IMPORTANCIA DE LA CIBERDEFENSA EN LA INFRAESTRUCTURA CRÍTICA FINANCIERA COLOMBIANA FRENTE A LAS NUEVAS CRECIENTES AMENAZAS CIBERNÉTICAS

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES
CARRERA DE RELACIONES INTERNACIONALES
BOGOTÁ D.C.
2020

IMPORTANCIA DE LA CIBERDEFENSA EN LA INFRAESTRUCTURA CRÍTICA FINANCIERA COLOMBIANA FRENTE A LAS NUEVAS CRECIENTES AMENAZAS CIBERNÉTICAS

CRISTHIAN GUILLERMO BENAVIDES NARVAEZ

DIRECTOR DEL TRABAJO DE GRADO
PROF. EDUARDO PASTRANA BUELVAS PH.D.

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES
CARRERA DE RELACIONES INTERNACIONALES
BOGOTÁ D.C.
2020

Tabla de contenido

Introducción 4

Planteamiento del problema, Pregunta de investigación y objetivos 4

Justificación 6

Metodología 7

1. Marco conceptual 9

1.1. El realismo estructural y la concepción de la ciberseguridad y ciberdefensa 9

1.2. Ciber anarquía y ciber escalado: Las capacidades aumentan en la medida en que nadie tiene control sobre ellas 16

1.3. Ciber-disuasión: Capacidades que previenen de ser atacado 19

1.4. La infraestructura crítica y su vínculo con la ciberseguridad y la ciberdefensa: protección del interés nacional y del funcionamiento del Estado 20

2. Nuevas tecnologías y ciberamenazas: un contexto histórico 24

2.1. Las nuevas tecnologías y su impacto en el Estado 24

2.2. Ciber amenazas internacionales 28

2.3. Ciberseguridad y ciberdefensa, un asunto de la agenda de seguridad de los Estados…. 33

3. Infraestructura crítica financiera colombiana: vulnerabilidades y puntos clave 35

3.1. La infraestructura crítica financiera y su importancia en el Estado colombiano .. 35

3.2. Ataques a la infraestructura crítica financiera colombiana 39

4. Las medidas de ciberseguridad en la Infraestructura crítica financiera colombiana 43

4.1. Medidas tomadas por el Estado colombiano para contrarrestar y superar los ataques a la infraestructura crítica financiera. 43

Conclusiones 48

Bibliografía 49

Introducción

Comprender la ciberseguridad como un ámbito de la defensa de los Estados es crucial en el siglo XXI. El presente trabajo tiene como objetivo resaltar la importancia que tiene justamente la ciberseguridad y la ciberdefensa en un área clave de cualquier Estado: su infraestructura crítica enfocada en el sector financiero.

En este orden de ideas, se eligió a Colombia como caso de estudio para analizar la debida importancia que tiene la ciberdefensa de su infraestructura crítica financiera a la luz de la teoría del realismo estructural, buscando explicar cómo es que surge una necesidad de cada uno de los Estados (y especialmente de Colombia) frente a las nuevas posibles amenazas que vienen no solo de otros Estados con altas capacidades para realizar ciberataques sino también de parte de nuevos actores organizados en el sistema internacional que hoy por hoy son considerados como un tema clave en la agenda de seguridad de la mayoría de gobiernos a nivel mundial. Estos nuevos actores, son especialmente relevantes por sus capacidades de daño a larga distancia sin la posibilidad de un contraataque; a estos grupos a pesar de que se les ha intentado vincular con Estados (en casos como por ejemplo grupos de Hackers vinculados con China, Rusia y Corea del Norte (Reuters, 2020; Semana (2020)), son en su mayoría grupos independientes de hackers o piratas informáticos que actúan por su cuenta y que funcionan en el marco de la criminalidad e incluso algunos cuentan con un trasfondo político.

Ahora bien, a esto se le suma la idea de que en una era moderna la dependencia en redes de comunicaciones y dispositivos electrónicos interconectados y propensos a ser ciber atacados es tal, que un simple fallo o descuido en sus estructuras de defensa puede resultar en un acontecimiento catastrófico para una nación.

Planteamiento del problema, Pregunta de investigación y objetivos

El asunto de la ciberseguridad se ha posicionado de manera clave en la agenda de la mayoría de los países a nivel mundial, pues el desarrollo de las nuevas tecnologías de la comunicación ha causado una mayor dependencia en los procesos de funcionamiento del Estado hasta el

punto donde existe una dependencia completa del adecuado funcionamiento de sus redes de comunicación y de transmisión de información.

En este orden de ideas, y teniendo en cuenta que los Estados, y más aún las grandes potencias, han empezado un escalamiento en cuestiones de ciberdefensa se hace fundamental preguntarse por la importancia que tiene para el resto de los Estados, y para este caso en específico, para Colombia.

Al ser la infraestructura crítica la mayormente vinculada con ciberseguridad y ciberdefensa, posicionándose específicamente en la infraestructura crítica financiera, la cual se ha vuelto recientemente un pilar importante para el manejo de las inversiones nacionales a extranjero y viceversa, además de que es la puerta de comunicación entre Colombia y los mercados internacionales, el tema recobra una fuerte importancia que deriva en la siguiente pregunta de investigación.

Pregunta de Investigación

¿Por qué es importante la ciberdefensa de la infraestructura crítica financiera del país de cara a las nuevas crecientes amenazas cibernéticas?

Objetivos.

Objetivo general:

Sustentar la importancia que tiene la ciberdefensa de la infraestructura crítica financiera en Colombia frente a las nuevas ciber amenazas

Objetivos Específicos:

1. Formular un marco conceptual que permita explicar las definiciones principales acerca de lo que es la Ciberdefensa y su importancia general

2. Desarrollar un contexto histórico conceptual de las nuevas tecnologías y las nuevas ciber-amenazas

3. Identificar y argumentar el estado de la vulnerabilidad que podría tener, en términos cibernéticos, la infraestructura crítica financiera colombiana

4. Identificar e interpretar las medidas adoptadas por el Estado colombiano frente a las nuevas amenazas cibernéticas en términos de ciberdefensa.

Justificación

El trabajo apunta a realizar una investigación frente a la importancia que tiene la ciberseguridad en la agenda de Colombia teniendo en cuenta el riesgo que representa a nivel internacional y se enfoca específicamente en ver cuáles son las medidas que el país ha adoptado respecto a la protección de la infraestructura crítica financiera.

La investigación aporta un nuevo enfoque frente a la comprensión de las prácticas de ciberseguridad en Colombia y aporta análisis frente a su importancia, sus posibles vulnerabilidades y, más allá, ofrece una mirada frente a las medidas tomadas por Colombia para proteger su infraestructura crítica financiera. El trabajo, se apoya teóricamente sobre argumentos de realismo estructural que apuntan a la necesidad de tener capacidades de seguridad y defensa, además de plantear en contexto del ciberespacio como un lugar totalmente anárquico donde no se ha definido una "gobernanza" ni unos principios base de actuación para todo tipo de actores, pues además de Estados, las amenazas también provienen de otros grupos organizados.

Finalmente, esta investigación puede brindar una aproximación hacia la idea de si Colombia se encuentra a la par de las amenazas internacionales y si esto realmente se traduce en una confianza de funcionamiento del sistema financiero y en capacidades de respuesta para proteger la infraestructura crítica de este.

Metodología

El presente trabajo, se fundamenta en un estudio cualitativo frente a la importancia que ha tenido para los Estados el construir capacidades de ciberseguridad y ciberdefensa, donde a partir del análisis de diversos autores, especialmente aquellos enfocados en realismo estructural además de otras fuentes secundarias como artículos y textos relacionados con el impacto de la ciberseguridad en el Estado, así como un par de análisis de expertos frente a cómo debería ser la relación entre privados y el Estado; con esto se buscó construir un contexto general de ciberseguridad y ciberdefensa.

Ahora enfocándose en el desarrollo del trabajo, el primer objetivo se buscará desarrollarlo a partir de los planteamientos formulados por John Mearsheimer, así como los plateados por Huth, Gelpi y Bennett, los cuales permiten por medio del realismo estructural explicar cómo la concepción de amenaza en el sistema internacional ha motivado a que los Estados desarrollen capacidades para protegerse teniendo en cuenta las cinco "bedrock asumptions" planteadas por este autor.

Con este análisis se pretende demostrar que se ha vuelto una necesidad el desarrollo de capacidades de todo tipo, no solo militares materiales sino también de infraestructura en temas de ciberseguridad, y más aún si el ciberespacio se ha convertido en un espacio de anarquía completa, de la misma forma en que el texto de Huth *et al* permite hacer una aproximación conceptual de distintas características propias del sistema internacional que concibe el realismo estructural y como estas funcionan como instrumento de análisis para comprender el escalado de ciber capacidades en el sistema internacional.

Todo esto, además, se complementa con la introducción de 4 términos claves para el desarrollo del trabajo: Ciber anarquía, ciber escalado, ciber disuasión e infraestructura crítica que permiten explicar de mejor forma cuál es el contexto y el vínculo que existe entre estos términos y la forma como los Estados han decidido prepararse en este campo. Estos cuatro términos fueron retomados de distintas fuentes secundarias principalmente de autores especializados que brindaron una contextualización de cada término; de la misma manera hay que decir que son claves para explicar más adelante el contexto colombiano.

El realismo ofensivo entonces, permite en un primer momento explicar la situación actual de como se está desenvolviendo un nuevo escalamiento, sin embargo, es de tener en cuenta que las principales amenazas no solo provienen entre Estados, sino que vienen de actores no estatales que están desarrollando importantes capacidades que son de tener en cuenta en el desarrollo del tema.

El segundo objetivo se fundamenta en diversas fuentes secundarias y textos referentes a los retos que tiene el Estado frente a la implementación de las nuevas tecnologías, así como textos que hablan puntualmente de las nuevas ciber amenazas, así como varios ejemplos de estas amenazas. Todos estos textos ofrecen diversas perspectivas y se analizará como el Estado moderno ha desarrollado un estrecho vínculo con las tecnologías de la información y la comunicación.

El tercer objetivo del trabajo retomará entonces diferentes trabajos presentados tanto por entidades privadas que forman parte del sistema financiero colombiano como del sector público mediante los cuales se retomaron datos frente a las principales amenazas percibidas y cuáles han sido las medidas que se han tomado para fortalecer el sistema financiero de las amenazas cibernéticas, con esto se procederá entonces al estudio del caso Colombiano, donde se buscara en primer lugar hacer un análisis de cara a como está estructurada la ciberseguridad y la ciberdefensa en el sistema financiero Colombiano, con ello entonces se buscará presentar cifras y datos respecto a los diferentes ciberataques que ha sufrido este para posteriormente hacer un recuento de cómo tanto el Estado como la empresa privada, la cual es clave para comprender el sistema financiero Colombiano, han tomado medidas para enfrentar este tipo de amenazas.

Para el estudio de caso que es la infraestructura crítica financiera colombiana se retomaron varias fuentes primarias como lo son diferentes reportes de entidades perteneciente al sector financiero en Colombia, así como los documentos CONPES 3995 y 3701, mediante los cuales se buscó interpretar las respuestas a las amenazas en ciberseguridad y ciberdefensa, enfocándose en cómo han protegido la infraestructura crítica financiera y cuáles son las medidas implementadas.

El presente trabajo entonces se divide en cuatro partes, la primera donde se abordará la idea de la necesidad de construcción de capacidades de ciberdefensa en el marco del realismo estructural, así como se abordarán e introducirán tres conceptos claves para comprender tanto el tema como el contexto actual, los cuales son ciber anarquía, infraestructura crítica y ciberseguridad. En la segunda, se abordará una contextualización acerca del impacto de las nuevas tecnologías en el funcionamiento del Estado, así como sus amenazas, las medidas adoptadas y la situación actual del ciberespacio como un activo clave y como un campo de batalla también.

La tercera parte, abordará un análisis del caso colombiano para constatar cuáles son las capacidades de este en cuánto a ciberdefensa ya aplicada al tema de infraestructura crítica financiera, de la misma forma se hará una revisión acerca de las cifras de ciber ataques que Colombia ha recibido en su sistema financiero y cuál ha sido la respuesta estatal y de parte del sector privado.

Finalmente, la última parte se encargará de realizar el análisis de cuáles son las medidas que ha tomado Colombia para proteger su infraestructura crítica financiera a partir del análisis de los ataques recibidos, así como se mostrar cómo el Estado colombiano ha tomado medidas al respecto para fortalecer las capacidades de ciberdefensa en este ámbito. En la última parte del trabajo se presentarán las conclusiones.

1. Marco conceptual

1.1. El realismo estructural y la concepción de la ciberseguridad y ciberdefensa

La tradición realista para comprender al sistema internacional tradicionalmente ha apuntado hacia un tema fundamental: la supervivencia del Estado nación, entendida como la razón de Estado. Actualizándolo al siglo XXI, las variables a tener en cuenta para lograr esta supervivencia se actualizan a las nuevas tecnologías y especialmente a los nuevos teatros de operaciones donde resalta de manera clara el ciberespacio, comprendido de la manera como

lo explica Maughan (2010, Pp. 29) quien dice que : "cyberspace is the complex, dynamic, globally interconnected digital and information infrastructure that underpins every facet of society and provides critical support for our personal communication, economy, civil infrastructure, public safety, and national security".

El primer punto para tener en cuenta es que como menciona Mearsheimer (2001), "the claim that security competition and war between the great powers have been purged from the international system is wrong. Indeed, there is much evidence that the promise of everlasting peace among the great powers was stillborn." (Pp. 25).

Lo planteado entonces por Mearsheimer, apunta a que bien existe una competencia de seguridad y guerra entre los Estados, más específicamente entre los grandes poderes, una competencia que se traslapa al ciberespacio, y que impulsa a los Estados en una constante competencia de superioridad armamentística, que, para el caso, se reduce a capacidades de ataque y defensa orientadas a la infraestructura del Estado, que para el siglo XXI, se ve identificado como parte de sus redes informáticas y de comunicación.

Kating-Borland (2012) de la mano con lo que explica Mearsheimer dice que:

> A cyber-attack can occur at any time and may not always be associated with political or economic activities or any actual military operations. Additionally, because identity can be concealed so easily online, it is unlikely that the source of an attack will be readily apparent. (Pp. 4)

En este orden de ideas, en un enfoque realista, el ciberespacio se ha convertido en una prioridad de los Estados para proteger sus intereses y su integridad, Kating-Boland (2012, Pp 6) en su texto "Cyberwar: A Real and Growing Threat" incluso retoma una frase clave que menciona Ene Ergma, Speaker del parlamento estonio la cual reza que "Like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything".

Esto presenta una idea de cuan real puede ser considerada esta situación, y como esta misma preocupación ha llevado a un escalamiento armamentístico y de defensa en cuestiones de ciberseguridad.

De esta forma, el ciberespacio puede ser considerado como un nuevo campo de guerra donde los Estados han venido construyendo nuevas capacidades de poder, sin embargo, a diferencia de otras situaciones de escalamiento similares, como por ejemplo la Guerra Fría, el desarrollo de capacidades en ciberseguridad y ciberdefensa no requieren de recursos físicos tan especializados como el caso del escalamiento nuclear a mediados del siglo XX; por supuesto requieren de recursos humanos y de un presupuesto considerable, cosa que es clara cuando se analizan las capacidades de "ciberguerra" que tienen grandes potencias como China o Rusia comparadas con las capacidades del resto de naciones.

Ahora bien, hay un segundo punto expuesto por Mearsheimer, y que funcionaría en cierto sentido para explicar cómo funciona la ciberdefensa actualmente, este es su concepción de la política internacional, para ello, este dice que:

> […] international politics has always been a ruthless and dangerous business, and it is likely to remain that way. Although the intensity of their competition waxes and wanes, great powers fear each other and always compete with each other for power. The overriding goal of each state is to maximize its share of world power, which means gaining power at the expense of other states." (Mearsheimer, 2001. Pp 27)

Lo que dice Mearsheimer, entonces, es que existe una competencia que, aunque en cuestiones críticas (ya sea crisis diplomáticas, hipótesis de guerra y demás) aumenta y disminuye, sin embargo, fuera de estas situaciones sigue existiendo un "miedo" de unos frente a otros Estados y sus capacidades, que se traduce en una competencia de poder donde cada Estado busca maximizar sus capacidades para protegerse de amenazas latentes y en cierta forma como un medio de participación en el poder mundial, proyectando influencia y especialmente capacidad de poder duro a otros Estados.

De la mano con Mearsheimer, Huth, Gelpi y Bennett (1993) presentan una serie de elementos claves que permiten comprender como el realismo estructural se enfoca en los atributos propios del sistema internacional y desde este estos se puede explicar también el escalado de capacidades en ciberdefensa. Los autores mencionan que particularmente el realismo estructural hace énfasis en "resolver y relativizar las capacidades militares de los Estados

adversarios", dando a entender que la construcción de capacidades se basa fuertemente en los atributos propios con los que cuenta el sistema internacional.

Los autores en su texto si bien presentan un análisis acerca de cómo el realismo estructural, de la mano con la teoría de la "rational deterrence" o disuasión racional, funciona para analizar el escalamiento de los conflictos entre Estados, ofrecen una serie de características importantes para comprender la visión del realismo estructural del sistema internacional y permiten conectar estas ideas con el tema del escalamiento de capacidades militares, para ello, se retoman cuatro puntos importantes.

El primero de estos elementos se trata de la Estructura del Sistema Internacional. Lo primero entonces es la idea de que existe un sistema autocontenido también puede ser visto como un grupo de unidades que interactúan y son interdependientes, donde el "orden" de las unidades dependerá de los recursos de poder de cada uno y a su vez la estructura del sistema se formará en base a los acuerdos y vínculos que se formen entre todas sus unidades; este sistema se prestará entonces para que los Estados o unidades desarrollen patrones comportamentales propios. (Huth *et al*, 1993. Pp 609)

En este orden de ideas los autores mencionan que a pesar del desacuerdo general de esta definición generalizada de la Estructura del sistema, complementan algunas ideas y debates frente a como se debería considerar este, donde se incluyen y retoman las concepciones de Waltz, quien menciona que los sistemas internacionales se distinguen en base a la cantidad de grandes potencias existentes, ya sea bipolar (dos grandes potencias) o multipolar (tres o más), las concepciones de Thompson quien adiciona la idea de que además del número de grandes potencias existentes, es importante tener en cuenta la distribución de capacidades; junto con esto, está también la idea de Deutch y Singer en Huth *et al*, (1993. Pp 610) quienes también adicionan que las alianzas y coaliciones son también parte fundamental para comprender cuál es la Estructura del sistema internacional.

Ahora bien, comprendiendo la idea del sistema en sí, se resalta la segunda parte y es la incertidumbre que existe al interior del sistema, la cual Huth *et al.* (1993, Pp. 610) definen como "la confianza que los tomadores de decisiones tienen en sus estimaciones del resultado

esperado de un conflicto armado resultante de las características de la estructura del sistema". La incertidumbre se considera con base en qué tan bien los tomadores de decisiones conocen el sistema, las capacidades de las otras unidades y la respuesta esperada (victoria, derrota o empate), con esto en mente, cuando hay un nivel relativamente bajo de incertidumbre las decisiones se tomarán con mayor seguridad pues hay una relativa confianza frente a la respuesta de los otros actores del sistema.

El tercer punto entonces apunta a la propensión del riesgo, y esta se refleja en el hecho de que diferentes individuos pueden tomar diferentes decisiones basados en sus atributos hacia los resultados probabilísticos. Este punto básicamente se resume en que, basado en las estadísticas y en las probabilidades los tomadores de decisiones pueden estar dispuestos a tomar decisiones más o menos riesgosas. La propensión al riesgo tiene un vínculo interesante por supuesto con la incertidumbre del sistema, y es que se podría llegar a pensar que entre mayor sea la incertidumbre por supuesto menor será la propensión al riesgo, pues las reacciones a cualquier decisión que se tome pueden ser mucho más radicales o agresivas de lo esperado. (Huth *et al,* 1993. Pp 610)

Finalmente, el cuarto punto explicado por los autores es el de "deterrence" o disuasión, la cual definen como: "a policy that seeks to persuade an adversary, though the threat of military retaliation, that the costs of using military force will outweigh the benefits" (Huth 1988, Pp.15 retomado por Huth *et al*¸1993. Pp 610).

El concepto de disuasión cobra especial importancia a la hora de comprender que es la amenaza del uso de capacidades militares superiores y más poderosas que causarían más pérdidas que beneficios a quien las desafíe, lo que hace que los Estados se interesen en construir capacidades mayores en orden de evitar ser atacados.

Estos cuatro puntos entonces recogen una idea frente a como se concibe la estructura del sistema internacional en el enfoque del realismo estructural, y nos presentan puntos importantes de cómo es que cada unidad (o Estado) se interesa por desarrollar capacidades de defensa basado primero, en la existencia y cantidad de grandes potencias, segundo en la incertidumbre y tercero en la propensión al riesgo. El resultado entonces de una política de

disuasión surge de estos tres puntos y el resultado es que hay una preocupación real y existente de que cuando se tome una decisión habrá una respuesta, la cual es incierta y en dado caso se debe estar preparado para responder.

Esta situación vista desde el enfoque de ciberseguridad y ciberdefensa se reflejaría primero en la premisa de la existencia de una asimetría en cuestión de capacidades frente a las grandes potencias respecto al resto del mundo, y esto se hace presente en la política disuasiva de las grandes potencias que entre ellas han dejado claro que la ciberguerra es una posibilidad y que están preparados para defenderse y para atacar, esta situación en particular es lo que impulsa a que todos los Estados contemplen la importancia de implementar capacidades propias en el área y a pesar de que no sean comparables con las de los Estados más grandes, entra en juego la descripción de la estructura del sistema, donde las alianzas y los patrones comportamentales definirán qué tan amenazado se siente un Estado de otro, o incluso qué tan amenazado se siente un Estado de un actor internacional con ciertas capacidades ofensivas.

El mismo sistema, sin embargo, ha buscado proponer varias maneras de concebir al ciberespacio de manera equilibrada en cuanto a condiciones de capacidades para justamente evitar un escalamiento, pero ninguna se ha logrado imponer, ya que la importancia que han cobrado las estructuras de redes de comunicación e información al interior de los Estados yace en el núcleo de su defensa nacional, que es, a su vez, parte de lo que se consideraría su propia "razón de Estado. Por ello, el ciberespacio se sigue considerando un espacio anárquico sin unas regulaciones internacionales claras o establecidas frente a cómo proceder o a los límites o alcances que tiene cada Estado a la hora de construir infraestructura de defensa o contraataque cibernética, a esto se le suma el argumento de que existen nuevas amenazas no convencionales que no son necesariamente Estados, pero que representan un peligro latente a su infraestructura crítica.

Continuando con la idea, Mearsheimer argumenta que bien las grandes potencias siempre están buscando poder para convertirse en hegemonías o incluso para retar la existente, y para ello plantea 5 "bedrock assumptions" que permitirían explicar por qué llegan a ser "agresivos en la búsqueda del poder".

La primera es la existencia de un sistema internacional anárquico, que no es caótico per sé. Por sí misma la noción realista apunta hacia un mundo caracterizado por una constante competencia de seguridad con el fin de "estar protegidos frente a una guerra", definición que concuerda con las características de la estructura del sistema que como mencioné anteriormente Huth *et al* (1993) considera en el marco del realismo estructural. .

La segunda es que las grandes potencias inherentemente poseen capacidad ofensiva militar lo que les da la posibilidad de causar daños importantes o incluso destruirse unos con los otros, la tercera apunta a que los Estados nunca podrán estar seguros frente a las intenciones de otros Estados, y que nadie en todo el sistema internacional tiene la certeza de que otro Estado no usará sus capacidades ofensivas militares para atacar a un primer Estado. (Mearsheimer, 2001 Pp. 29-30)

La cuarta apunta a la supervivencia como el principal objetivo de grandes potencias, y explica además que específicamente los Estados buscan mantener una territorialidad integral y la autonomía del poder doméstico, asimismo la supervivencia domina otras motivaciones, porque una vez un Estado es conquistado, es poco probable que se enfoque en buscar otros objetivos. Finalmente, la quinta establece que las grandes potencias son actores racionales, están conscientes del ambiente exterior y piensan estratégicamente frente a como considerar sus propias preferencias respecto al comportamiento de otros Estados, e incluso consideran como su propio comportamiento puede afectar el comportamiento de los otros Estados y prestan especial atención al largo plazo tanto como a las consecuencias inmediatas de sus acciones. (Mearsheimer, 2001 Pp. 30-31).

De estas 5 "assumptions" de Mearsheimer, se puede interpretar la construcción de, primero, una anarquía en el ciberespacio, donde nadie por encima de nadie puede decidir sobre normatividades o acciones agresivas de otros Estados en el mismo (idea que Kello (2017, Pp 213) presenta), y más allá de condenarlos si es demostrada la culpabilidad, cuestión que se vuelve complicada debido al tipo de conflicto que la ciberguerra representa, la alternativa que queda es fortalecer sus propias capacidades.

Segundo, debido a que ningún Estado puede dar por sentada la actuación de otro o el uso de la fuerza de su parte, cada uno se ha preparado individualmente para enfrentar lo peor y precisamente para proteger sus propios intereses, traducido a ciberseguridad, esto se ve reflejado, de nuevo, en el crecimiento del interés tanto de las grandes potencias como de los demás Estados en sus políticas de ciberseguridad y ciberdefensa, mientras que los países más pequeños y menos desarrollados se ven replegados a adoptar las medidas que pueden en función en que consideran esto como una amenaza.

1.2. Ciber anarquía y ciber escalado: Las capacidades aumentan en la medida en que nadie tiene control sobre ellas

Ahora bien, el hecho de comprender el Sistema Internacional, tan intercomunicado y sofisticado del siglo XXI requiere comprender también el funcionamiento de las nuevas redes, del internet y del papel tan importante que desempeña en funcionamiento de cada uno de los Estados, pues toda la teoría que se viene explicando anteriormente deriva en que las amenazas han trascendido más allá de las capacidades armamentísticas convencionales y ha surgido la necesidad de construir capacidades de respuesta en defensa y ataque cibernético

Inicialmente, para comprender como ha evolucionado el sistema de gobernanza en la nueva estructura del sistema internacional, Kello (2017 Pp. 205) presenta una serie de elementos fundamentales bajo los cuales la gobernanza bajo condiciones de anarquía internacional (de la mano con la teoría del realismo estructural) funciona.

El primero de estos apunta a que esta no emerge de manera natural, y que bien es una variable que recae en la existencia de tres factores fundamentales, el primero es el acuerdo alrededor de los enfoques problemáticos, cuyas soluciones son un mérito de atención colectiva que se opone a aquellas unidades que planean tomar decisiones de manera unilateral, el segundo, es una variedad de prioridades básicas entre los "jugadores", ya que si sus preferencias chocan y la complementariedad de intereses es débil, la existencia de una amenaza o problema urgente será garantía de contención más no de cooperación y, por último, el tercero es la existencia de instrumentos institucionales adecuados, bien sean formales o informales, que clarifiquen monitoreen y si es necesario refuercen el comportamiento necesario para aliñarse

a las prioridades compartidas, y solamente cuando estos tres factores se presenten es posible hablar de la existencia de una gobernanza "estable", que a fin de cuentas sería un modo de conducta regularizada donde las unidades aceptan unos principios sobre qué es legítimo y qué no, además de que establecen que la violación de estos significaría una ruptura el mismo orden internacional. (Kello 2017 Pp. 205)

Todos estos principios o factores precursores de la gobernanza global han sido difíciles de mantener en la era del "ciber dominio", pues los grandes Estados están en desacuerdo en qué asuntos de la ciberseguridad realmente merecen una "solución multilateral", en este orden de ideas el primer concepto explicativo es la "ciber anarquía". Kania menciona en una primera aproximación al término que ciertos aspectos técnicos del dominio cibernético, como su actual dominio delictivo, constituyen desafíos más objetivos, así como respuestas de los Estados-nación a la percibida "ciberanarquía" la cual se ha visto agravada por la falta de normas establecidas o marcos legales para constituir un ciberespacio coherente orden (Kania, 2016. Pp. 1)

En este orden de ideas, Kania presenta un punto bastante importante y es que esta "ciber anarquía" está "exacerbada" por la falta de normas o marcos legales establecidos para construir lo que pueda ser considerado como un ciber orden y en este punto precisamente es que yace el principio de anarquía dentro de lo Wendt consideraría en su famosa frase "Anarchy is what states make of it: the social construction of power politics" (Retomada por Kania, 2016 de Wendt, 1992), y es que justamente Kello explica que esta situación está presente en el mundo, pues el consenso dividido en torno a la regulación de la guerra cibernética es más prominente que nunca, enfatizado por la falta de acuerdo y cooperación entre los estados, el derecho internacional y las instituciones sobre la gobernanza cibernética global. (Kello, 2017, p.212)

Con eso que explica Kello, la regulación de la "ciber warfare" están dividida sin lograr llegar a un acuerdo común, pues a pesar de que el fenómeno del internet y especialmente el debate frente a la regularización del uso del ciberespacio, no solo en términos militares sino civiles y el debate jurisdiccional viene desde hace más de 20 años, como lo hace evidente Goldsmith en su publicación titulada "against ciberanarchy" en 1999, donde explica que hay un conflicto

jurisdiccional frente a como se debe entender las acciones en el ciberespacio y cómo existe un debate de los que denomina como “escépticos”, quienes según este autor afirman que la aplicación de concepciones geográficas de regulación legal y elección de la ley a una actividad del ciberespacio geográfico no tiene sentido o conduce a una confusión irremediable. (Goldsmith, 1999. Pp. 1200)

Encontramos entonces que esta idea, de una ciber anarquía sustentada en el realismo, ofrece un punto de inicio para el desarrollo del marco conceptual y se posiciona como el primer concepto fundamental del trabajo. Todo ello entonces, nos permite comprender que el precedente de la inexistencia de un control multilateral, así como la ausencia de una serie de amenazas concebidas de manera conjunta por los Estados, junto con la dificultad de regular de forma legal y territorial las acciones en el ciberespacio, ha provocado lo que definen Jensen y Valeriano (2019) como “Cyber escalation”

Jensen y Valeriano plantean entonces que se está presentando una nueva carrera armamentísta no regulada (en parte también por las razones mencionadas anteriormente), que además implica una combinación de señales de dominio cruzado abiertas y encubiertas que los Estados utilizan para gestionar la escalada y brindar opciones que podrían ayudarlos a promover sus intereses en caso de un conflicto. (Jensen y Valeriano, 2019. Pp. 2)

Además de ello, es importante retomar también la idea de que las operaciones cibernéticas tienden a ofrecer rampas de salida escalonadas de las grandes potencias en la misma medida en que proporcionan mecanismos de señalización que han permitido a los Estados moldear el comportamiento de un adversario sin involucrar a las fuerzas militares y sin correr el riesgo de una escalada militar y es que a pesar de la incertidumbre en torno a cómo los Estados les dan uso las nuevas tecnologías para fines estratégicos, las operaciones cibernéticas han mostrado una tendencia a estabilizarse y brindan opciones para evitar conflictos costosos y prolongados. (Jensen y Valeriano, 2019. Pp. 4)

Por otro lado, como mencionan Jensen y Valeriano, el desarrollo de capacidades en ciberseguridad tiene como premisa una serie de requerimientos que los autores explican forma parte también del escalamiento, pues como explican Jensen Y Valeriano (2019, Pp 6)

las operaciones cibernéticas requieren una inversión en redes, infraestructura y capital humano o sumas de dinero suficientes para comprar capacidad en el mercado negro, pues estas operaciones son instrumentos complejos del arte de gobernar que los actores de la política exterior integran con otros instrumentos de poder diplomáticos, informativos, militares y económicos.

Los autores complementan la idea diciendo que una combinación de estos instrumentos envía una señal clara a los estados rivales. Por lo tanto, las operaciones cibernéticas pueden ayudar a estabilizar la competencia entre grandes potencias en el siglo XXI. (Jensen Y Valeriano 2019, Pp 6)

Esta inversión de la que hablan, claramente se da en la medida en que cada Estado considera que tiene una amenaza inminente de ser atacado, y en la medida en que considera que al interior del propio sistema hay una fuerte incertidumbre en la construcción de capacidades que pueda representar un riesgo o un desbalance de poder. Con esto que mencionan los autores, se puede hablar entonces de que hay un aumento de las capacidades y hay un interés estratégico en construir capacidades de ciberdefensa, y si tenemos en cuenta los elementos de la teoría realista estructural que se ha venido planteando en el desarrollo del marco conceptual, encontraremos que se puede inferir que este escalamiento es también resultado de la estructura del sistema internacional, la presencia de múltiples potencias y de Estados rivales que representan una amenaza (por ejemplo: China, Rusia, Irán, Corea del Norte frente a Estados Unidos), así como el surgimiento de otro tipo de actores, como grupos organizados de hackers, con bases en diferentes partes del mundo y con capacidades de atacar en cualquier momento las vulnerabilidades de los Estados y de las empresas privadas, han aumentado la incertidumbre de forma considerable frente a un ataque en cualquier momento.

1.3. Ciber-disuasión: Capacidades que previenen de ser atacado

Por otra parte, Reardon & Choucri (2012) en Craig y Valeriano (2018) complementan esta perspectiva y la vinculan también con la teoría realista, e incluyen de nuevo el concepto de disuasión o “deterrence”, pues mencionan que las teorías realistas de disuasión, gestión de crisis y conflictos pueden utilizarse para comprender si el ciberespacio se está estabilizando

o desestabilizando, si las tecnologías cibernéticas serán una nueva fuente de conflicto o de paz, y si los estados participarán en carreras de armas cibernéticas.

En este orden de ideas, el análisis desde la perspectiva realista cobra aún más sentido para explicar las nuevas situaciones de ciber guerra. Craig y Valeriano (2018) cuentan además que, con la proliferación de la información de las tecnologías de la información y la comunicación, la ciberseguridad se ha convertido en un "tema de primer nivel" para policy-makers, así como un tema relevante y de gran interés para académicos de las relaciones internacionales. Se hace evidente como el realismo ofrece herramientas para comprender el ciberespacio, inicialmente como un espacio anárquico, pero también como otro escenario de actuación de los Estados, el cual no tiene un mismo control como lo sería las intervenciones militares o incluso económicas. Con todo ello, el realismo entonces ofrecería herramientas para considerar que la protección de la infraestructura crítica, cualquiera que fuese, de cualquier estado, va más allá de un sistema de gobernanza y es comprendida como una carrera individual por protegerse de otros Estados u actores con capacidades de incluso impedir el normal funcionamiento de otro Estado.

1.4. La infraestructura crítica y su vínculo con la ciberseguridad y la ciberdefensa: protección del interés nacional y del funcionamiento del Estado

Ahora bien, ahondando en directamente el significado de la Infraestructura crítica, el cual es un concepto transversal de todo el trabajo, López *et al* (2012) explica que:

> Modern societies depend on the continuous and reliable availability of several services and are at risk of severe economic impacts or loss of life and limb if such products and services are disrupted or unavailable in a larger region for a significant length of time. These services are those provided by the so-called *critical infrastructures* (CI).

La definición de los autores lleva entonces a considerar primero, que nos encontramos en una sociedad primeramente dependiente de la continua confianza frente a la disponibilidad de variados productos y servicios y segundo, que aquello que nos brinda o presta esos productos y servicios es considerado en ese orden de ideas como "infraestructura crítica". Esta

definición es de principal utilidad tanto en el desarrollo del marco conceptual, así como será necesario retomarla al momento de presentar la explicación de cómo se relacionan los términos de manera directa con la ciberseguridad más adelante. Aun así, la definición va más allá, los autores ahondan en la idea de que los riesgos relacionados a esta llamada "infraestructura crítica" comienzan desde la pieza más pequeña y simple y su probabilidad de que sea modificada, atacada o simplemente falle.

En primer lugar, es pertinente presentar lo mencionado por Kramer y Butler quienes explican la importancia que tiene defender la infraestructura crítica y los recursos claves de cualquier Estado, mencionando que:

> The critical infrastructure and key resources (CIKR) that support the foundation of society and how we live, work, and survive. These include energy, especially the electric grid, and oil and gas pipelines; finance; telecommunications; transportation, particularly air, rail, and maritime; and water and wastewater treatment. Disruption of any of these could have significant cascading effects on the economy (2019, Pp. 5)

López *et al* y también Benkler (2006) también explican que la construcción moderna de infraestructura crítica ha recaído en sistemas electrónicos o de almacenamiento y manejo de la información, porque simplemente hacerlo de otra forma es ineficiente y riesgos, además de que de otra forma no es posible tomar medidas en caso de ataque. López *et al*, comenta entonces que la misma concepción de infraestructura crítica está dividida en varios sectores, mientras que la composición precisa de esta varía tanto en el análisis que se le esté dando como en el enfoque bajo el cual se esté estudiando.

El vínculo entonces entre las Tics y la infraestructura crítica empuja al desarrollo de un tercer concepto que surge en el desarrollo y la protección de esta: la ciberseguridad. Para esta definición Kshetri (2016) retoma de Choucri (2012):

> CS involves technologies, concepts, policies, processes, and practices used to protect assets (e.g., computers, infrastructure, applications, services, telecommunications systems, and information) and the cyber environment from attack, damage, and

> unauthorized access (ITU 2008). From a nation's perspective, put simply, CS is the "ability to protect itself and its institutions against cyber-threats."

Esta definición en particular incluye varios puntos importantes, tecnologías, conceptos, políticas, procesos y prácticas, y es útil entonces para aplicar directamente al caso colombiano, pues con esta definición será posible definir qué decisiones o que información más detallada hace parte efectivamente del programa o de la iniciativa en ciberseguridad del país. En este orden de ideas, la definición de Kshetri cobra fuerza también para centrar que las amenazas en tres puntos importantes: Ataque, daño y acceso no autorizado, y simplifica al final diciendo que es para la nación simplemente la habilidad de protegerse a sí misma y sus instituciones contra las ciber amenazas.

Craigen, Diakun-Thibault y Purse (2014. Pp. 1) explican por otro lado que el término "ciberseguridad" es ampliamente utilizado y cuenta con definiciones son muy variables, que a menudo son subjetivas y, en ocasiones incluso llegan a ser poco informativas.

Craigen *et al* (2014. Pp. 1) mencionan también que la ausencia de una definición concisa y ampliamente aceptable que capture la multidimensionalidad de la ciberseguridad obstaculiza los avances tecnológicos y científicos al reforzar la visión predominantemente técnica de la ciberseguridad al tiempo que separa las disciplinas que deberían actuar en conjunto para resolver los complejos desafíos de la ciberseguridad.

La complejidad de definir este término y las múltiples formas de definirlo son también un factor clave a la hora de estudiar fenómenos relacionados con esta, y está claro que, para abordar los desafíos más complejos del tema, aclararla es un punto bastante importante. Estos autores, en un segundo punto explican además que los desafíos relacionados con las dimensiones organizativas, económicas, sociales, políticas y otras dimensiones humanas que están fuertemente vinculadas a los esfuerzos de ciberseguridad, e incluso presentan una definición que a su vez retoman de Friedrick Chan, ex director de investigación de la Agencia de Seguridad Nacional en los Estados Unidos, quien menciona que:

> A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about

> an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed. (Chan 2012, en Craigen *et al,* 2014. Pp. 2)

Justamente esta interdisciplinariedad es lo que le da al término la posibilidad de ser estudiado desde distintos ámbitos, incluyendo el de las relaciones internacionales. Con ello, comprendemos que este concepto en sí mismo aborda distintas áreas del funcionamiento del Estado y de la vida diaria, cuya protección se ha vuelto una necesidad en el marco de la dependencia del funcionamiento de las redes de datos y de computación.

Ya introducidos los tres conceptos completamente claves para desarrollar el marco conceptual del trabajo, ciber anarquía, infraestructura crítica y ciberseguridad y comprendidos dentro del marco del realismo estructural, hay un punto de partida desde dónde será posible presentar, primero la comprensión a nivel estatal, donde se entrecruzan las tres definiciones con el propósito de defensa nacional, y segundo, es posible comenzar a centrar la importancia que tienen estas definiciones a la hora de comprenderlas a nivel sistémico y en particular para Colombia en los objetivos que se desarrollarán más adelante.

Más precisamente para Colombia, qué será el tema central, hay que interpretar como en el marco del interés de las grandes potencias por temas del ciberespacio, este tema puede convertirse también en parte de la agenda de seguridad y a pesar de no tener las mismas capacidades, puede comprender que también existe una vulnerabilidad que impulse a proteger su infraestructura (especialmente la crítica) con políticas públicas propias orientadas, quizá, no al ataque de otros Estados, pero si a la defensa contra actores no estatales con capacidades de hacer daño considerable a su infraestructura, cosa que en capítulos posteriores se resaltará.

Con todo ello, es posible cerrar el marco conceptual, concluyendo que el tema de la ciberseguridad y la ciberdefensa, comprendida desde un realismo estructural, se ha convertido en un tema que hace parte de la agenda de seguridad de la mayoría de los Estados, así mismo, la constante lucha de poder entre las grandes potencias releva a los Estados más

pequeños a adaptarse a las discusiones y mandatos de los más grandes, y en un tema tan poco regulado donde el choque entre gigantes hasta ahora empieza a materializarse, el ciberespacio sigue siendo un lugar anárquico casi de bandos donde cada quién ha decidido defenderse por su propia cuenta.Nuevas tecnologías y ciber-amenazas: Un contexto histórico

2. Nuevas tecnologías y ciberamenazas: un contexto histórico

2.1. Las nuevas tecnologías y su impacto en el Estado

Para comenzar con este componente del impacto de las nuevas tecnologías en el Estado, retomo lo mencionado Downes (2018, Pp. 81) quien cuenta que a partir del incidente Y2K, cuando se pensó que todas las computadoras mundiales podrían fallar debido al cambio de milenio, fue que se reveló el grado de dependencia de los sistemas informáticos en sociedades y economías altamente industrializadas.

La autora menciona que, desde ese momento, esta dependencia solo ha aumentado y se ha extendido a todas las industrias y sectores gubernamentales, y mientras que la "superficie" a asegurar continúa expandiéndose exponencialmente con desarrollos como IPv6, plataformas de redes sociales, Internet de las cosas y el crecimiento global en Internet / dispositivos y usuarios móviles, las presiones competitivas comerciales de los primeros en salir al mercado a menudo han demostrado ser mayores que las advertencias sobre la necesidad del diseño temprano de características de seguridad en los productos. (Downes, 2018 Pp. 81)

Ahora bien, la consecuencia de falta de seguridad sobre estos nuevos dispositivos y sus tempranas implementaciones de hardware y software han incluido errores, fallas y otras vulnerabilidades que más adelante se transformarían en riesgos y amenazas a la seguridad de sus usuarios, usuarios que al final van desde las personas del común, hasta incluso grandes empresas.

Así entonces, Downes (2018 Pp. 81) también explica que los nuevos lanzamientos de tecnologías han sido acompañados del crecimiento de una industria "alternativa" para la creación y distribución de ataques y exploits que aprovechan o abordan estas vulnerabilidades; como resultado, los gobiernos y las empresas se han fijado en defender y

proteger sus datos, dispositivos de TI, sistemas y redes de los intentos perniciosos de penetración y explotación y los éxitos de los ladrones cibernéticos, espías, piratas informáticos y matones patrocinados y no estatales.

Downes (2018 Pp. 81) retoma entonces de parte de un analista cuyo nombre no es mencionado, algo que vale la pena resaltar y es que los pronósticos de los analistas de TI (tecnologías de la información) no pueden seguir el ritmo del dramático aumento de la ciberdelincuencia, la epidemia de ransomware, la reorientación del malware desde PC y portátiles a teléfonos inteligentes y dispositivos móviles, así como el despliegue de miles de millones de dispositivos vinculados al Internet de Things (IoT), así como las legiones de hackers forhire (por contrato) y los ciberataques más sofisticados que se lanzan a empresas, gobiernos, instituciones educativas y consumidores de todo el mundo.

Así mismo, retoma que la serie de violaciones y robos cibernéticos de alto perfil han ejercido una presión cada vez mayor sobre los gobiernos y las empresas para que redoblen sus inversiones en ciberdefensas. Las estimaciones dramáticas de los costos de estas brechas, los costos de la ciberseguridad y los requisitos relacionados con la fuerza laboral refuerzan el enfoque. (Downes, 2018 Pp. 81)

Todo esto presentado por parte de la autora, es un buen abrebocas de la idea de por qué es tan necesaria la implementación de medidas de seguridad en cada nueva tecnología que se implementa, y es que como bien explica, los gobiernos están adoptando constantemente nuevas herramientas cuyo desarrollo y cuya seguridad está casi a la par de quienes constantemente intentan violarla. Ahora bien, James (2013, Pp. 1) también menciona algo bastante importante acerca del impacto de las nuevas tecnologías emergentes y es que estas son un tema de considerable interés para académicos y profesionales no solo en el campo de la capacidad militar y la seguridad internacional, sino también en los campos de la economía y los negocios. Se dice que las tecnologías emergentes tienen el potencial de cambiar "las reglas del juego", ya sea que ese "juego" sea el equilibrio del poder militar entre los agentes de seguridad o el equilibrio de la ventaja competitiva en un mercado entre las empresas establecidas y los nuevos participantes.

James en esta cita abre las puertas a hablar de las tecnologías emergentes como el punto clave con la capacidad de cambiar las reglas de juego tanto en el campo de las capacidades militares como en el campo de la economía y los negocios y es que, justamente los Estados más poderosos son en cierto sentido también los más desarrollados, quienes han realizado más inversiones en la tecnificación de sus sistemas, de la misma forma en que ha diseñado mejores "seguros" y defensas para estos.

La idea del autor apunta entonces a que bien las tecnologías se han convertido en una ventaja competitiva en el nuevo sistema internacional, que no solo apunta a la mejora de los procesos internos del Estado, sino que desarrolla un vínculo con la economía bastante importante donde la adecuada conectividad logrará posicionar los intereses de mejor forma; esto debido a que justamente, en la actualidad, somos una sociedad interconectada que depende de los medios de comunicación virtual para realizar desde cosas simples como enviar y recibir mensajes hasta transacciones de magnitudes colosales en cuestión de segundos.

James (2013, Pp. 3) menciona además que las tecnologías emergentes son importantes porque las nuevas tecnologías pueden presentar una amenaza u oportunidad para la seguridad misma del Estado y, sin embargo, están veladas por la incertidumbre, especialmente en el campo militar se ha logrado comprender el potencial de las nuevas tecnologías pero, como sus contrapartes en la estrategia empresarial civil, la incertidumbre que caracteriza a las tecnologías emergentes significa que no pueden saber qué tecnologías emergentes maduran para tener impactos profundos, así como tampoco pueden saber cuánto tiempo llevará esa maduración ni la trayectoria tecnológica que tendrán. Con esto entonces, el autor explica que la mayoría de las tecnologías emergentes representan mejoras incrementales con respecto a lo que sucedió antes y mejoran las competencias en dimensiones que tradicionalmente han valorado.

Por otra parte, Bacay Watson (2020), explica que las nuevas tecnologías y especialmente la "gobernanza de la tecnología global" se enfrenta a una serie de retos y desafíos que, de la mano con lo que menciona James, presentan un punto importante para analizar cómo es que se presenta el impacto de las nuevas tecnologías en el interior del Estado. La autora cuenta que los esfuerzos actuales para mejorar la tecnología de la gobernanza global enfrentan serios

retos en el siglo XXI entre los que destaca cinco en particular; el primero y que considero es de gran importancia para el desarrollo de este trabajo, apunta a que precisamente los procesos de gobernanza vinculados a la cuarta revolución industrial dependen en gran medida de instituciones, procesos y prioridades, así como de los niveles de desarrollo tecnológico y económico de los países, pues estos toman decisiones de tecnificarse en base a como los tomadores de decisiones individuales consideran la necesidad de hacerlo. (Wattson, Pp. 39)

De la mano con el segundo punto que plantea la autora, encontramos entonces el reto de que los Estados desarrollan capacidades individuales tecnológicas en base la necesidad que tengan (o en base a su propio interés nacional) y en el mismo camino con lo mencionado por James, cada Estado ha tomado iniciativas de desarrollo tecnológico que caerían en un desbalance y en una "incertidumbre" frente a si efectivamente existen amenazas directas para sí y si es necesario que se construyan capacidades para combatirlas, esto encuadra también dentro de la explicación que presenta el enfoque realista que se maneja en el interior del trabajo. (Wattson, Pp. 39)

El tercer punto que presenta la autora es que justamente hay una "escasez" de órganos de gobernanza adaptados a la cuarta revolución industrial, y que no se han adaptado a las dinámicas de la tecnología emergente, las cuales presentan un sistema que funciona con múltiples actores y es multidisciplinario. (Wattson, Pp. 39)

Este último punto, puede ayudar a comprender en la idea de que algunos Estados siguen un poco atrapados en el anacronismo tradicional de la gobernanza tradicional, y de la misma forma en que se mencionaba anteriormente de que van considerando el desarrollo tecnológico en forma individual, la consideración de la gobernanza en la era digital será posicionada en su agenda en la medida en que la consideren importante. Aun así, la crítica de la autora apunta a que de la misma forma en que se implementas nuevas tecnologías se debe tener en cuenta cómo van a cambiar las formas de gobernanza y aquí especialmente, entrarían debates como el de la regulación del ciberespacio, cosa que se profundiza en el siguiente punto.

El cuarto punto, de nuevo muy conectado con el tercero apunta a que, justamente debido a la falta de cuerpos de gobernanza modernos y a la par de los retos que representa la

implementación de nuevas tecnologías, las iniciativas de gobernanza que existen tienen una vida útil corta, y rápidamente se vuelven ineficaces cuando se enfrentan a los requisitos normativos de las innovaciones nuevas y en rápida evolución. (Wattson, Pp. 39)

Esto apunta a algo que anteriormente se mencionaba en el marco teórico y es que, no existe un consenso general frente a como se debe regular las capacidades tecnológicas, así como no hay una forma de regular o equiparar para todos los Estados la construcción de relaciones entre actores (no necesariamente estatales) por medio de la red, e incluso el debate de cómo se debe regular la construcción de capacidades (ofensivas o defensivas) en la era de la ciberguerra.

Finalmente, el quinto punto mencionado por la autora apunta a la idea de que los tomadores de decisión pueden preferir la ausencia de mecanismos de gobernanza de la tecnología para tener una gama más amplia de opciones estratégicas en lo que respecta al uso de tecnologías emergentes particulares para proteger los intereses nacionales (Wattson, Pp. 39), esto también se conecta con todo lo anteriormente dicho y encuadra muy bien con los planteamientos realistas estructurales, y es que primará el interés del escalamiento tecnológico antes que una regulación impuesta por el sistema en detrimento del interés individual de cada Estado.

Estos cinco puntos entonces son bastante ilustrativos para mencionar cuál ha sido el impacto de las nuevas tecnologías en el Estado, y especialmente para comprender como se ha transformado el actuar del mismo y el sistema de gobernanza especialmente con la adquisición de nuevas tecnologías en el ámbito militar, que de nuevo como menciona James, son un problema de incertidumbre para los otros que no saben cuál será el impacto ni las repercusiones de las nuevas capacidades, así como desconocen el tiempo de maduración que han tenido porque justamente, son basadas en las necesidades individuales, así como en el interés nacional individual de cada nación.

2.2. Ciber amenazas internacionales

Ahora bien, esta parte del capítulo apunta hacia como se conciben las nuevas amenazas a partir de estas nuevas tecnologías. Como se mencionó anteriormente en este capítulo, se sabe

que los Estados han desarrollado nuevas capacidades tecnológicas dentro de las cuales, destacan las militares y por supuesto como se narraba en el marco teórico, las vinculadas al funcionamiento de las infraestructuras críticas del mismo, en base a esto, las amenazas que representa el hecho de estar en un mundo interconectado y las nuevas capacidades que tienen ciertos actores de atacar de forma remota llevan a que se empiece a considerar cuáles son efectivamente los posibles riesgos a la seguridad, la estabilidad y el funcionamiento normal de los Estados.

Diniz, Muggah y Glenny mencionan respecto a las consideradas como "ciber amenazas" que, Debido a la novedad y la naturaleza técnica del problema, los gobiernos y los ciudadanos no están lo suficientemente bien informados acerca cómo responder a las nuevas amenazas y mientras que los ciudadanos, las empresas y las instituciones a constantemente sienten que comprender los problemas está más allá de su capacidad o que las amenazas no son relevantes para ellos. (2014. Pp.8)

De la misma forma, Diniz, Muggah y Glenny explican que la ignorancia o las percepciones erróneas a menudo resultan en una falla en abordar directamente las amenazas de seguridad cibernética y que las estrategias, si es que se adoptan, tienden a improvisarse basándose en premisas falsas y no probadas que rara vez están apoyadas sobre datos sólidos para impulsar la toma de decisiones, por ende se vuelve necesario y con relativa urgencia un nuevo enfoque más basado en la evidencia para evaluar las amenazas cibernéticas, uno informado por el conocimiento de los numerosos e interconectados riesgos en línea. (2014. Pp.8)

Esta primera aproximación de parte de los autores, se nos ilumina primero una realidad que no es tan evidente y es que, primero el riego latente y la gravedad de las ciber amenazas se han venido intensificando con el paso de los años y en la medida en que los ciberataques han afectado de peor forma a los Estados, e incluso los ciudadanos y la sociedad no son totalmente consientes de los diferentes riegos a los que también están expuestos. En ese orden de ideas, Diniz, Muggah y Glenny (2014. Pp.9) muestran en la tabla 1 presentada en la siguiente página, una aproximación a los distintos tipos de riesgos a los que, en este caso Brasil, está expuesto, sin embargo, considero ilustrativa la forma en la cual este los clasifica y los ejemplos que presenta.

La tabla muestra entonces que se clasifican tres tipos de riesgos, el primero es el ciber-crimen convencional, donde se muestran los crímenes más comunes cometidos en la red y que no representan un riesgo claro propiamente dicho a la seguridad del Estado, sino que se califican dentro de los problemas relacionados con la ciudadanía y el crimen común.

El segundo punto, apunta hacia el ciber-crimen complejo, que es un asunto que ya podría considerarse como un punto de afectación más clave a la seguridad propia del Estado, pues ya se trata de situaciones como el ciber terrorismo, la ciber guerra, los ataques a la infraestructura crítica y demás. Este punto de ciber-crimen complejo, es justamente el tipo de amenazas directas al Estado y los que causan mayor preocupación directamente pues ya son ataques directos a su infraestructura crítica, situaciones de ciberterrorismo y ciber espionaje que podrían poner en riesgo la estabilidad y el normal funcionamiento de este.

Ahora bien, aquí hay un concepto que considero es importante de comprender para explicar por qué significa un riesgo tan prominente, este es el ciberterrorismo, el cual el Ministerio de Tecnologías de la Información y la Comunicación de la República de Colombia define como: "El del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas." (MinTIC, 2020)

Categoría	Definición	Ejemplos
Ciberdelito convencional	Estas son las formas de ciberdelincuencia más extendidas en el mundo y siguen la tipología propuesta por la Unión Internacional de Telecomunicaciones (UIT) (2009).	Acceso ilegal (craqueo), interceptación de datos, pornografía infantil, spam, incitación al odio, fraude bancario, robo de identidad, infracciones de derechos de autor

Ciberdelitos complejos	Esto considera y amplía la definición de la UIT de delitos cibernéticos complejos o combinados, aquellos que pueden caer dentro de más de una categoría de delito cibernético convencional.	Ciber-terrorismo, ciberguerra, ataques contra infraestructura crítica, ciberespionaje y hacktivismo
Amenazas emergentes	Amenazas relacionadas con la expansión del ciberespacio que no encajan bien en las categorías de la UIT, ya sea porque son emergentes o porque están más relacionadas con el mundo en desarrollo.	TIC utilizadas por grupos criminales más tradicionales, como las bandas y el crimen organizado (tráfico de drogas y armas, extorsión en línea, difusión de una cultura de violencia), lavado de dinero cibernético y evasión fiscal, etc.

Tabla 1. Los tres tipos principales de ciber amenazas en Brasil (Fuente elaboración propia en base a la información de Diniz, Muggah y Glenny 2014. Pp.9)

Algunos ejemplos de ciberterrorismo los presenta el Cyber Report, un documento publicado por el International Institute for Counter-Terrorism (ICT) donde cada cierto periodo de tiempo publica un reporte respecto a las principales amenazas internacionales en el campo de la ciberseguridad y la ciberdefensa. Ahora bien, tal como menciona el ICT (2020, Pp. 10), El 3 de febrero de 2020, Al-Qaeda Arabian Peninsula (AQAP) publicó un video en el que Qasim al-Rimi, su líder, afirmaba ser responsable de un ataque perpetrado por un pistolero saudí en una base de la Armada de los EE. UU. En Pensacola, Florida, el 3 de diciembre de 2019. Además, al-Rimi llamó a los musulmanes que residen en el oeste para atacar (por ejemplo, apuñalar) objetivos occidentales, especialmente los Estados Unidos, de la misma

manera el mensaje instaba a las personas que poseen conocimientos cibernéticos a atacar ciberataques a los bancos y corporaciones estadounidenses.

Este ejemplo es especialmente ilustrativo para el ciberterrorismo pues es la capacidad que existe de parte de algún actor para generar terror y miedo generalizado a la población por medio de la amenaza directa a la vida de las personas.

Ahora bien, otro ejemplo ilustrativo es presentado por otro informe del ICT y es el ataque a la infraestructura crítica. En 2017, según menciona el ICT (2017, Pp. 25) se conoció información de que piratas informáticos iniciaron una campaña de ataque la infraestructura crítica de algunas naciones, incluidas instalaciones eléctricas, energéticas, nucleares y de aviación.

Estas campañas tendrían el propósito de espiar, sin embargo, según menciona el reporte, parece que los atacantes tenían tanto el conocimiento como la experiencia ofensiva para causar daños sustanciales, un ejemplo de ataque de esta campaña fue el realizado por el grupo de hackers, "Dragonfly", quienes hackearon instalaciones eléctricas estadounidenses y europeas el 7 de septiembre de 2017. Este grupo es de origen europeo del este y es responsable de las campañas de ciberespionaje contra la infraestructura crítica de las empresas energéticas en varios países en los últimos años. En 2014, se informó que el grupo Dragonfly tenía la capacidad de realizar actividades cibernéticas destructivas contra los operadores de oleoductos, empresas eléctricas y otros sistemas de control industrial (ICS). Los investigadores de Symantec ahora advierten contra Dragonfly 2.0, que dicen que puede interrumpir o tomar el control de dichos sistemas si así lo deciden.

El Departamento de Seguridad Nacional de EE. UU. Y el FBI advirtieron el 22 de octubre de 2017 que los piratas había estado llevando a cabo Ciberataques sofisticados contra instalaciones nucleares, eléctricas, de aviación y de agua, infraestructura crítica y agencias gubernamentales en los EE. UU. (ICT, 2017. Pp. 25)

Con esto en cuenta, encontramos que el ciberterrorismo puede llegar a representar una amenaza en primera línea para los Estados, y es justamente el tipo de amenaza que se ha

venido resaltando y como se evidencia en los informes del ICT la vulnerabilidad está presente y a pesar de que una gran potencia como lo es Los Estados Unidos tiene capacidades importantes sigue siendo vulnerable, ahora el resto de Estados también comprenderá en la medida en que sienta el riesgo la necesidad de estar preparado frente a estas amenazas.

2.3. Ciberseguridad y ciberdefensa, un asunto de la agenda de seguridad de los Estados

Ahora bien, ahondando más profundamente en como la ciberseguridad y la ciberdefensa es un asunto propio de cada Estado. Gehem, Usanov, Frinking y Rademaker (2015) explican que las Estrategias Nacionales de Seguridad Cibernética (NCSS, por su siglas en inglés) son un fenómeno nuevo, pues las primeras estrategias comenzaron a aparecer solo en los primeros años del siglo XXI. Estados Unidos fue uno de los primeros países en publicar una estrategia de este tipo en 2003. Demostrando claramente que la seguridad cibernética ya se ha convertido en una prioridad nacional.

Lo mencionado por estos entonces, deja claro que la ciberseguridad se ha convertido en una prioridad de seguridad nacional, sin embargo, según datos que retoman Gehem *et al¸* de la European Network and Information Security Agency (ENISA), a 2015 solo se tenía conocimiento de 33 países que tenían aprobada una Estrategia Nacional de Ciber Seguridad o NCSS por sus siglas en inglés, así como solamente se conocía de 8 que tenían su NCSS en preparación.

Por otra parte, Bauer y Dutton (2015, Pp. 2) explican que las razones para la existencia de estas medidas de protección yacen en la necesidad de combatir amenazas de todo tipo, pues argumentan que la amplia gama de problemas relacionados con asuntos de seguridad en el mundo en línea es grande y creciente, y se está volviendo cada vez más grave, aunque si destacan que se han realizado muchos esfuerzos a lo largo de los años para mejorar la ciberseguridad.

Los autores argumentan que esto se debe en parte a la creciente centralidad de Internet en el desarrollo económico y social, lo que la convierte en un objetivo más valioso, pero también se debe a la dinámica cambiante del problema, como el número creciente de usuarios que no solo son vulnerables a amenazas de ciberseguridad, pero también cada vez más culpables

incluso si no participan directamente en actividades malévolas en línea. (Bauer y Dutton, 2015, Pp. 2)

El planteamiento de estos autores, apuntan a que justamente la "centralidad creciente" del internet en distintos ámbitos sociales, políticos, económicos y como relataba anteriormente militares, han llevado a que surja la necesidad de implementar medidas nuevas de protección frente a la creciente cantidad de atacantes y de diversas amenazas que se presentan. Ahora bien, Maughan (2010, Pp. 29) presenta una aproximación frente a esta situación y a como los Estados deberían tomar el asunto de la seguridad, pues menciona que:

> The U.S. and the world at large are currently at a significant decision point. We must continue to defend our existing systems and networks. At the same time, we must attempt to be ahead of our adversaries, and ensure future generations of technology will position us to better protect critical infrastructures and respond to attacks from adversaries.

Esta cita es contundente al afirmar que primero, se debe continuar construyendo defensas para las estructuras ya existentes a la vez que se asegura que en los próximos desarrollos estarán por encima de los rivales y que a su vez van a permitir proteger de mejor manera los diferentes puntos críticos del Estado. Esto va por la misma línea con lo que se mencionaba anteriormente, donde primero se debe entender que el desarrollo de capacidades en ciberdefensa va de la mano de la agenda de cada Estado, que, a su vez, dependerá de si consideran o no que hay un nivel de riesgo suficiente para invertir en este tipo de capacidades, que representan un gasto importante en infraestructura y mano de obra capacitada.

Ahora bien, con todo esto es posible entrever que la agenda de la ciberseguridad en el Estado está presente debido a la alta sistematización, la alta dependencia del funcionamiento de puntos críticos del Estado y de la sociedad con las redes computarizadas, además de que como menciona Dutton: "the rapid adoption of mobile phones and devices, as well as the networking of an increasing number of objects in IoT, has further increased the number of attack points and expanded the footprint of cybercrime […]" (Orji 2012; Shalhoub & Al Qasimi, 2010 en Dutton 2012 Pp. 3).

3. Infraestructura crítica financiera colombiana: vulnerabilidades y puntos clave

3.1. La infraestructura crítica financiera y su importancia en el Estado colombiano

Una vez definidas las amenazas y planteado un poco la importancia que tienen los programas de ciberseguridad y ciberdefensa en el mundo, así como los riesgos a los que constantemente se ven enfrentados, es momento de enfocar como todo esto cobra especial importancia en el ámbito de la infraestructura crítica financiera.

Para empezar, quisiera retomar a Borghard (2018) quien presenta una serie de puntos clave respecto a la importancia de la ciberdefensa de la infraestructura crítica (I.C) financiera. La autora se centra en analizar la problemática en los Estados Unidos, sin embargo, la aproximación que ofrece al problema es bastante útil para explicar la importancia de la I.C financiera a nivel general.

la autora entonces presenta una serie de Key Concepts, el primero de estos menciona que debido a que las entidades privadas poseen y operan la mayor parte de la infraestructura crítica del sector financiero que sería el objetivo de adversarios extranjeros con fines estratégicos, el gobierno y las empresas de la Sección 9 deben colaborar como socios para defender este aspecto de la patria de los Estados Unidos. (Borghard, 2018. Pp. 4)

De esto podemos rescatar dos puntos clave, el primero de ellos es que la I.C financiera está en su mayoría en el sector privado. El hecho de que la mayoría de las transacciones que hacen que funcione la economía y el mercado interno son de parte del sector privado, especialmente bancos, firmas encargadas de tranzar en mercados internacionales y demás, aquí entra el segundo punto que es la importancia que tiene la cooperación entre Estado-Privados para la defensa de los intereses mutuos, y como menciona la autora el caso de los Estados Unidos es bastante particular e incluso está regulada, pero tal como decía anteriormente Gehem *et al*¸ los Estados Unidos es de los primeros países en implementar una estrategia compleja de ciber seguridad y ciber defensa, así que esto nos da una idea de cómo considera esta nación este tipo particular de amenazas.

Ahora es bien sabido que la economía norteamericana es una de la más grandes del mundo, dentro de la cual dependen y funcionan muchos aspectos del mercado internacional, así que las medidas que este adopte son proporcionales a la importancia que tiene, así mismo como a la cantidad de actores que le amenacen.

Ahora bien, el segundo Key concept de la autora es también importante a considerar, apunta a que la implementación de una relación verdaderamente colaborativa entre las empresas de la Sección 9 en el sector financiero y el gobierno de los EE. UU. Enfrenta importantes obstáculos que deben reconocerse y abordarse, obstáculos como lo son por ejemplo, la naturaleza multinacional de muchas empresas, la cual aumenta las tensiones potenciales entre las empresas estadounidenses con intereses financieros globales y el gobierno de los Estados Unidos, creando desafíos para compartir información confidencial de seguridad nacional. (Bogarth, 2020. Pp. 4)

Este punto menciona justamente que la colaboración entre las empresas del sector privado y lo público representa una serie de retos, pues primero, el hecho de compartir datos sensibles con el gobierno (al menos en el caso norteamericano) puede acarrear problemas de conflictos de interés e incluso tensiones como menciona la autora. Ahora bien, esta situación no es necesariamente ajena en otros países, pues la seguridad de la información es un asunto bastante sensible especialmente en las entidades relacionadas al sistema financiero, a esto se le puede sumar una idea que retoma Parra (2018, Pp. 6) donde dice que "el sector financiero es particularmente vulnerable a los ciberataques, ya que sus instituciones son objetivos atractivos, debido a su papel crucial en la intermediación de fondos".

Ahora el tercer punto, presenta otro reto bastante clave a tener en cuenta, pues la autora menciona que las partes interesadas de ambos lados deben tener en cuenta las posibles consecuencias no deseadas de profundizar la cooperación entre el gobierno y las empresas pues la cooperación puede producir inadvertidamente una dinámica de escalada o justificar ataques de represalia contra el sector financiero. (Bogarth, 2020. Pág. 4)

Este punto habla de que, la cooperación entre privados y estatales, puede llevar incluso a crear una dinámica de escalamiento de ataques hacia el sector financiero. Este punto de la

autora se podría entender en parte debido a que el gobierno tiene un rango más amplio de amenazas por su cuenta que la empresa privada; sin embargo, es claro que hasta el momento las empresas privadas también tienen sus propias medidas de seguridad y de protección de datos de sus usuarios y una alianza con el Estado se vuelve más factible en el momento en que precisamente las empresas privadas consideren que requieren la ayuda del Estado.

Con esto en cuenta, se podría afirmar que la infraestructura crítica financiera en gran parte se encuentra en manos de los privados, sin embargo, debido a su naturaleza y propensión a ser atacada es que surge la necesidad de la intervención del Estado con Alianza Publico-Privadas, que como mencionaba Bogarth, representan un reto bastante grande para ambas partes debido a la sensibilidad de los datos y el conflicto de interés que puede existir entre darle acceso de información sensible y propia de la empresa privada al gobierno. Con esas consideraciones generales, es posible proceder entonces a revisar más a profundidad el caso colombiano, para ello Parra (2018, Pp. 2) hace una aproximación al tema, y menciona que justamente el sector financiero en el país presenta grandes avances en materia de seguridad de la información y protección de datos porque justamente este sector es uno de los más afectados por ciberataques a causa de los recursos e información que maneja.

De la misma manera, Parra (2018, Pp. 2) explica que el hecho de que el sector financiero en Colombia sea el más afectado, ha generado una mayor conciencia de los impactos que se pueden presentar y de la misma forma se ha convertido en uno de los sectores que presenta mayor inversión y de los cuales propenden por implementar las mejores prácticas de ciberseguridad y seguridad de la información

Lo que menciona la autora es importante de tener en cuenta debido a que menciona dos puntos claves, el primero de ellos es que efectivamente el sector financiero en Colombia es uno de los más afectados por ataques cibernéticos debido a precisamente la cantidad de recursos e información que maneja, esto como se explicaba anteriormente en las diferentes amenazas, cabría entre el cibercrimen común, en asuntos relacionados a robo y fraude, y en cibercrimen complejo si se habla de la extracción masiva de datos con fines de espionaje o con fines de perjudicar directamente al sistema financiero colombiano.

El segundo punto para tener en cuenta de parte de la autora es que justamente debido a esta amenaza percibida es que se ha convertido en uno de los sectores con mayor inversión en el país. Esta percepción de amenaza va de la mano con la idea que se viene manejando, donde los Estados se ven obligados a construir capacidades en base a la incertidumbre que se tiene frente a amenazas directas a su seguridad y en este caso Colombia ha tomado acciones frente a esto.

Por otra parte, la Asociación Bancaria y de Entidades Financieras de Colombia (ASOBANCARIA) en cooperación con la Organización de Estados Americanos (OEA) presentan también un informe bastante interesante respecto a la situación de ciberseguridad y ciberdefensa en el país. El informe se basó en un estudio proveniente de una base de datos de 73 entidades financieras participantes del Sistema Financiero Colombiano, y presenta una serie de hallazgos importantes respecto a la seguridad digital en las entidades financieras del Sistema, de los cuales retomaré algunos a continuación.

Uno de los puntos, explica cuál es la posición de gran parte de estas empresas respecto al tema y qué tanta prioridad le dan en la agenda de parte de la alta dirección de la entidad financiera. Ahora bien, el reporte menciona que en el país el 97% de las entidades financieras, la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales. (OEA, 2018 en la OEA y ASOBANCARIA, 2020)

Esto nos indica precisamente que hay un interés claro en la implementación y fortalecimiento de nuevas medidas de seguridad por parte de las empresas bancarias en el país, y que efectivamente el sector privado ha estado implementado capacidades en ciberseguridad de la misma manera en que reconoce que efectivamente hay una amenaza sus intereses.

Con esto entonces, encontramos que bien la I.C financiera juega un rol bastante importante en el Estado Colombiano, de la misma forma en que ocupa un lugar en la agenda de seguridad de parte tanto de la empresa privada como del Estado Colombiano, sin embargo, la respuesta estatal será evidenciada más a profundidad en el siguiente capítulo donde se hablará de las medidas tomadas por este.

3.2.Ataques a la infraestructura crítica financiera colombiana

Para comenzar a hablar de los ataques más significativos a la infraestructura crítica financiera colombiana, Parra (2018) retoma de Dinero (2017) una serie de cifras que son bastante ilustrativas frente a los ciberataques que se han producido en el país, pues menciona que

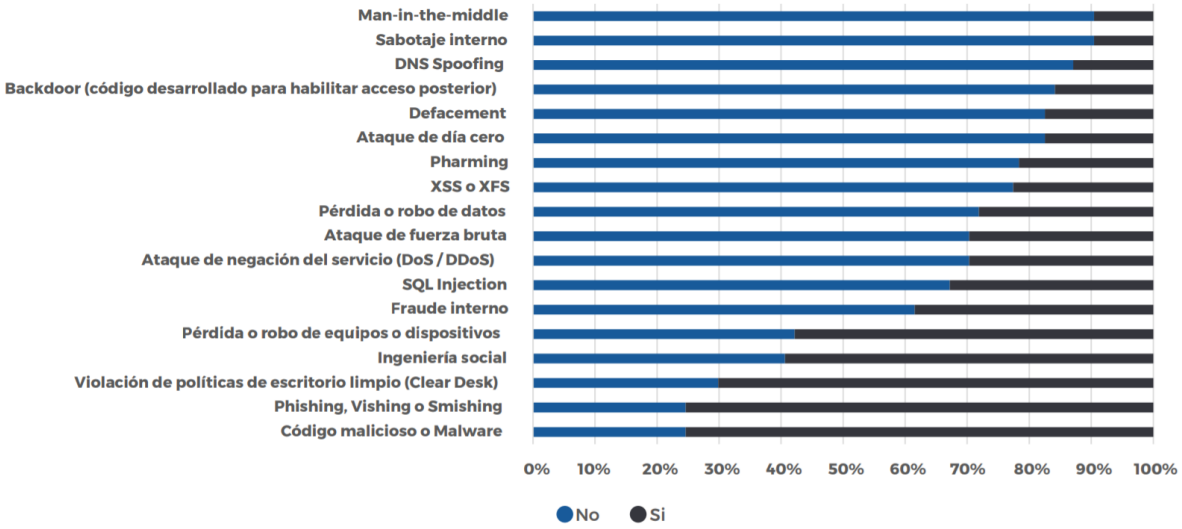
> "Según la firma Digiware, el sector financiero en Colombia en el 2017 fue el más afectado dado que recibió 214.600 ataques al día que representa el 39,6%, en segundo lugar, las telecomunicaciones con el 25.5%, seguido del gobierno con un 15.4%" (Pp. 5)

Con esto en mente, el CSIRT financiero de ASOBANCARIA (2019) reporta por su parte también la distribución de las amenazas reportadas por su entidad, donde destacan específicamente los Troyanos Bancarios, los cuales representaron el 29% de los ataques totales a entidades y particulares.

Este término de "troyanos bancarios" alude al subconjunto de malware que persigue el robo de datos de cuentas bancarias electrónicas, así como el acceso a otros servicios financieros, como por ejemplo realizar operaciones de bolsa online, o de banca electrónica (Unilibre, 2015).

Ahora bien, respecto a esta amenaza, el CSIRT profundiza explicando que Durante el 2019 se observó un crecimiento de ataques realizados a través de los troyanos bancarios, de la misma forma que se evidenciaron algunas mejoras en su desempeño y en las capacidades utilizadas para la exfiltración de información de los usuarios y dispositivos comprometidos (ASOBANCARIA, 2019. Pp. 20).

ASOBANCARIA, además, presenta una gráfica producto de su informe de ciberseguridad en el sistema financiero colombiano donde muestra la cantidad de ataques exitosos y ataques no exitosos en contra de la seguridad de la información (incluyendo ciberseguridad) contra entidades financieras identificados durante los últimos doce meses del año 2019.



Grafica 1: Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra entidades financieras identificados durante los últimos doce meses. Recuperada de ASOBANCARIA y OEA (2020, Pp. 65)

Como es posible observar en la gráfica, aunque hay algunos ataques contra entidades financieras que tienen tasas de fracaso del 80% o más, en contraste la tasa de éxito de los ataques de Malware es del 80%. Estos datos además se complementan con lo mencionado por el CSIRT de ASOBANCARIA (2019) quien menciona que justamente las amenazas que se vendrían para 2020, estarán vinculadas también con la exfiltración de información ya sea para venta o para explotación.

La filtración de información según mencionan, se presenta como una de las principales ciberamenazas del 2020, pues las diveres técnicas avanzadas de SQL injection y/o el query string manipulation, facilitan la intervención de formularios de datos, cookies e incluso las cabeceras http abriendo la posibilidad a la exfiltración masiva de la información por parte de los cibercriminales. (ASOBANCARIA, 2019 Pp. 60)

De la misma forma, mencionan que el error humano seguirá presente como una fuente constante de riesgo, pues en las bases de datos mal configuradas o las que no tienen suficientes medidas de seguridad habrá espacio para que piratas informáticos aprovechen vulnerabilidades. (ASOBANCARIA, 2019 Pp. 60)

Finalmente, se menciona que se ha evidenciado que la venta de datos en el mercado negro continúa siendo una de las más dinámicas más rentables y comunes para los ciberdelincuentes, llegando incluso a considerarse un "commodity" o necesidad. (ASOBANCARIA, 2019 Pp. 60)

Por otra parte, algunos casos particulares de ataque son presentados presentadas por el Centro Cibernético Policial estos están también vinculados al sector financiero y sirven como ejemplos de ataques exitosos con una respectiva respuesta por parte de la fuerza pública. El primero de estos es la operación Darkode, donde en una operación liderada por el FBI y apoyada por el European Cybercrime Centre (EC3) junto con la Dirección de Invetigación Criminal e INTERPOL (DIJIN) de la Policía Nacional de Colombia y otras agencias de Ley en el ámbito internacional, se logró dar de baja al denominado "más prolífico foro de cibercriminalidad que ha podido existir: Darkode." (PONAL, s.f)

El centro cibernético policial menciona que, este foro se logró dar de baja en una acción internacional conjunta, pues en este espacio los delincuentes informáticos comercializaban e intercambiaban su experiencia en distintas modalidades de hacking, cracking, así como en actividades delictivas como robo de tarjetas de crédito, ataques de denegación de servicios (DDoS), creación de programas malignos y conformación de botnets. (PONAL, s.f)

Del mismo modo, la policía menciona que este foro se constituía como punto de encuentro para coordinar ataques informáticos y que la operación dio como resultado la captura de 28 personas, 37 allanamientos, así como numerosas incautaciones de computadores y otros equipos. (PONAL, s.f)

El segundo caso vinculado a una banda delincuencial, donde se menciona que el Centro Cibernético Policial de la DIJIN logró la captura de una organización delincuencial dedicada a realizar defraudaciones millonarias a través de medios informáticos a diferentes entidades financieras. Se habla del posible hurto mediante la utilización de medios informáticos, de un monto superior a los diez mil millones de pesos **($10.000.000.000)**, causó alrededor de 326 afectaciones a diferentes cuentas en hechos relacionados con pagos de planillas de seguridad social a través de PSE. (PONAL, s.f)

La PONAL (s.f) menciona que la modalidad delictiva empleada por esta organización criminal, se basaba en el desarrollo de programas informáticos especializados llamados (MALWARE), que en su momento aprovecharon las vulnerabilidades que ofrece la banca online y el uso desprevenido de dichos servicios por parte de los usuarios con el fin de apoderarse de diversa información personal y privilegiada como lo son números de cuentas, contraseñas, cédulas, entre otros datos de productos financieros que fueron utilizados posteriormente para realizar el robo del dinero.

Finalmente, el tercer caso que mencionan también está vinculada al accionar de otra banda delincuencial. Según se menciona, Investigadores del Centro Cibernético Policial, dieron captura en Barranquilla a 8 miembros de una banda que se infiltraba en empresas para desocupar las cuentas de nómina y logró hurtar más de setenta y siete millones de pesos ($77.128.500) millones de pesos; la modalidad delictiva, consistía en desarrollar programas informáticos para vulnerar los servicios de la banca virtual como accesos remotos y el uso desprevenido de computadores sin los niveles de seguridad requeridos. (PONAL, s.f)

Estos tres casos muestran entonces las capacidades de bandas delincuenciales de causar daños al sistema financiero colombiano, y aunque son separados hablan de la existencia de bandas criminales dedicadas al uso de expertos criminales para acceder a vulnerabilidades propias de la banca electrónica, situación que cabe en las preocupaciones de ciberseguridad que tanto se vienen mencionando durante el trabajo.

Los datos encontrados, apuntan entonces a que justamente el sector financiero colombiano es constantemente atacado con métodos cada vez más novedosos y con herramientas tecnológicas y software de avanzada, que como se mencionaba anteriormente, va a la par de los mismos avances en seguridad de la información que se viene manejando.

Esto entonces, continúa enmarcando la necesidad que viene mencionando en todo el trabajo respecto a la creación de capacidades de seguridad y defensa, pero la particularidad es que debido a que el sector financiero y la I.C financiera se fundamentan en la empresa privada, y el reto va principalmente hacia como el sector privado les ha dado manejo a estas situaciones.

4. Las medidas de ciberseguridad en la Infraestructura crítica financiera colombiana

4.1. Medidas tomadas por el Estado colombiano para contrarrestar y superar los ataques a la infraestructura crítica financiera.

Ahora bien, para conocer la aproximación que se le ha dado al tema de la ciberseguridad y ciberdefensa de parte del Estado Colombiano, es importante hablar del documento CONPES 3995 titulado *"Política Nacional de Confianza y de Seguridad Digital*" el cual fue publicado en el año 2016, este junto con el documento CONPES 3701 titulado *"Lineamientos de Política para Ciberseguridad y Ciberdefensa"*, publicado en el año 2011.

Estos dos documentos como menciona el Departamento Nacional de Planeación (DNP) (2016, Pp. 9) "procuraron el fortalecimiento y generación de capacidades en el Gobierno nacional, con un enfoque de gestión de riesgos, para brindar seguridad y defensa a los ciudadanos, así como a las instituciones en el ciberespacio".

Ahora bien, entrando a analizar estos dos documentos, se encontró que presentan un marco interesante para comprender cuál ha sido el enfoque desde el sector público que se le ha dado al problema, pues como se relataba anteriormente, el sector privado ha tomado iniciativas y se ha logrado mostrar que efectivamente representa una amenaza para estos, pero es como mencionaba Bogarth un reto el ver cómo se puede lograr una alianza público-privada para combatir las amenazas.

En un primer punto, se tiene entonces la aproximación al documento CONPES 3701, el cual menciona que surge en un momento donde se consideró que la capacidad del Estado colombiano en ese momento para enfrentar las amenazas cibernéticas presentaba debilidades y no existía una estrategia nacional al respecto (DNP, Pp. 2), además de que como mencionan la conectividad en el país estaba creciendo de forma muy considerable, mencionando que en Colombia se había incrementado el uso de tecnologías de la información y las comunicaciones elevando su nivel de exposición a amenazas cibernéticas, pues el número de usuarios de internet aumentó en 354% entre el 2005 y el 2009, así como el número de suscriptores a internet se incrementó en un 101% entre el 2008 y el 2010 alcanzando un total de 4.384.181 suscriptores de internet fijo y móvil. (DNP, Pp. 7)

El CONPES 3701 implementa entonces un esfuerzo por decidir una política conjunta de ciberseguridad y ciberdefensa para el país, reuniendo un análisis de la normatividad vigente en ese momento y proyectando un plan de acción para implementar nuevas medidas y nueva infraestructura orientada a la ciberseguridad y la ciberdefensa de la nación, aquí destaca especialmente la implementación de organismos con la capacidad técnica y operativa necesaria para la defensa y seguridad nacional en materia cibernética, que en coordinación multisectorial permitiría atender las situaciones relacionadas al tema de mejor forma.

De este documento se destaca entonces el planteamiento de una comisión intersectorial que se planteó en el siguiente modelo de coordinación:

Gráfica 2: Modelo de coordinación. Recuperada de DNP (2011, Pp. 21)

Lo que nos muestra este modelo es que se planteó un sistema de coordinación y comunicación, así como de cooperación entre las tres entidades encargadas de los asuntos relacionados con la ciberseguridad y la ciberdefensa en el país, entre los cuales está el Comando Conjunto Cibernético, el cual forma parte de las Fuerzas Militares del país y especifica claramente que se trata de la defensa del país en el ciberespacio, así mismo está el Centro Cibernético Policial, encargado de velar por la seguridad ciudadana y el COLCERT o Grupo de Respuestas a Emergencias Cibernéticas de Colombia, el cual puede ser considerado como un punto intermedio entre la respuesta estatal y privada para combatir las ciber amenazas, pues como mencionan en su página oficial, uno de sus objetivos es el de coordinar y asesorar a diferentes CSIRT's y entidades tanto del nivel público, como privado y de la sociedad civil para responder ante incidentes informáticos.

Ahora bien, tal como menciona Parra (2018):

> "durante el trascurso de los años se vio necesidad de actualizarla y fortalecerla (La política de ciberseguridad y ciberdefensa) teniendo en cuenta las recomendaciones emitidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), es por ello por lo que en el 2016 se aprobó a través de un nuevo documento el CONPES 3854" (Pp. 3)

Este nuevo documento, como también destaca Parra (2018, Pp. 3) presenta una nueva política nacional de seguridad cibernética siendo Colombia 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, además de que como menciona, "se implementaron nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación". (Parra, 2018, Pp. 3)

La autora también resalta que desde la implementación del nuevo documento Este diseño se basa en los siguientes cinco frentes de acción:

- Gobernanza de la seguridad digital.
- Marco legal y regulatorio de la seguridad digital

- Fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital.
- Cultura ciudadana
- Gestión de riesgos de seguridad digital. (Parra, 2018, Pp. 3)

Ahora bien, la respuesta de la empresa privada, por su parte, como reconoce ASOBANCARIA y la OEA (2020), ha sido también la implementación de iniciativas de protección bastante importantes como lo es el CSIRT Financiero o Centro de Respuestas de Incidentes en Ciberseguridad, el cual como mencionan:

> "lideramos los esfuerzos de colaboración en el sector para compartir los incidentes de ataques cibernéticos. El CSIRT sectorial se fundamenta en estrechos lazos de cooperación local e internacional con agencias de investigación y una continua articulación con autoridades; a través de una plataforma en línea las entidades financieras y centros de investigación a nivel global, regional y local comparten información de amenazas cibernéticas bajo estándares internacionales." (Pp. 35)

Esta iniciativa como se mencionaba en el capítulo inmediatamente anterior es altamente apoyada por el sector privado al interior del país desde la gran mayoría de entidades que forman parte del sistema financiero en el país, y de la misma forma representan una prioridad dentro de la agenda de seguridad que manejan, pues las cifras de ciberataques que se presentan anualmente ameritan darle importancia a este problema.

Aquí entonces tenemos dos puntos importantes para comprender cuál ha sido la respuesta a las ciber amenazas de la infraestructura crítica financiera colombiana, desde el Estado, el cual tiene una entidad central (COLCERT) para manejar asuntos relacionados con las amenazas a la infraestructura crítica del Estado colombiano y el esfuerzo privado materializado en la iniciativa del CSIRT financiero.

Con todo esto entonces, es posible bosquejar las medidas que tiene el país en cuanto a respuesta y capacidades de actuar frente a un ataque a la infraestructura crítica financiera del país, que se compone en tres niveles:

El primero, la seguridad individual que cada entidad ha implementado al interior de sus sistemas, que son las medidas de seguridad propias para repeler los ataques a escala individual. Este nivel es para el país el más importante y fundamental pues la gran mayoría de ataques que se presentan son a nivel individual y no a gran escala y al mismo tiempo, así que estas capacidades individuales que son parte de la agenda de las organizaciones que forman el sistema financiero

El segundo nivel, se enfoca en las capacidades del CSIRT Financiero, el cual funciona como una organización que agrupa a gran parte de las entidades financieras del país y establece puntos comunes frente a las amenazas más preocupantes para todas las organizaciones, este nivel específicamente se enmarca en una organización dedicada específicamente a dar respuesta a las necesidades y problemáticas del sistema y de sus miembros así como también se enfoca en ser un tanque de pensamiento y de investigación frente a todo tipo de amenazas que puedan ser relevantes para el sistema financiero.

Finalmente, el tercer nivel está enfocado en las acciones propias del gobierno colombiano para combatir las amenazas al sistema financiero, primero con la implementación del COLCERT, entidad central en todo el tema de la ciberseguridad y la ciberdefensa al interior del país y segundo también implementando una serie de normatividad legal que castiga el accionar delincuencial de organizaciones dedicadas a los ciber crímenes en el país. Este segundo punto va de la mano también con la creación de un grupo policial dedicado a la persecución de los cibercrímenes en el país, además de un grupo especializado al interior de las Fuerzas Militares para proteger la defensa de la nación en el ciberespacio.

El COLCERT entonces, se encarga de ser un punto central desde donde el Estado colombiano recibe la retroalimentación y brinda apoyo y asesoría los distintos CSIRT's y para el caso de la Infraestructura Crítica financiera el CSIRT financiero de Asobancaria es un punto claro que agrupa a una parte muy importante de todo el sistema.

Con esto definido, se procede entonces a dar las reflexiones finales del trabajo.

Conclusiones

Con lo investigado se encontró que primero, hay una creciente preocupación internacional respecto a los temas de ciberseguridad y ciberdefensa, que abarcan tanto los Estados en primera medida, pero también los privados en ciertos sectores particulares como los financieros, esto se presenta como resultado de que hay actores con capacidades de atacar las redes y los sistemas con el riesgo de afectar de forma grave el funcionamiento incluso de una nación, así que esto posiciona al tema de ciberseguridad y ciberdefensa en las primeras posiciones de la agenda.

Se encontró también que a pesar de que el tema es una preocupación generalizada, no todos los Estados cuentan con las mismas capacidades tanto económicas como tecnológicas para invertir en el área de la ciberseguridad y la ciberdefensa, lo que ha llevado a que algunos Estados estén mejor preparado respecto a otros frente a estos ataques y amenazas, de la misma forma en que algunas naciones tienen una mayor inminencia a ser atacados debido a la importancia global que tienen, claro ejemplo son los Estados Unidos y aplicado al caso su sistema financiero.

Ahora para el caso colombiano, queda por decir que según todo lo investigado, efectivamente si existe una preocupación y se ha ejecutado una estrategia de ciberseguridad y ciberdefensa al interior del país pues en la medida en que se hizo evidente la tecnificación y la inclusión digital de la población, el Estado ha respondido preparándose frente a las amenazas del siglo XXI y específicamente en el marco de su sistema financiero de la mano con las empresas privadas se ha construido una estrategia de respuesta a las amenazas ya existentes y se consiguió formar un esquema de respuesta que ya se prepara para responder a las amenazas a gran escala que puedan afectar al país.

Ahora bien, la relación que existe entre el COLCERT y el sistema financiero representa como lo decía Borghart (2018) tiene una serie de retos donde privados y Estado deben ser capaces de construir una relación que no afecte los intereses en ninguna de las dos partes y que permita estar a la par de todos los atacantes, que como bien se decía anteriormente van evolucionando casi al mismo ritmo que las mismas medidas de seguridad. Es importante

resaltar que específicamente en la construcción de capacidades para proteger el sistema financiero en el país y su infraestructura crítica el sector privado ha jugado un papel sumamente importante, pues son las capacidades individuales las que mitigan gran parte de los ataques que reciben.

Concluyo este trabajo, diciendo que el país y en general las empresas privadas se están preparando para enfrentar las nuevas amenazas que se vienen, y que tienen clara la importancia de proteger el sistema financiero del país para que este continúe prosperando en el tiempo.

Bibliografía

ASOBANCARIA (2020) Memoria Anual CSIRT financiero ASOBANCARIA 2019. Programa de ciberseguridad del sector - CSIRT Financiero - de Asobancaria. Recuperado de: https://www.asobancaria.com/wp-content/uploads/2020/06/CRT-MA_2020_compressed.pdf

Bauer, J & Dutton, W (2015) *The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet.* Joint working paper for the Oxford Global Cybersecurity Project at the Oxford Martin Institute, University of Oxford, and the Quello Center at MSU .Available at SSRN: https://ssrn.com/abstract=2614545 or http://dx.doi.org/10.2139/ssrn.2614545

Borghard, E. (2018). (Rep.). Protecting Financial Institutions Against Cyber Threats: A National Security Issue. Carnegie Endowment for International Peace. doi:10.2307/resrep20722

Castillo, Y (2018) Normatividad De Ciberseguridad En El Sector Financiero Colombiano. Universidad Piloto de Colombia. Seminario de investigación aplicada de la gestión de la seguridad y el riesgo. Recuperado de: http://polux.unipiloto.edu.co:8080/00004756.pdf

Ciberseguridad | Centro Cibernético Policial. (s. f.). Recuperado 7 de diciembre de 2020, de https://caivirtual.policia.gov.co/ciberseguridad/recomendaciones/bancario

Ciberterrorismo—Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). Recuperado 1 de diciembre de 2020, de https://www.mintic.gov.co/portal/inicio/18728:Ciberterrorismo

colCERT. (s. f.). Recuperado 7 de diciembre de 2020, de http://www.colCERT.gov.co/?q=acerca-de

Craig, Anthony & Valeriano, Brandon. (2018). Realism and Cyber Conflict: Security in the Digital Age.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. http://doi.org/10.22215/timreview/835

Departamento Nacional de Planeación (2011) Documento CONPES 3701: "Lineamientos de política para la Ciberseguridad y Ciberdefensa". Recuperado de: https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

Departamento Nacional de Planeación (2020) Documento CONPES 3995: Política Nacional De Confianza Y Seguridad Digital. Recupeardo de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Diniz, G., Muggah, R., & Glenny, M. (2014). *Assessing cyber threats* (Deconstructing Cyber Security in Brazil:, pp. 8-9). Igarape Institute. http://www.jstor.org/stable/resrep19169.6

Downes, C. (2018). Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns. The Cyber Defense Review, 3(1), 79-104.

Goldsmith, J. L. (1998). Against Cyberanarchy. *The University of Chicago Law Review*, *65*(4), 1199-1250. https://doi.org/10.2307/1600262

Huth, P., Gelpi, C., & Bennett, D. S. (1993). The Escalation of Great Power Militarized Disputes: Testing Rational Deterrence Theory and Structural Realism. *The American Political Science Review*, *87*(3), 609-623. https://doi.org/10.2307/2938739

James, A. D. (2013). *Emerging Technologies and Military Capability*. S. Rajaratnam School of International Studies. http://www.jstor.org/stable/resrep05804

Jensen, B., & Valeriano, B. (2019). *What Do We Know About Cyber Escalation?: Observations From Simulations And Surveys*. Atlantic Council. http://www.jstor.org/stable/resrep20705

Kania, E. B. (2016). Cyber deterrence in times of cyber anarchy—Evaluating the divergences in U.S. and Chinese strategic thinking. *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 1-17. https://doi.org/10.1109/CYCONUS.2016.7836619

Katin-Borland, N (2014) Cyberwar: A Real and Growing Threat. En Costigan, S & Perry, J (e) Cyberspaces and Global Affairs. Part I: Chapter I. Ashgate Publishing Limited. Farnham, England.

Kello, L (2017) 11. Cyber Security: Gridlock and Innovation. In Held, D & Hale, T (e) Beyond Gridlock. Polity Press. London, U.K.

Kshetri, N (2016) The Quest to Cyber Superiority. Cybersecurity Regulations, Frameworks, and Strategies of Major Economies. Springer International Publishing. Switzerland. 2016

Lopez, J & Setola, L & Wolthusen, S (e) (2012) Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense. Springer-Verlag Berlin Heidelberg 2012. Berlin, De.

Maughan, D. (2010). The need for a national cybersecurity research and development agenda. *Communications of the ACM*, *53*(2), 29-31. https://doi.org/10.1145/1646353.1646365

Mearsheimer, J (2014) The Tragedy of Great Power Politics. Norton. New York. U.S

Organización de Estados Americanos & ASOBANCARIA (2020) Estado de la Ciberseguridad en el Sistema Financiero Colombiano. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. Recuperado de: https://www.asobancaria.com/wp-content/uploads/2020/10/20201014-ASOBANCARIA-2020_compressed.pdf

Satter, R. (2020, mayo 13). EEUU acusa a hackers vinculados a China de intentar robar investigaciones sobre el virus. Reuters. https://fr.reuters.com/article/salud-coronavirus-china-hackers-idESKBN22P2N8

Semana. (2020, diciembre 14). Hackers rusos sospechosos de espiar agencias gubernamentales de Estados Unidos. Semana.com Últimas Noticias de Colombia y el Mundo. https://www.semana.com/mundo/articulo/hackers-rusos-sospechosos-de-espiar-agencias-gubernamentales-de-estados-unidos/202038/

UniLibre. (2015). ¿Qué son y cómo funcionan los troyanos bancarios? Recuperado 7 de diciembre de 2020, de http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/260-que-son-y-como-funcionan-los-troyanos-bancarios

Watson, V. B. (2020). *The Fourth Industrial Revolution And Its Discontents: Governance, Big Tech, And The Digitization Of Geopolitics* (HINDSIGHT, INSIGHT, FORESIGHT, pp. 37-48). Daniel K. Inouye Asia-Pacific Center for Security Studies. http://www.jstor.org/stable/resrep26667.8