) en materia cibernética; algunas para seguridad y defensa, otras para regular servicios electrónicos" (Sánchez & Jones, 2016, p.86). De esta forma, el Estado colombiano logró robustecer la regulación y legislación en el ámbito cibernético para blindar el ciberespacio, también, desde el ámbito normativo[14].

En 2015, con la creación de un nuevo borrador de CONPES en materia cibernética y en el marco del Plan Nacional de Desarrollo (2014-2018) "Todos unidos por un nuevo país", se delineó la "Política Nacional de Seguridad Digital en Colombia", a partir de ahora CONPES 3854 de 2016. En concordancia con lo argumentado hasta aquí, dentro del PND (en sus bases) se estableció que el respeto de la soberanía nacional y la protección de los intereses nacionales implicaría un reconocimiento del dominio ciberespacial -también

[14] (Ver Anexo 4).

conocido como quinto dominio-, lo que involucra, además, que el país debe desarrollar sus capacidades de neutralización y reacción frente amenazas que atenten contra la crítica digital (DNP, 2014). En las bases del DNP, también quedó claro cómo la estrategia nacional de ciberseguridad debe cumplir algunas iniciativas precisas.[15]

Se debe señalar que, a partir de la aprobación del CONPES 3854 el 11 de abril de 2016, se proyectarían algunas novedades en materia cibernética al introducir un nuevo enfoque para la seguridad digital: *la gestión del riesgo en Colombia*. "Esta transversalidad implica que los actores sufren los impactos provenientes de los riesgos digitales y, en consecuencia, se requiere de un esfuerzo cooperativo para gestionarlos" (Organisation, 2015, p.4). De esta forma, se evidencia cómo los retos de Colombia en el ciberespacio se plantean dentro el nuevo documento a la luz de las recomendaciones de organismos internacionales como la Organización Económica para la Cooperación y Desarrollo (OECD) y la Organización de Estados Americanos (OEA).

En este sentido, vale la pena destacar cómo Colombia se convirtió en el primer país de Latinoamérica, y uno de los primeros en el mundo en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas por la OECD. Según este organismo internacional, en la medida que se cuente con una aproximación basada en la administración del riesgo, y siempre que se mantenga un enfoque económico y social, los riesgos digitales pueden aproximarse como riesgos económicos. Adicionalmente, aseguran que una aproximación diferencial de la seguridad digital genera una respuesta excluyente que contraviene la naturaleza transversal del ámbito digital (Sánchez & Jones, 2016, p.91).

[15] (Ver Anexo 5).

Para generar este nivel de confianza, la "Política Nacional de Seguridad Digital en Colombia" dispone de cinco dimensiones y objetivos estratégicos, todos soportados en cuatro principios fundamentales. El primero de estos principios es salvaguardar los derechos humanos y valores fundamentales de los individuos, lo cual gira en torno a temáticas tan complejas como garantizar la libertad de *expresión, confidencialidad, y protección de la* intimidad (Consejo, 2016, p.71). El segundo principio es la adopción de un enfoque influyente y colaborativo que involucre a los actores que hacen uso del entorno digital. El tercer principio se refiere a la corresponsabilidad de estos actores para proteger el entorno, mientras que el último principio enfatiza la necesidad de contar con un enfoque basado en la gestión de riesgos (Sánchez & Jones, 2016, p.92). Las cinco dimensiones estratégicas que encaminan la formulación de los objetivos son: fortalecimiento del marco legal y regulatorio, gobernanza, gestión sistémica del riesgo, cultura ciudadana, y capacidades para la gestión del riesgo (Consejo, 2016, págs.71-72).

Así, el CONPES 3854 otorga una visión estratégica a Colombia que le permite vincular integralmente las partes interesadas para gestionar los riesgos de la seguridad digital, maximizar las oportunidades en el desarrollo de actividades socioeconómicas, desarrollar las capacidades de ciberdefensa y ciberseguridad necesarias y fortalecer los esfuerzos de cooperación y colaboración nacional e internacional (Consejo, 2016, págs.47-65). Las anteriores líneas estratégicas se consolidarían dentro de la nueva política a partir de aportes realizados por los representantes del sector privado, del Gobierno, de la sociedad civil, de la industria TI y de la Academia (Portafolio, 2017, párr.13).

Adicionalmente, y bajo la misma lógica de la OECD, el CONPES 3854 parte de la premisa que mayor confianza en el entorno digital significará mayor prosperidad económica, política y social, y que esta puede construirse mitigando el riesgo proveniente de

vulnerabilidad y amenazas a niveles aceptables (Consejo, 2016, págs.10-55). Lo anterior, implica que las medidas de seguridad que se tomen deben tener un entendimiento holístico de las necesidades de todos los actores, y que no deberían ser tan férreas que impidan el uso del ambiente digital abierto requerido para generar capital. Este nuevo enfoque de política para Colombia es más entendible cuando se conocen las cifras nacionales, pues los sectores más afectados en Colombia por los incidentes digitales para el año 2015, fueron también los que más aportaron al Producto Interno Bruto (PIB) (Sánchez & Jones, 2016, p.91).

Para finalizar, se debe aducir que el tema de cooperación internacional en materia de defensa del ciberespacio, eje fundamental del CONPES 3854, se abordará en los siguientes capítulos de la investigación.

II. CIBERAMENZAS: UN PROBLEMA DEL ORDEN TRANSNACIONAL

2.1. La Cooperación Internacional como medida de contención para las ciber amenazas.

Como se expuso a lo largo del primer capítulo de la presente investigación las amenazas al ciberespacio representan un problema del orden transnacional[16] 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"[17] planteado por Robert Keohane y Joseph Nye en su obra *Power and Interdependence*.

A partir de este término, Keohane y Nye fundamentaan 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 (Ver Anexo 5). 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.

[16] Según la Comisión Europea, la transnacionalidad es la noción que define y engloba lo que excede el marco de una nación.

[17] Para Keohane, la interdependencia se entiende como "el uso de la fuerza, la falta de jerarquía en los asuntos a tratar y la presencia de múltiples canales de contacto entre las sociedad" (Keohane & Nye, 1989, p.165).

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 las mismas, 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. Cooperación internacional en el marco de la lógica de ciberseguridad

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. Colombia y su posicionamiento en los escenarios de Cooperación Internacional para asuntos de ciberdefensa y ciberseguridad

Como se examinó en el anterior capítulo, la agenda internacional ha incluído 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 decidio 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 amanezas 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 adealantado 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)[18] 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*[19], 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

---

[18] A través del Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), se ha logrado trabajar con varios Equipos de respuesta ante incidencias de seguridad (CSIRT) en la región. Colombia es parte de una red de alerta que proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernética, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente (Consejo, 2016, p.15).

[19] El 11 de septiembre de 2013, como resultado del análisis de la normatividad de Colombia en materia de delito cibernético, el Consejo de Ministros del Consejo de Europa dio su aprobación para invitar a Colombia a adherirse a la Convención sobre delito cibernético. En esa oportunidad, también se abrió la puerta para que fuera parte de su Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. A partir de tal decisión, Colombia tiene un máximo de cinco años para adherir al instrumento internacional (Consejo, 2016, p.15).

> 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[20] 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

[20] Grupo de Respuesta de Emergencias Cibernéticas de Colombia

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[21] viene adelantando el proceso de elaboración del catálogo de infraestructuras críticas

[21] Comando Conjunto Cibernético

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 CIBERDIPLOMACIA COMO HERRAMIENTA DE COOPERACIÓN INTERNACIONAL

3.1 El cambio de lógica de la diplomacia tradicional a la ciberdiplomacia

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 Unión Europea como configurador de 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 La ciberdiplomacia: Una tarea pendiente para Colombia

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.

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.

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.

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 Colombia en atención a la garantía de la ciberseguridad, pues si bien se reconocen importantes avances en el sector (especialmente derivados del Conpes 3864 de 2016), se 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[22], 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.

[22]Se entiende por interméstico aquellos temas que en el contexto de la globalización, contienen dimensiones internacionales y domesticas que interactúan ente sí de múltiples formas (González Carrillo, 2011). En éste sentido, una política interméstica es aquella que tiene lugar en un espacio de 'overlapping' entre políticas exteriores y políticas domésticas dentro de un escenario globalizado (Gress, 1996). De manera similar lo define Bayless Manning quien señala que el término "interméstico" se trata de un neologismo para designar una cuestión que es simultáneamente internacional y doméstica (Manning, 1997).

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.

En síntesis, Colombia debe propender por el fortalecimiento de su estrategia de ciberdiplomacia la cual a su vez debe estar articulada con acciones de orden domestico tendentes a garantizar un ciberespacio seguro.

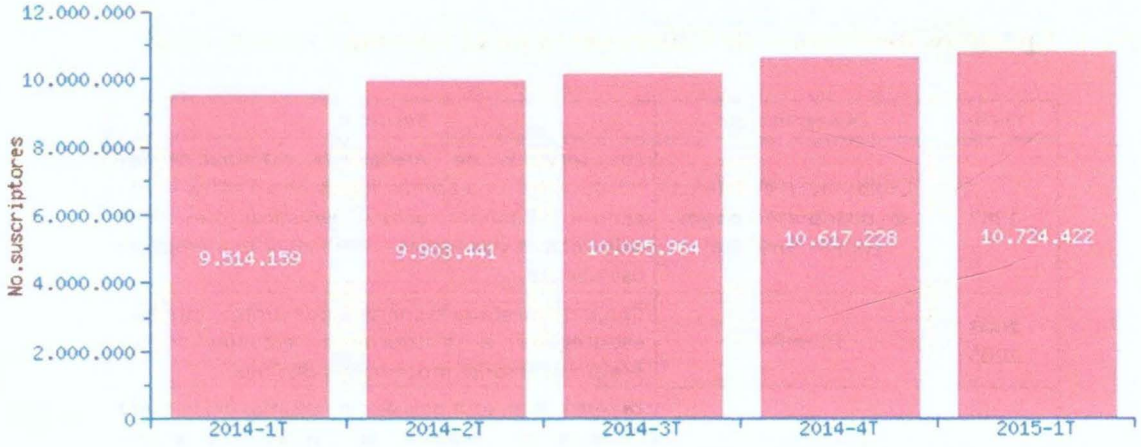
ANEXOS

Anexo 1. Resumen de Estado de Riesgo del Ciberespacio.

AUTORÍA	OBJETIVOS		
	Gobierno	Sector Privado	Ciudadanos
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Privados	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de datos personales
Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	
Impacto	Alto		
	Medio		
	Bajo		

Fuente: Instituto Español de Ciberseguridad, 2012.

Anexo 2. Total de suscriptores de Internet.



Gráfica: Total de suscriptores de Internet
Total Internet-

Fuente:
http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=34#TTC

Gráfica: Total de suscriptores de Internet
Total Internet-

TRIMESTRE	TOTAL	VARIACIÓN
2010-1T	3.309.952	0.00%
2010-2T	3.586.748	7.72%
2010-3T	4.046.997	11.37%
2010-4T	4.384.181	7.69%
2011-1T	5.054.877	13.27%
2011-2T	5.524.069	8.49%
2011-3T	5.907.004	6.48%
2011-4T	6.140.271	3.80%
2012-1T	6.466.167	5.04%
2012-2T	6.657.735	2.88%
2012-3T	7.057.612	5.67%
2012-4T	7.115.944	0.82%
2013-1T	7.531.911	5.52%
2013-2T	8.052.732	6.47%
2013-3T	8.448.331	4.68%
2013-4T	9.061.322	6.76%
2014-1T	9.514.159	4.76%
2014-2T	9.903.441	3.93%
2014-3T	10.095.964	1.91%
2014-4T	10.617.228	4.91%
2015-1T	10.724.422	1.00%

Tabla: Total de suscriptores de Internet
Total Internet-

Fuente:

http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=34#TTC

Anexo 3. Episodios destacados de Ciberguerra en el Sistema Internacional.

Fecha	Denominación	Resumen
1982	Explosión en el sistema de distribución de gas (Unión Soviética)	Los servicios de inteligencia estadounidenses introdujeron una *bomba lógica* en un software de *control* de infraestructuras gasísticas que había sido robado por espías soviéticos a una empresa canadiense
2003 2005	Titan Rain	Conjunto de ataques coordinados contra empresas estratégicas e instituciones estadounidenses presumiblemente procedentes de China
2007	Ciberataque contra Estonia	La retirada en este país de una estatua del período soviético desencadena un conjunto de graves ataques procedentes de Rusia que afectan a las instituciones estatales, bancos y medios de comunicación
2007	Ciberataque contra Siria	La aviación israelí bombardea una instalación nuclear secreta. El ataque aéreo fue precedido de un ciberataque que engañó a los sistemas de defensa aérea e impidió detectar la incursión de los aviones en el territorio sirio
2008	Guerra en Osetia del Sur	De manera paralela al conflicto hubo ciberataques coordinados desde Rusia contra sitios gubernamentales de Georgia que quedaron inutilizados y tuvieron que ser reubicados en servidores de otros países
2010	Stuxnet	Un troyano provoca la destrucción de maquinaria del programa nuclear iraní

Fuente: Torres, 2013

Anexo 4. Marco normativo colombiano en materia de ciberdefensa y ciberseguridad.

NOMENCLATURA	TEMÁTICA
Ley 1480 de 2011	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas.
Decreto Ley 019 de 2012	Racionalización de trámites a través de medios electrónicos. Criterio de seguridad.
Ley 1581 de 2012	Ley estatutaria de Protección de datos personales.
Ley 1623 de 2013	Ley de Inteligencia –Criterios de seguridad.
Ley 1712 de 2014	Transparencia en el acceso a la información pública.
Decreto 2364 de 2012	Firma electrónica.
Decreto 2609 de 2012	Expediente electrónico.
Decreto 2693 de 2012	Gobierno electrónico.
Decreto 1377 de 2013	Protección de datos personales.
Decreto 1510 de 2013	Contratación Pública electrónica.
Decreto 333 de 2014	Entidades de certificación digital.

Fuente: Cárdenas, 2014. Instrumentos Normativos de Ciberseguridad. Certicámara.

Anexo 5. Iniciativas de ciberseguridad según Bases del PND.

Consolidación del Grupo de Respuestas a Incidentes Cibernéticos de Colombia (ColCERT), como ente articulador del gobierno.
Creación y fortalecimiento del Observatorio del Ciberdelito y el Centro de Mando y Control, comunicaciones y Coordinación del Cibercrimen (C4) de la Policía.
Fortalecimiento de la capacidad de protección de las Fuerzas Militares y la Policía de sus propios activos digitales.
Armonización del marco legal con las necesidades en materia de prevención, detección y atención del Ciberdelito.
Creación de los Centros de Respuesta Cibernética Sectoriales (CSIRTs)
Fortalecimiento de los mecanismos de cooperación internacional, propiciando el intercambio de mejores prácticas y de información y la creación de redes de vigilancia y alerta internacionales.

Fuente: Colombia, 2014. Bases del Plan Nacional de Desarrollo: Todos por un Nuevo País. Bogotá. págs. 353-355.

BIBLIOGRAFÍA

Capítulo 1

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.

Feliu, L. (2012). "La ciberdefensa y la ciberseguridad". En: Ministerio de Defensa de España. *El Ciberespacio. Nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa.

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

Capítulo 2

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.

Capítulo 3

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.