UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
PROGRAMA DE POSGRADO EN CIENCIAS POLÍTICAS Y SOCIALES

CAMPO DE CONOCIMIENTO: RELACIONES INTERNACIONALES

CIBERSEGURIDAD: UN ENFOQUE TEORÍCO Y ANALÍTICO PARA LA SOBERANÍA, SEGURIDAD NACIONAL Y LA POLITICA EXTERIOR

TESIS

QUE PARA OPTAR POR EL GRADO DE:

DOCTOR EN CIENCIAS SOCIALES

PRESENTA:
JUAN MANUEL AGUILAR ANTONIO

TUTOR PRINCIPAL
DR. ALEJANDRO CHANONA BURGUETE
FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES (FCPYS)

MIEMBROS DEL COMITÉ TUTOR:

DR. RAÚL GUILLERMO BENÍTEZ MANAUT
CENTRO DE INVESTIGACION SOBRE AMÉRICA EL NORTE (CISAN)

DR. JUAN CARLOS BARRÓN PASTOR
CENTRO DE INVESTIGACION SOBRE AMÉRICA EL NORTE (CISAN)

CIUDAD DE MÉXICO, AGOSTO, 2022

Índice General

Índice de tablas.

Índice de figuras

Introducción General

La presente investigación parte de la hipótesis de que el ciberespacio es una nueva arena de la política internacional en la que es posible vulnerar la soberanía, seguridad nacional y política exterior de los Estados-Nación, a través de la manipulación y vulneración de sistemas de seguridad de la información por medio del dominio del ciberespacio. En este sentido, la investigación se divide en cuatro capítulos, que se describen a continuación:

I. En el capítulo 1, se contextualiza cómo desde el ciber incidente de Estonia, en 2007, la ciberseguridad se transformó en un tema de seguridad nacional y política exterior para los gobiernos de las naciones alrededor del mundo. En consecuencia, se hace una revisión histórica desde la creación del internet, en 1969, con el proyecto ARPANET, que surgió como una red de información entre universidades y el Departamento de la Defensa, de los Estados Unidos, ante situaciones de crisis, hasta transformarse en dominio clave en la comprensión de eventos como el *Cablegate* de *Wikileaks* (2011), la *Primavera Árabe* (2011), o *Stuxnex* (2010). También se analizan las características del ciberespacio que representa un régimen híbrido de componentes físicos y virtuales que coexisten en el mundo real. Y se define al ciberespacio como una arena de interacción compuesta por una parte virtual, integrada por una infraestructura web (protocolos de internet y softwares), y una parte física, (infraestructura de telecomunicaciones, critica y hardware), en que se suscitan dinámicas, fenómenos o hechos sociales en diferentes canales o esferas (política, económica, cultural, prensa, etc.), que poseen un potencial de transferencia o impacto de estos eventos al mundo material, con repercusiones al contexto o integridad del Estado-Nación,

gobierno o sociedad. También, se aborda la comprensión del ciberespacio, como dominio de influencia de las naciones, desde la perspectiva de la Teoría de la Guerra, el enfoque neorralista, y la teoría de la comunicación, con una perspectiva electica, para presentar un marco de análisis para entender este nuevo campo de interacción de la política internacional. Por último, se discute, desde la visión de las teorías tradicionales, la influencia que pueden tener actores como el Estado-Nación, en este campo, dentro del ciberespacio. Para posteriormente, presentar una conceptualización dentro de este nuevo dominio de las relaciones internacionales.

II. En el capítulo 2 se discute el concepto de soberanía nacional, desde el enfoque estado-céntrico, en el marco de las controversias surgidas a razón de que se define de que dicha noción no es aplicable en su comprensión dentro del ciberespacio. Por lo cuál se aborda el concepto de la soberanía, desde una concepción postwhestphaliana, con el fin de presentar una propuesta para discutir el tema de la soberanía y su influencia en el ciberespacio. Esta acción, sirve como preámbulo para presentar los puntos de encuentro entre la soberanía, la seguridad nacional, y el papel que juega la ciberseguridad dentro de esta. En consecuencia, se analiza el proceso de securitización del internet, para entender el papel que juega la ciberseguridad en la doctrina y estrategia de seguridad nacional de los Estados-Nación. Con lo cuál, se hace una revisitación a este concepto, y se analiza cómo las naciones construyen una Estrategia Nacional de Ciberseguridad (ENCS), como parte crucial de su Estrategia de Seguridad Nacional. Para esto, se analizan ENCS de las naciones de la Organización del Tratado del Atlántico Norte (OTAN) y se identifican las líneas claves que contemplan estos documentos. Posteriormente, se abordan el lugar que ocupan el resto de las naciones y regiones del mundo, respecto a su desarrollo de una ENCS con relación a las naciones de la OTAN. Finalmente, se presenta una clasificación de los diferentes tipos de amenazas provenientes del ciberespacio, se introducen los conceptos de resiliencia y disuasión en el dominio del ciberespacio. Y cómo las naciones deben construir cibercapaciades para consolidar estas dos nociones.

III. En el capítulo 3, se analizan los vínculos entre la soberanía y la política exterior. Para esto, se aborda el concepto del interés nacional, y se rastrean los nexos con la capacidad de acción y ofensa en la política exterior desde diferentes perspectivas teóricas como el paradigma realista, la visión liberalista, la Teoría de la Guerra, y el Constructivismo. Posteriormente, se analizan los entornos de ciberseguridad y desarrollo de ciber capacidades, en las diferentes regiones del mundo como los países de la OTAN, el resto de los países de Europa, Asía, América Latina, Medio Oriente, África y Oceanía a través de métricas internacionales, como el *Global Cybersecurity Index* de la Unión Internacional de Telecomunicaciones, y el *National Cybersercurity Index* (NCSI) de la E-Governance Academy, vinculados a construcción de cibercapacidades por parte de los Estados-Nación. A continuación, se presenta la medición del *National Cyberpower Index* (NCPI), creada por el Belfer Center, de la Harverd Kennedy School, que presenta una noción de construcción de capacidades cibernéticas, por parte de las naciones del mundo, más centrada en el ciberpoder. En este contexto, se presenta, el conjunto de naciones que son consideradas líderes en la construcción de ciber poder y son consideradas las cinco superpotencias del ciberespacio, que son los países de Estados Unidos, China, Reino Unido, Rusia e Israel. Por último, se presenta el panorama de las Amenazas Persistentes Avanzadas o *Advanced Persistent Threat*, una serie de ciber comandos definidos por la agencia de Fire Eye, formados y bajo el resguardo de China, Rusia, Irán, Corea del Norte y Vietnam, que tienen una alta presencia mediática por ejecutar ciber operaciones en aras de alcanzar objetivos particulares de estos países a través del dominio del ciberespacio.

IV. En el capítulo 4 de la investigación, se realiza un estudio de caso para analizar los hechos en torno al *Russiangate* y *SolarWinds,* con la finalidad de utilizar el abordaje teórico y metodológico de los primeros tres capítulos para abordar un evento en el cuál se demuestre la hipótesis de la investigación. Para eso, se utiliza una estrategia de análisis divida en cuatro diferentes apartados que son: 1) Un análisis de fuentes abiertas a través de medios de prensa, mediante el cual se

presentará una narrativa y contextualización de lo que fue el *Russiangate* y el incidente *SolarWinds*. 2) Un análisis del contenido del Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016. 3) Un análisis de las ciber capacidades de los Estados Unidos y Rusia para valorar la evidencia presentada por el análisis de fuentes abiertas y el análisis al Informe Mueller. Por último, 4) la realización de un total de diez entrevistas con especialistas en ciberseguridad de las Américas, para generar un análisis de teoría fundamentada de los comentarios estratégicos obtenidos en cada conversatorio, con el fin de realizar un estudio crítico sobre la viabilidad de la intromisión de Rusia en las elecciones de Estados Unidos de 2016.

Una vez concluida la investigación, se indica que la hipótesis de este trabajo se verificó, a razón de que el estudio de caso reveló que la Federación Rusa operó al menos tres estrategias en el marco de las elecciones presidenciales de 2016 y el incidente *SolarWinds*, para utilizar a este como un nuevo dominio en aras de alcanzar una ventaja estratégica contra Estados Unidos, los cuales fueron: 1) La extracción y filtración de información del Comité Nacional Demócrata, así como de la correspondencia de la candidata Hillary Clinton y su jefe de campaña John Podesta, en el marco de la elección presidencial de 2016. 2) La estructuración y ejecución de operaciones a través del ciberespacio, en el marco de la elección presidencial de 2016, con el fin de influir en la opinión pública y ciudadanía, para difundir desinformación y promover los radicalismos políticos, a través de redes sociales y eventos (*rallies*), que impactaron en la intención de voto del proceso electoral. 3) La capacidad de intervenir los sistemas informáticos de las empresas más importantes del país e instituciones del más alto nivel del gobierno de los Estados Unidos. A través de una ciber operación que vulneró a la empresa *SolarWinds,* lo que implicó un ciber ataque con fines de ciber explotación.

Capítulo 1. El Ciberespacio como arena de la política internacional

Introducción

El objetivo de este capítulo es presentar una introducción en torno de cómo el ciberespacio se ha transformado en una nueva arena de interacción e influencia de los Estados-Nación, en dentro de la política internacional. Para esto, se contextualiza cómo desde el ciber incidente de Estonia, en 2007, la ciberseguridad se transformó en un tema de seguridad nacional y política exterior para los gobiernos de las naciones alrededor del mundo. En consecuencia, se hace una revisión histórica desde la creación del internet, en 1969, con el proyecto ARPANET, que surgió como una red de información entre universidades y el Departamento de la Defensa, de los Estados Unidos, ante situaciones de crisis, hasta transformarse en dominio clave en la comprensión de eventos como el Cablegate de Wikileaks (2011), la Primavera Árabe (2011), o Stuxnex (2010). También se analizan las características del ciberespacio que representa un régimen híbrido de componentes físicos y virtuales que coexisten en el mundo real. Y se define al ciberespacio como una arena de interacción compuesta por una parte virtual, integrada por una infraestructura web (protocolos de internet y softwares), y una parte física, (infraestructura de telecomunicaciones, critica y hardware), en que se suscitan dinámicas, fenómenos o hechos sociales en diferentes canales o esferas (política, económica, cultural, prensa, etc.), que poseen un potencial de transferencia o impacto de estos eventos al mundo material, con repercusiones al contexto o integridad del Estado-Nación, gobierno o sociedad. También, se aborda la comprensión del ciberespacio, como dominio de influencia de las naciones, desde la perspectiva de la Teoría de la Guerra, el enfoque neorralista, y la teoría de la comunicación, con una perspectiva electica, para presentar un marco de análisis para entender este nuevo campo de interacción de la política internacional. Por último, se discute, desde la visión de las teorías tradicionales, la influencia que pueden tener actores como el Estado-Nación, en este campo, dentro del ciberespacio. Para posteriormente, presentar una conceptualización dentro de este nuevo dominio de las relaciones internacionales.

1.1 Estonia 2007: internet, soberanía y seguridad nacional

25 de abril de 2007, es un día soleado en Tallin, la capital de Estonia, hace mes y medio que la primavera ha iniciado y el país vive un clima de tranquilidad. Sin embargo, el ambiente político se ha mantenido tenso desde comienzos de año e indica que una crisis social está a punto de estallar. ¿El objeto central del conflicto? El Monumento a los Libertadores o *Soldado de Bronce*, ubicado en la Plaza Tõnismägi, en el centro de la ciudad. Desde la independencia de Estonia de la Unión Soviética, en 1991, el monumento ha sido objeto de polémica. Para los habitantes de origen ruso representa un motivo de orgullo que dignifica el triunfo de la extinta URSS sobre el nazismo y la liberación del país. Mientras que, para los residentes de etnia estonia, es un símbolo la ocupación soviética de más de cincuenta años, marcada por el autoritarismo y la supresión de libertades (Ottis, 2008).

Meses antes, el 10 de enero, el *Riigikogu*[1] aprobó el *Acta de Protección de Tumbas de Guerra*, un documento que especifica que las sepulturas o mausoleos de caídos en conflictos armados, en territorio nacional, no deben estar ubicados en lugares inadecuados –con énfasis para plazas públicas -como la Tõnismägi, donde reside el *Soldado de Bronce* (BBC News, 2007). La legislación es el primer paso para su remoción a una nueva ubicación y un clima de confrontación se gesta entre la población. En este contexto, el 15 de febrero, el parlamento aprobó a *Ley de Construcciones Prohibidas*, que restringe los monumentos que hacen honor a la ocupación soviética. El decreto termina por dividir al país y cimenta el inicio la crisis política.

El destino del *Soldado de Bronce* será el cementerio militar de las Fuerzas de Defensa, ubicado a las afueras de Tallin. Su traslado se decide aplazar debido a las elecciones nacionales por parte del Primer Ministro, en marzo, para no mermar o polarizar el proceso político que será el primero que permita el voto a través del uso de plataformas de digitales internet (Detlefsen, 2015). Hecho que forma parte del proyecto *X-Road*, plan de modernización tecnológica que adoptó Estonia para la digitalización de todos los servicios públicos estratégicos, en aras de convertirse en la capital digital de Europa en el corto plazo (BBC News, 2017).

[1] La Asamblea Legislativa de la República de Estonia

En las elecciones resultó ganador Andrus Ansip, representante del Partido Reformista Estonio, quien ocupaba el cargo de Primer Ministro desde 2004 y buscó la reelección en el proceso electoral de 2007. El 24 de abril, en un discurso frente a la *Riigikogu*, referente al *Soldado de Bronce*, Ansip expresa que los restos de los soldados enterrados en el mausoleo pueden pertenecer a miembros ebrios o saqueadores del ejército rojo, durante el sitio de Tallin. Sus comentarios llegan a la opinión pública nacional e internacional y exaltan las emociones de la población de ascendencia rusa (Regnum, 2007). Incluso, en Moscú, el Kremlin reprueba sus palabras y una gran cantidad de medios informativos rusos, como *Ria Novosti* o *Russia Today*, dan una amplia difusión a la nota. La siguiente jornada el país despierta en un clima de efervescencia. La población rusa empieza a organizarse y convocan a una marcha y protesta pacífica para el mediodía del 26 de abril, en la Plaza Tõnismägi. Los temores por parte del gobierno, y de que la protesta se transforme en disturbios violentos, no son menores. Se estima que un total de 350,000 de personas (de un total 1.5 millones de habitantes de Estonia) hablan la lengua rusa y siente afinidad con el pasado soviético del país y con lo que representa el *Soldado de Bronce* (Herzog, 2011).

El día de la convocatoria, 1,500 personas se presentan frente al monumento soviético para evitar su remoción. Muchos de los asistentes portan banderas de la Federación Rusa y gritan consignas en favor de la superpotencia, la policía trata de calmar su euforia, pero su intervención sólo deriva en disturbios violentos. A las 21:20 horas, los manifestantes pro-rusos empiezan a cometer actos de agresión, y en defensa, la policía utiliza gas lacrimógeno y balas de goma para disolver la muchedumbre. Las acciones derivan en un incremento en las acciones violentas por parte de los manifestantes que responden con bombas de petróleo, a la par que empiezan a realizar actos de vandalismo en los edificios y comercios del centro de la ciudad. La confrontación es ríspida poco antes de la media noche. Los diarios nacionales estiman que una persona ha fallecido, 153 están heridas y 800 han sido arrestadas, la noche del 26 de abril es denominada como los peores disturbios de Estonia, desde su independencia (BBC News, 2007).

Ante esto, las autoridades estonias convocan a reunión del Comité de Crisis, un órgano gubernamental que opera en situaciones políticas extraordinarias que comprometan la estabilidad y seguridad del país. El Comité está integrado por el Primer Ministro, Andrus

Ansip, el Ministro de Defensa, Jaak Aaviksoo, y es precedido por el ministro del Interior Jüri Pihl (Eesti Päevaleth, 2007). Si bien, los tres miembros del gobierno consideran que el eje central de la sesión abordará la inestabilidad política, que acontece en las calles, reciben una noticia paralela a los disturbios. Desde las 10:00 p.m., los sitios web gubernamentales han recibido un tránsito inusual de datos que ha causado inestabilidad en los portales *online* y servicios estatales. Los correos institucionales y de los funcionarios del gobierno se llenaron en pocos segundos de *spam* y son inoperables. El sitio de internet del Parlamento y la página del Primer Ministro han sido *hackeadas*, al parecer todo se debe a un ataque de tipo *DDoS*[2], No obstante, éste es tan severo y coordinado que hasta el sitio *valitsus.ee/et,* que conjunta toda la información y sirve de guía para los servicios públicos del *Vabariigi Valitsus* o Gobierno de la República, es inoperable (Schmidt, 2013). En un instante, los disturbios y protestas que comprometen la seguridad nacional del Estado se han movido de las calles al ciberespacio.

Pronto, la amenaza se extiende a servidores de internet privados. Los portales de noticias, como el *postimes.ee* –uno de los más visitados en Estonia- empiezan a formar parte del ciberataque, y para su sorpresa, los comentarios negativos sobre notas gubernamentales han sido enviados a los correos de múltiples instituciones y funcionarios estatales. Lo que satura el tránsito de datos y les imposibilita de compartir contenido sobre lo que está sucediendo en ese momento en las calles. El siguiente sector en mostrar fallas son los sitios de instituciones bancarias, con la misma técnica de satura a través de sobrecargas de información, los bancos se ven obligados a suspender el uso de los cajeros electrónicos y todos los servicios que se realizan por internet. Por último, las páginas de organismos internacionales como la Unión Europea, OTAN o la ONU, que operan con contenido local en Estonia, sufren el mismo destino (Detlefsen, 2015).

[2] *DDoS* son las siglas en inglés de *Denial of Distributed Service* o "Denegación de Distribución de Servicio", una de las técnicas de ataques a través del ciberespacio más utilizada por *hacker*s o *cracker*s. Su finalidad es hacer inaccesible o inoperable una red de internet o sistema computacional a sus propietarios o usuarios legales. La técnica de un ataque *DDoS* consiste en la saturación de los puertos de un sitio de internet a través de la sobrecarga de información inusual a un portal en internet. Para esto es necesaria la utilización de una red de *bots* o robots informáticos programados para enviar contenido que satura la línea, desde múltiples puntos geográficos, hasta dejar inoperable el portal objetivo. La técnica de *DDoS* es de las más sencillas y efectivas para quebrantar un sitio web.

En vista de la magnitud del problema, el Comité de Crisis convoca a una reunión extraordinaria que involucra a todos los funcionarios de gobierno. La resolución que alcanza el Presidente y el Primer Ministro es la del traslado inmediato del *Soldado de Bronce* para evitar peores disturbios, tanto en las calles, como en el ciberespacio. A primeras horas del 27 de abril, la policía acude a la Plaza Tõnismägi y retiran el monumento. Para este momento, el gobierno de Estonia ha identificado que las direcciones de los protocolos TCP/IP[3] que saturan todos los servicios de internet del país tienen origen en Rusia. A pesar de esto, lo más agravante es que los ataques empeoran cada minuto y se intensifican, a tal grado que se estima un millón de *bots*, con una sofisticada coordinación, están implicados en el ciber ataque. Ante la severidad de los ataques se comienda al *Equipo de Respuesta de Emergencia Informática* (*CERT*, por sus siglas en inglés) estructurar un plan de acción para revertir la agresión (Nguyen, 2013).

Mientras tanto, las calles de Tallin viven su segundo día de disturbios consecutivos. En esos momentos, una de las principales interrogantes de la urbe embravecida es: ¿dónde se encuentra el *Soldado de Bronce?*, desde su remoción la estatua fue trasladada a una ubicación secreta que mantiene a los manifestantes en estado de histeria. Pronto, en portales de noticias rusos empiezan a compartirse notas que expresan que la estatua ha sido destruida, y los restos de los soldados del mausoleo, también. Incluso, un sitio muestra una foto en la que puede observarse al monumento desintegrado en múltiples partes que hacen más creíble esta información, que es atribuida al Servicio de Prensa del Gobierno Estonio. Lo anterior, incrementa los niveles de violencia, el caos y la confusión para cometer saqueos en locales y negocios de la ciudad. Al terminar la jornada, los daños se estiman en 99 actos reportados de vandalismo y la cifra de heridos ha ascendido de 153 a 300, mientras que los arrestados de 800 a 1000 (BBC News, 2007).

Mientras tanto, el CERT presenta ante el gobierno su plan de acción para detener el ataque *DDoS*. Los ejes de acción del programa se centran en tres puntos clave: 1) incrementar la capacidad de los servidores de internet para poder manejar el exceso de tráfico de datos; 2) implementar un filtro que separe el tráfico de buenos mensajes de los falsos o fraudulentos

[3] TCP/IP son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés *Transmission Control Protocol/Internet Protocol*), un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

asociados a una ciber amenaza; 3) trabajar en conjunto con las autoridades para identificar la raíz de los servidores *DNS*[4] que utilizan los *bots* fuera del país. En adicional, el CERT sugiere bloquear todos los sitios de internet del país a usuarios foráneos y sólo permitir su acceso a usuarios nacionales. A la par de bloquear todos los dominios *.ru* (provenientes de Rusia), dado que se estima que el 99% del exceso de información proviene de ese país (Detlefsen, 2015).

El plan resulta exitoso y los incidentes disminuyen los días 28, 29 y 30 de abril. A pesar de la pacificación de las protestas de Tallin y la retoma del control y operatividad de los sitios de internet del gobierno, en la última jornada el Ministerio de Relaciones Exteriores notifica al gobierno estonio una nueva problemática: su Embajada, en Moscú, ha sido asediada por manifestantes rusos que condenan el traslado del *Soldado de Bronce* y proclaman que se dé a conocer la ubicación del monumento y su estado (TIME, 2007). En pocas horas, el edificio es bloqueado completamente para su acceso y el Presidente Toomas Hendrik reclama al gobierno ruso su poca disposición para defender a la representación diplomática y su personal. Por su parte, el gobierno del Kremlin no realiza acción alguna para atender la petición, hasta que el 2 de mayo la embajadora Marina Kaljurand es atacada en su automóvil durante un traslado de trabajo y el gobierno de Estonia declara la evacuación de la titular y todos los funcionarios de la misión (Iltalehti, 2007). En los próximos días el gobierno estonio adjudicó la responsabilidad de los ciberataques al Kremlin. No obstante, la imposibilidad de determinar la localización exacta de las direcciones TCP/IP no permitió a las autoridades atribuir completamente el ciber ataque a la potencia eslava. Al mismo tiempo que el gobierno ruso negó injerencia alguna o responsabilidad en los sucesos del 27 de abril (Sputnik, 2007).

Ante esto, el gobierno de Estonia apeló frente a la Unión Europea (UE) la necesidad de presentar una queja derivada de la conducta de su vecino del este en la cumbre UE-Rusia, que se celebró el 17 de mayo. En este evento, el Consejo de Europa sólo hizo alusión al bloqueo de la Embajada de Estonia en Moscú y la nula acción del Kremlin por este evento, así como el incumplimiento de la obligación de proporcionar seguridad a los diplomáticos de acuerdo con la Convención de Viena de 1961. Sin embargo, no se refirió en concreto a los

[4] Un servidor DNS en informática responde a las siglas *Domain Name System*, estos permiten conocer los nombres y ubicación en las redes, como las de Internet o las de una red privada. Es decir, se conoce la dirección IP de un computador, donde está alojado geográficamente, el dominio del portal al que se accede.

ciberataques (El País, 2017). También, el gobierno estonio presentó el caso a las autoridades de la OTAN y personal de la alianza atlántica visitó Tallin en los días posteriores a la crisis cibernética. Ante ellos, el Presidente Hendrik y el Ministro de Defensa, Jaak Aaviksoo, proclamaron el artículo 5 del Tratado del Atlántico Norte, que cita: *"un ataque armado contra uno o varios aliados, en Europa o en América del Norte, será considerado como un ataque dirigido contra todos".* Además de enfatizar que el tratado de la OTAN contemplaba amenazas terrestres, marítimas o aéreas, más no ataques a a través del ciberespacio. El mensaje llegó hasta el Secretario General del organismo, Jaap de Hoop Scheffer, quién atendería la petición e incluiría a los ciber ataques y ciber amenazas como parte de las injurias y agresiones en contra de los países miembros de la alianza militar. Por último, la OTAN promovería la creación del Centro Cooperativo de Ciber Defensa de Excelencia (*NATO Cooperative Cyber Defence Centre of Excelence*), con sede en Tallin, con la finalidad de realizar estudios en aras de mejorar la capacidad, cooperación e información entre los miembros del organismo en el ciberespacio (Foreing Policy, 2017).

Hasta nuestros días, la responsabilidad de Rusia en la coordinación y perpetración del ataque no ha sido probaba. Y los *hackers* operadores y ejecutores del ataque nunca lograron ser localizados o juzgados por sus acciones.

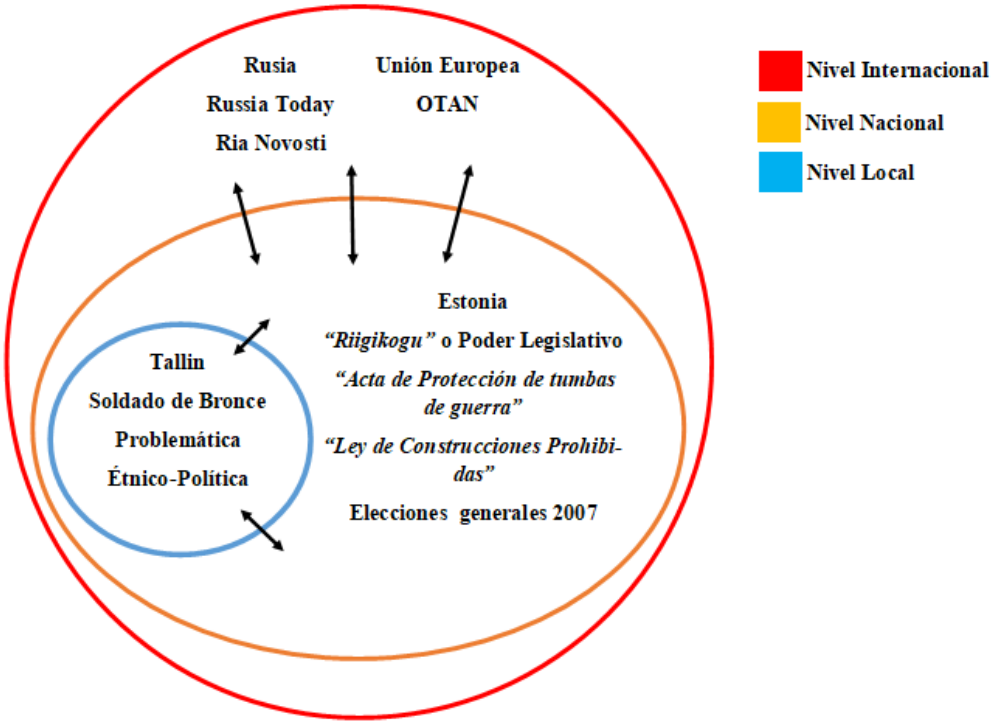
1.2 El ciberespacio: ¿una nueva arena de la política internacional?

Los ciberataques de Estonia, de 2007, son considerados dentro de los estudios de ciberseguridad como el primer caso de trascendencia global que comprometió la seguridad nacional de un Estado-Nación con consecuencias y daños a su soberanía, seguridad nacional y política exterior. Las esferas de análisis derivados de este evento son de múltiples niveles y requieren de una perspectiva transdisciplinarias para su comprensión y abordaje.

En primera instancia, se resalta como una problemática de nivel local, derivada de la crisis política de identidad, que promovió el traslado del *Soldado de Bronce*, se transformó en un problema de seguridad pública local, para posteriormente volverse un tema de defensa de la soberanía y seguridad nacional de una amenaza exterior (ciberataque *DDoS*). Y, finalmente, transformarse en un tema de agenda de política internacional que el gobierno de Estonia llevó a múltiples organismos regionales o internacionales como la Unión Europea o la

Organización del Tratado del Atlántico Norte (OTAN). De esta forma, la Figura 1 ilustra como la problemática en torno a los ciberataques de Tallín atravesó diferentes esferas de la influencia de la política nacional e internacional, mostrando la complejidad de las ciber amenazas y la utilización del ciberespacio como instrumento para vulnerar la seguridad nacional de un Estado-Nación.

Figura 1. Esferas de influencia del ciber ataque de Tallin (2017).



Fuente: Elaboración propia.

Para varios autores, el ejemplo de Estonia implica el primer caso real de *ciberguerra* en la historia moderna. Para otros, solo refleja el potencial que tiene el ciberespacio para influenciar en los eventos políticos del mundo real y los conflictos entre diferentes actores estatales, políticos o sociales. No obstante, las sentencias vertidas sobre este referente llevan a los mismos cuestionamientos: ¿Por qué estudiar el campo cibernético? ¿Hay una revolución en la política internacional vinculada al ciberespacio? ¿Deben articular protocolos y tácticas de seguridad los gobiernos para la regulación del ciberespacio? ¿Cuál es el potencial real del ciber peligro dentro de la seguridad nacional de un Estado? ¿Cuál es el margen de poder real o tangible del ciberespacio en la política internacional?

Desde la creación del internet, en 1969, con el proyecto ARPANET, hasta nuestros días, la función central del ciberespacio es ser un medio de intercambio y carretera para el flujo de información. En la actualidad, el internet es un servicio global necesario e inmerso en todos los campos de la vida cotidiana, que detenta 3.4 billones de usuarios, 47% del total la población global (ICT, 2017). Sus funciones, usos y esferas de influencia se han extendido del objetivo de ser una red de información entre universidades y el Departamento de la Defensa, de los Estados Unidos, ante situaciones de crisis. A un medio de intercambio de noticias, ocio, entretenimiento, comercio, prestación de servicios bancarios y gubernamentales, control de infraestructura crítica, etc., con capacidad de influencia en temas políticos, económicos, sociales, de libertad de prensa u opinión pública. Asimismo, destaca la diversidad de usuarios que han accedido a este campo en los últimos cincuenta años, de un uso restringido por parte del gobierno, para después diversificarse a empresas y ciudadanos comunes que requieren de él de forma imprescindible.

En los estudios de Relaciones Internacionales, vinculados a tópicos y análisis referentes al Estado-Nación, se debate si el internet y sus capacidades de poder e influencia están promoviendo una revolución en cómo se entiende la política internacional (Kello, 2013), de lo que nace la necesidad de su estudio, comprensión y análisis por parte de teóricos y tomadores de decisiones gubernamentales. Por otra parte, autores como Hughes (2010) y Dobbins *et al.* (2015) expresan que el internet es un nuevo campo de confrontación bélica e influencia de poder, como lo fue en el pasado el campo terrestre, marítimo, aéreo o espacial, por lo que es necesaria la creación de un *Tratado del Ciberespacio* que debe ser regulado por un régimen global, basado en normas y leyes para su control, en el que será vital la participación de actores clave, como países líderes de la comunidad internacional y empresas privadas. En ese sentido, la idea de un régimen del ciberespacio lleva otro debate: la definición y negociación de las responsabilidades, derechos y límites de acción de las partes de interesadas en su vigilancia. Lo que deriva, en que el ciberespacio se transforme en un espacio de securitización, en el cual debe construirse una gramática de seguridad para su uso y control (Hansen y Nissenbaum, 2009).

En los hechos, desde hace más de una década, el contexto internacional, las dinámicas y procesos políticos, han estado vinculados fuertemente al internet como instrumento y arena

de poder, capaz de impactar en la agenda global y de múltiples gobiernos. Entre estos se encuentra el *Cablegate* de los 251, 287 documentos del Departamento de Estado, de EE. UU., filtrados por Wikileaks durante 2010 y 2011. Evento que se transformó en la extracción ilegal de información más grande que haya sufrido un gobierno en la historia reciente del internet y generó un debate sobre el carácter secreto de la política y las comunicaciones diplomáticas, además de sentar un referente sobre la transparencia global de los gobiernos (Medcalf, 2011). A la par que el contenido de los cables, así como el modo en que el personal diplomático que los redactó se expresaba de diferentes mandatarios del mundo, causó tensiones entre Estados Unidos y sus aliados, que derivaron en quejas diplomáticas externadas al gobierno de Washington y en la afectación a su imagen pública internacional (Ghori, 2011a; Farrel & Finnemore, 2013).

Otro caso de relevancia se presenta con el papel que jugó el uso de las redes sociales en el derrocamiento de dictaduras militares en Medio Oriente, durante la *Primavera Árabe*. Dado que durante la década de los noventas países del Magreb como Túnez, Egipto, Libia o Siria, mantuvieron tasas de crecimiento económico elevadas, que si bien no reflejaron un desarrollo social inclusivo, sí promovieron cambios estructurales dentro de las clases media de estos países. Entre los que destacan el mayor acceso de las nuevas generaciones a estudios profesionales o posgrados, inclusión de las mujeres en los mercados laborales, una disminución considerable de la brecha digital y una expansión del uso del internet entre la población más joven (Ghanem, 2016). Durante el período 2000-2009, el incremento de usuarios de internet en los países árabes registro una tasa anual de crecimiento del 920%, y se estima que las personas con acceso a esta red pasaron del 4.5% al 20% durante la primera década de siglo XXI en países como Túnez y Egipto[5] (Kamel *et al.*, 2009; Bachrach, 2011).

Para varios autores, este incremento en el uso de internet como medio de ocio o consulta ayudó a un amplio grupo de la sociedad a evadir los controles de censura de los regímenes

[5] El papel del control del internet como tema de seguridad nacional y su uso por sectores sociales para la crítica y construcción de protesta en el Medio Oriente presenta un caso de análisis interesante de interacción entre actores estatales e individuales que se traslada del ciberespacio al espacio físico. Los textos dan un análisis de interés de cómo los países con mayor número de usuarios de internet fueron aquellos que derrocaron con mayor facilidad y eficacia al régimen político, así como se estima que los que tenían menor acceso a esta tecnología afrontaron más dificultades, como es el caso de Libia, o inclusive, Siria, en el que el control de internet (así como fuerza del Estado) eran más fuertes a tal grado que las protestas no lograron derrocar al régimen de Bashar Al-Asad.

autoritarios y afianzó la crítica razonada respecto al gobierno. Lo que promovió debates sociales en torno a su legitimidad a través de plataformas como *Facebook* o *Twiiter,* para cimentar una identidad progresista que derivó en las manifestaciones en contra de mandatarios como Hosni Mubarak, Zine El Abidine Ben Ali o Muamar El Gaddafi.

En los hechos, el gobierno egipcio, y menor medida el tunecino, intentaron bloquear el acceso a portales ICT una vez que la convocatoria de las protestas había alcanzado un margen que empezó a comprometer la estabilidad del régimen político (Aouragh, 2012). Situación que impactó en acciones de política exterior de otros actores globales, como Estados Unidos, dado que el *New York Times* externó en junio de 2011 que el gobierno del presidente Barack Obama ordenó a un conjunto de empresas estadounidense fortalecer la red de internet de los manifestantes y disidentes de los países del Medio Oriente (Ghori, 2011b). Operación que fue supervisada por la entonces Secretaria de Estado, Hillary Clinton, y se cree tuvo una fuerte influencia en el caso egipcio y la caída de Mubarak. Hecho que revela la capacidad del internet para comprometer la sobrevivencia de un régimen político, que de forma evidentemente, es un tema de seguridad nacional.

En ese sentido, para muchos países y regímenes políticos –ya sean autoritarios o democráticos-, la regulación y el control del internet es un tema de seguridad nacional que se extiende a Estados como China, Corea del Sur e Irán. El caso de la República Popular de China, contrasta fuertemente con lo acontecido en los países árabes, ya que desde la expansión del uso del internet en la década de los noventas, el gobierno del Partido Comunista Chino desarrolló una regulación de los contenidos en red que incluyó a instancias gubernamentales como la Comisión Estatal de Educación China y el Ministerio de Información Industrial, para crear una muralla digital que regula el contenido de toda la red en el país asiático (Harwit y Clark, 2001), a tal punto que se reguló el flujo de la información en los dos primeros buscadores web de China para solo presentar contenidos con un discurso político neutral. A la fecha, el control de los sitios y bases de datos en ese país siguen bajo un estricto control de seguridad informática que neutralizan el nacimiento de cualquier discurso antisistema entre la población civil con gran efectividad (Tang y Huhe, 2014; Yingfa y Hongna, 2014).

También, las acciones de ciberseguridad son una práctica implementada por el gobierno de la República Islámica de Irán. Sin embargo, a pesar de que este país usa métodos y acciones de control de contenido semejante a los utilizados por China, el régimen iraní ha promovido la creación de sitios en línea, blogs, redes sociales o páginas de ocio en que se refuerce la identidad musulmana chiita y los valores sociales referentes al Islam, permitiendo un nivel de diálogo social y político dentro de su población, siempre y cuando este se mantenga dentro de los límites del Corán y sus valores religiosos (Nazeri, 1996; Tkacheva, 2013).De esta forma, cada uno de estos eventos ha servido para exponer entre los debates actuales del ciberespacio el concepto de seguridad vinculada al internet, así como explicar su importancia y papel dentro de la seguridad nacional de los Estados.

Entre los principales casos de análisis, dentro de los estudios de ciberseguridad, se encuentran -junto al ciberataque de Estonia-, el gusano de *Stuxnet*, en 2010, y *LulzSec*, en 2011. El primero correspondió a la utilización de un virus o *malware* programado para atacar un determinado objetivo de sistema computacional, en específico, el referente al equipo encargado de controlar el enriquecimiento de uranio de la Central de Nuclear de Natanz, Irán. Se especula que el *malware* fue creado en colaboración entre los gobiernos de Israel y Estados Unidos, en conjunto con la empresa *Microsoft* (Detlefsen, 2015). El caso de *Stuxnet* es de relevancia dado que fue un virus con un diseño direccionado a atacar un sistema computacional e infraestructura especifico, dentro del marco de esta ciber operación, que se creé, inició en 2008. El objetivo de *Stuxnet* fue las centrifugas *Siemens S7-315*, encargadas del sistema de presión que controlaba el proceso de enriquecimiento de uranio de la central de Natanz (Lagner, 2011). Para esto, el *malware* se disfrazó de una actualización del software de *Siemens* encargado del controlador de las centrifugas, el cual infectó a las computadoras a través de una USB y alcanzó un total de 1,000 equipos hasta enero de 2010, año en que fue descubierto por inspectores de la Agencia Internacional de Energía Atómica. En ese punto, el personal científico de Natanz se dio cuenta que el virus había dejado sin funcionamiento veinte por ciento del total de las centrifugas (Matrosov, Rodionov, Harley & Malcho, 2010). Stuxnet under the microscope. ESET LLC (September 2010). Daño que atrasó por tres años el desarrollo del Programa Nuclear Iraní y que transformó a *Stuxnet* en la primera *ciber arma* que dañó infraestructura física crítica del mundo real.

Por otra parte, el caso LulzSec[6] hace referencia a la declaración que hizo este grupo *hacktivista*, durante 2011, de que realizaría cincuenta días de ciberataques a diferentes empresas y páginas de internet de organismos gubernamentales de Estados Unidos, como una forma de protesta ante compañías bancarias como *PayPal* y *Mastercard*, dado que estas habían implementado acciones para evitar que el sitio Wikileaks pudiera recibir fondos de usuarios a través de plataformas web (Yang, 2013). Durante el período de tiempo establecido, LulzSec hackeó sitios de internet de organizaciones privadas y públicas indiscriminadamente, entre las que se encontraron *American Online,* AT&T, la CIA, el Senado de Estados Unidos, Sony, PBS, y algunos sitios del FBI. Después del cumplimiento del plazo establecido, los ataques terminaron y múltiples gobiernos empezaron aplicar procedimientos jurídicos para encarcelar a los implicados. Esta acción requirió de una coordinación entre autoridades de impartición de justicia británicas –como la Policía Metropolitana de Londres- y estadounidenses –el FBI-, quienes descubrieron que los *hacktivistas* de LulzSec provenían de diferentes sitios como Estados Unidos, Gran Bretaña e Irlanda (Aaron, 2012; Pendergrass, 2012). Para 2012, la colaboración entre estos dos países permitió la captura del líder de LulzSec, Xavier Monsegur (quien posterior se volvió informante del FBI) y consecuentemente de todos los demás militantes de la organización, quienes recibieron una pena de veinte meses a diez años de prisión por sus delitos cibernéticos (Murphy, 2012).

En los hechos, casos como los de *Stuxnet y LulzSec* han promovido el desarrollo de Estrategias Nacionales de Ciberseguridad (ENCS) por diferentes países del mundo, rama de la seguridad nacional que es considera como un factor crucial para salvaguardar la integridad de los Estados-Nación. A la fecha, se estima que un total de 106 países del mundo detentan Estrategias Nacionales de Ciber Seguridad, de los cuales 27 pertenecen a la OTAN, 40 a Europa (considerando a los 27 miembros de la Unión Europea y 13 países no miembros), 55 de África (considerando a la Unión Africana y 13 países con estrategias autónomas), y 9 en América Latina y el Caribe (CCDCOE, 2021). Lo que denota un incremento importante en la preocupación y atención de los gobiernos por comprender el manejo del ciberespacio, crear

[6] Acrónimo para el nombre del grupo de hacktivistas Lulz Security.

instrumentos para la defensa de su seguridad nacional y mecanismos de acción vinculados a estos campos para explotar a través de la política exterior.

Antes de empezar el análisis sobre el trascendente papel del internet en las esferas de influencia, y los canales de comunicación de las dinámicas de la sociedad internacional, es necesario que entendamos el régimen hibrido de ciberespacio. Del mismo modo, abordemos el concepto de ciberpoder, y los conceptos clave para entender su lógica e impacto en las relaciones internacionales.

1.3 El régimen híbrido del ciberespacio

"El ciberespacio es un régimen híbrido de componentes físicos y virtuales que coexisten en el mundo real" (Nye, 2010; Demchack, 2012). Esta es la primer noción clave que debemos analizar para entender el potencial del internet como nueva arena de la política internacional y su influencia en los conflictos o dinámicas globales. Sin embargo, ¿a qué nos referimos estrictamente con un régimen híbrido? Para entender está noción debemos establecer cuáles son los elementos físicos del ciberespacio y diferenciar estos de los componentes virtuales, así como los fenómenos en los que ambas narrativas se interponen y que serán de nuestro interés.

En la actualidad, el internet, junto con las Tecnologías de Información y Comunicación (TIC´s) es un recurso crucial de los gobiernos, una parte de la infraestructura nacional crítica, y un elemento clave del desarrollo socioeconómico (Hathaway y Klimburg, 2012). Su uso se vincula al crecimiento y modernización de las naciones prosperas, y se estima genera ganancias de más 4.2 trillones de dólares tan sólo entre los países del G-20, esto representa, en promedio, 8% del PIB de cada país en el grupo. Asimismo, si el internet pudiera representarse como una economía, sería la quinta economía más importante del mundo, tan sólo detrás de Estados Unidos, China, Japón e India (Dean *et al.*, 2012). En datos concretos, el comercio electrónico y actividades económicas vinculadas al internet detentan un valor de 1.474 trillones de dólares (Kemp, 2018). Lo que denota su trascendencia en términos de la economía global y su capacidad para influenciar en diferentes áreas de la sociedad como la salud, educación, servicios financieros básicos, agricultura, etc.

Paralelo a los beneficios monetarios que genera, el internet también posee una fuerte regulación y control de los gobiernos para su uso y explotación. En el Informe *Freedom of*

the Net[7] de 2018, sólo 23% de los países evaluados mantenían un acceso libre dentro del ciberespacio. Mientras que 28% mantenían un acceso parcialmente libre y 36% eran calificados como redes no libres. En compañía de estas cifras, se estima que múltiples regímenes gubernamentales comúnmente utilizan tácticas de manipulación política al interior de los sitios web de su país para neutralizar el debate o la discusión política entre la opinión pública nacional (Freedom House, 2017). Entre las que destacan la realización de prácticas como creación de medios de comunicación pro-gobiernos (33 países de 65), pago por comentarios pro gobierno (30 de 65), creación y utilización de *bots* políticos (20 de 65), promoción de noticias falsas en elecciones (16 de 65) y hackeó o secuestro de cuentas contestarías (10 de 65).

Asimismo, el ciber crimen, definido como las prácticas ilícitas o al margen de la ley realizadas a través del ciberespacio, se ha vuelto una de las industrias ilegales más rentables del mundo y se estima que por estas prácticas anualmente se pierden 6 trillones de dólares en daños al sector privado (Jayanthi, 2017). Entre los costos de daño a empresa y personas se incluyen destrucción de datos, robo de dinero, pérdida de productividad, hurto de propiedad intelectual y datos personales, malversación, fraude, pornografía infantil, tráfico de drogas, trata de personas, eliminación de datos, sistemas pirateados y daños a la reputación (Morgan, 2017). Cada uno de estos casos, nos denota una serie de eventos en que el mundo físico y el virtual se interponen para crear dinámicas o procesos sociales que afectan al mundo material, lo que muestra una dinámica en que el espacio físico puede impactar en el internet y viceversa. Casos como estos serán nuestro objeto principal de interés y unidades de análisis.

1.3.1 El régimen de lo *cíberfísico*

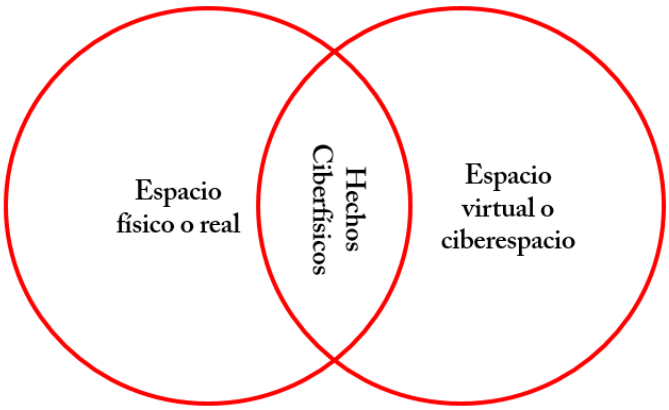
Los ejemplos anteriores, centrado en el desarrollo económico de los países y uso de TIC's, control político y libertad de opinión en internet, ciber crimen, etc., en conjunto con los casos de estudios presentados en la sección anterior (*Wikileaks*, Primavera Árabe, *LulzSec*, *Stuxne*, control del internet en China e Irán, y los ciber ataques de Estonia) son el marco de referencia

[7] El informe *Freedom of the Net (FN)* es una publicación realizada por *Freedom House,* un *think tank* con sede en Washington, D.C., Estados Unidos. La organización realiza investigaciones en torno a la promoción de la democracia, la libertad política y los derechos humanos. El informe *FN* presenta cifras y estadísticas en torno al uso libre de internet respecto a libertad de expresión y prensa en temas políticos en 65 países del mundo, que en conjunto, detentan el 87% de los usuarios globales de internet.

para entender el régimen *ciberfísico* que posee el ciberespacio. No obstante, primero debemos explicar y definir el sentido de este término y el porqué lo utilizaremos.

El concepto *ciberfísico* representa una categoría de análisis para delimitar los eventos, casos o unidades de estudio en que las dinámicas o procesos sociales que vinculan al internet y el espacio físico tienen repercusiones, impacto o consecuencias en la condición del Estado-Nación y sus componentes, con principal atención a casos que vulneren la integridad de la seguridad nacional o política exterior (Aguilar-Antonio, 2019). La idea anterior argumenta, que para que un caso de estudio de un evento del ciberespacio se transforme en un elemento de interés para los estudios de seguridad nacional y relaciones internacionales, es necesario que los hechos derivados de éste tengan una materialización en el espacio físico y una implicación desde el espacio virtual. Es decir, que una acción o suceso gestado en el internet, se traslade a un evento del mundo físico o viceversa como se presenta en la figura 2.

Figura 2. Hechos ciberfísicos en el régimen híbrido del ciberespacio



Fuente: Aguilar-Antonio (2019).

En ese sentido, se destaca que los campos de manifestación de los hechos *ciberfísicos* pueden contemplar cualquiera de los canales de comunicación típicos de la sociedad internacional y sus actores: la diplomacia, la política, la economía, el comercio, la cooperación internacional, el conflicto, etc. La concepción de los hechos *ciberfísicos* responde a la noción de que el ciber espacio es un régimen hibrido con características materiales e inmateriales, ligadas al uso del internet y su capacidad de impacto en las dinámicas sociales (Nye, 2010; 2014).

Para mejorar la comprensión de los hechos ciberfísicos utilizaremos dos conceptos similares que pueden ayudar a su entendimiento. El primero corresponde al término *glocal*, y el segundo al enfoque de seguridad *interdoméstico*, ambos de surgimiento y gran popularidad durante la última década del siglo XX. El término *glocal* fue utilizado por los sociólogos, politólogos y economistas durante la década de los noventa para analizar los fenómenos y dinámicas sociales derivados del proceso de la globalización, en que la reducción de fronteras (económicas, financieras, políticas, etc.) cambió las características típicas de los fenómenos locales y globales entre los que era cada vez más indisociable determinar los límites de lo provinciano y lo internacional.

De esta forma, la palabra glocal surgió como un neologismo de la combinación de las palabras "local" y "global" (Martins, 2009). En sus primeras concepciones, la palabra se utilizó para describir el incremento de la superposición e interpenetración de las fuerzas de la economía política global y las respuestas a éstas de las comunidades local-regionales dentro de los parámetros de la particularidad, noción que influyó en una nueva escala del marco de análisis de la organización socio territorial del Estado-Nación (Taylor, 1996; Peck y Tickell; 1994, Beck; 1992; Brenner, 1998). Para varios autores, la globalización transformó las demarcaciones de territorios nacionales, regionales o locales para dar pasó a una nueva dimensión que se encontraba entre las dos esferas y las abarcaba. El concepto alcanzó tal popularidad que fue empleado por organismos internacionales y ONGs. Asimismo, se aplicó para analizar múltiples mecanismos desarrollados por procesos de integración económica - como fue el caso de la Unión Europea, el Mercosur, o el TLCAN (Brenner, 1998; Weber, 2007; Keeling, 2004), para explicar las dinámicas financieras y multiculturales que acontecieron en las grandes urbes del mundo, como Nueva York, Paris o Londres (Curtis, 2011; McNeill, 2001; Sidaway, 2006), o para presentar las procesos sociales derivados de fenómenos como la migración, con lo que se creó una categoría para unidades o casos de análisis de características y escala hibrida (Morawska, 2001; Hoerder, 2010; Van Wijk, J. y Bolhuis, M., 2017).

Por otra parte, el *enfoque de seguridad interdoméstico* surge en los años inmediatos al final de la Guerra Fría, como parte de una reconceptualización a la noción de la seguridad nacional más allá del paradigma del mundo bipolar, en el que imperó una visión centrada en la

integridad territorial de los Estados utilizado por entidades como la OTAN (Lindstrom y Luiijf, 2012). En el contexto posterior a este periodo, los creadores y encargados de estructurar políticas de seguridad encontraron que la visión centrada en mantener la seguridad territorial de los Estados era limitada frente a las nuevas amenazas y retos no tradicionales para la seguridad nacional. El debate se vio nutrido por nuevas nociones como la *seguridad comprensiva*, que expandió el margen de las políticas de seguridad a dominios como la alimentación, salud o medio ambiente (OSCE, 2009), la *seguridad humana*, que cuestionó la visión estado céntrica de la seguridad e incrementó el énfasis en las personas e individuos (UNDP, 1994, Chanona, 2015), o la *seguridad multidimensional*, centrada en el análisis regional o hemisférico en contra de las amenazas conjuntas (Benítez, 2005; Tulchin *et al.*, 2006; Mace *et al.*, 2012)

En este debate, la *seguridad interdoméstica* tomó aportes de la Escuela de Copenhague para su diseño que delineaban las condiciones de un problema de seguridad y la necesidad de atenderlo, para el caso concreto de la seguridad hemisférica del continente americano (Lenz-Raymann, 2014). Entre los principales aportes vinculados al enfoque de seguridad interdoméstico se encuentran la creación de *complejos regionales de seguridad,* que se insertó en las reinterpretaciones del concepto de seguridad más allá del aspecto militar, para incluir amenazas de diverso tipo y no tradicionales (Buzan *et al.*, 1998). En ese sentido, la creación de complejos de seguridad se vio potenciado por los acuerdos de cooperación (bilateral o multilateral) y los procesos de integración económica (TLCAN, Mercosur, Unasur) de las Américas, que promovieron transformaciones internas en los países y cambios en la estructura de la región respecto a la noción de nuevas amenazas. Lo que pasó a incluir problemáticas no militares, vinculadas a temas con actores no estatales y de carácter trasnacional en la visión de seguridad nacional, entre los que se incluyeron tópicos como el crimen organizado, narcotráfico, estabilidad política, secesión, migración, ecología, terrorismo, etc. Cada uno de estos factores fueron considerados amenazas regionales y domesticas en el hemisferio americano, es decir, nichos de conflicto que tienen una incidencia en el nivel interno de cada Estado, pero que de igual modo afectaban a la región o un conjunto de países, por lo que también eran un problema regional-internacional, que requerían acciones de los gobiernos locales y procesos de cooperación que involucraran a todos los actores afectados en la región.

La exposición anterior, nos sirve para presentar como ambas categorías (*glocal* y *seguridad interdoméstica)* surgieron como dos reconceptualizaciones para abordar nuevos fenómenos sociales, desde diferentes disciplinas y enfoques teóricos, para una serie de acontecimientos que no se ajustaban a la escala de lo local o global, o los enfoques internacional, regional o doméstico, sino que poseían características de más de uno de estos conceptos, y por lo tanto, requerían de un esquema de análisis hibrido. En ese sentido, la categoría de los hechos *ciberfísicos* es una comprensión que rescata la experiencia de la reconceptualización realizada por estos dos términos.

De esta forma, los casos de análisis que competen al ciberespacio, desde los estudios de política internacional y seguridad, se suman a esta serie de cambios en los fenómenos sociales que promovió la visión glocal e interdoméstica. Asimismo, se externa que la cada vez mayor interpenetración o superposición del ciberespacio en los hechos físicos o materiales, y viceversa, se ha visto influenciada por las transformaciones sociales de carácter internacional que sufrió el mundo desde el proceso de globalización que inicio en los noventa. Dado que el internet fue uno de los principales instrumentos que permitió el proceso globalizador y de reducción de fronteras que transformó las dinámicas y niveles de escala de los fenómenos sociales. No obstante, su nivel de complejidad tardó más tiempo en desarrollarse y ser observable como objeto de estudio.

Para el caso de la categoría de un hecho *ciberfísico* se aclara que esta dimensión sólo será tangible cuando los casos de estudio tengan algún impacto, consecuencia, repercusión o materialización tanto en el espacio tangible, como en el internet. De esta forma, los hechos *ciberfísicos* deben desenvolverse en dos narrativas: la material y la virtual. Además de poseer espacios de superposición o interpenetración que vinculen a ambas esferas. En la tabla 1 se presentan los seis eventos citados en la sección anterior presenta las dos narrativas de los hechos *cíberfísicos.* El acontecimiento más representativo en los estudios de ciberseguridad, los ciberataques de Estonia, nos muestra como un conflicto étnico-político de la población de éste país *se* transformó en un conflicto que afectó al espacio material y el ciberespacio. A la par que este evento detentó puntos de superposición e interpenetración que afectaron esferas como la política, económica, seguridad pública y nacional, etc. Este análisis aplica el

resto de los casos señalados, lo que ayuda a explicar las características del régimen híbrido del ciberespacio y los hechos ciberfísicos.

Tabla 1. Método de análisis de estudios de caso del ciberespacio

Casos de análisis	Narrativa virtual	Narrativa material
1. Ciberataques de Tallin	i. Ataque DDoS a todos los sitios gubernamentales y de empresas privadas ii. Interrupción de servicios bancarios y noticias.	i Conflicto étnico-político entre estonios y rusos. ii. Protestas sociales en Tallin.
2. Cablegate	i. Extracción de 251, 287 documentos del Departamento de Estado. ii. Publicación de los cables por el sitio Wikileaks y 5 diarios internacionales.	i. Tensión diplomática entre EUA y 16 países referidos en los cables. ii. Quejas diplomáticas de gobiernos señalados en los cables a EUA.
3. Uso de redes sociales en Primavera Árabe	i. Uso libre, sin restricciones, de internet para libertad de opinión en Egipto y Túnez. ii. Promoción de debates sociales y organización de protestas contra el régimen autoritario en Twitter y Facebook.	i. Protestas sociales y represión policiaca y militar de civiles. ii. Renuncia de los mandatarios o jefes de Estado y reestructuración política.
4. Stuxnet	i. Planeación y diseño de un ciber ataque entre actores estatales (EUA, Israel) y no estatales (Microsoft). ii. Creación de un malware con capacidad de afectar las centrifugas Siemens S7-315. iii. Infección de más de 1,000 sistemas informáticos en la Central Nuclear Natanz, Irán.	i. Daños a las centrifugas de la central nuclear de Natanz, Irán. ii. Daños a Infraestructura Nacional Crítica de Irán. iii. Retraso de tres años del Programa Nuclear iraní.
	i. Control de los contenidos de internet y espionaje del Estado de la población	i. Arrestó de opositores y uso de vigilancia de internet para contener protestas o utilizar

Casos de análisis	Narrativa virtual	Narrativa material
5. Regulación del uso de internet en China	en redes sociales por motivos de seguridad nacional. ii. Prohibición de redes sociales de occidente (Facebook, Twitter, etc.) por parte del gobierno, y cambio por una oferta nacional.	evidencia en juicios del Estado. ii. Uso económico del internet con fines para la economía China
6. LuzlSec	i. Protesta cibernética en contra de PayPal y Master Card. ii. Convocatoria y amenaza de ciber ataques a sitios de gobierno y empresas por 50 días y realización de los ciberataques.	i. Imposibilidad de uso de redes públicas (FBI, CIA) y privadas (Sony, AT&T). ii. Interrupción de comunicaciones y servicios gubernamentales. Y perdidas económicas de las empresas.

Fuente: Elaboración propia.

En consecuencia, el esquema anterior nos lleva un nuevo replanteamiento: especificar que compone la parte física y la parte virtual del ciberespacio. Aclaración que será importante para el uso, control o dominio de los Estados-Nación y otros actores de las relaciones internacionales de esta nueva arena de la política global.

1.3.2 La parte física del ciberespacio

La aclaración de las narrativas del ciberespacio nos lleva al entendimiento de que el mismo internet posee una *parte física* y una *parte virtual*. Señalar a qué componentes o características corresponden éstas es un hecho crucial que determinar la participación de un actor dentro del ciberespacio y su capacidad de influir en los hechos ciberfísico. En este sentido, nos ocuparemos en primera instancia de la *parte física* del ciberespacio, ligada a recursos materiales o tangibles.

El primer objeto de referencia para señalar la parte física del ciberespacio señala a la Infraestructura de Telecomunicaciones (IT), que representa el medio físico a través del cual se da la conectividad de internet y fluye el tráfico de información (Kittichaisaree, 2017). La infraestructura de telecomunicaciones ésta integrada por los *SITE*s, satélites, cables de fibra óptica, redes telefónicas y tecnología móvil de telecomunicación y TIC´s. El control,

regulación, e incluso posesión o acceso a este tipo de tecnología es un factor vital para los gobiernos nacionales que los involucra estrechamente con las empresas o entidades privadas, proveedoras de este servicio. En ese sentido, no resalta que la infraestructura de telecomunicaciones sea regulada por esquemas jurídicos públicos y privados, así como por niveles nacionales o internacionales. En la actualidad, todos los países cuentan con algún recurso de IT, que es considerada parte de la *Infraestructura Nacional Crítica,* así como legislaciones, códigos y normas que regulan su uso, control y acceso.

Por otra parte, el organismo internacional clave en la regulación de la IT es la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), que promueve reglas de coordinación entre los sistemas nacionales de telecomunicaciones de manera global, determina la localización de los espectros radiales de las redes web, y administra la posición de satélites. La ITU abarca un total de 893 miembros, de los cuales 193 son países y 700 organismos privados. También, la Organización Mundial de Comercio (OMC) juega un rol clave en las políticas de acceso, precios y liberación de mercados de internet.

A la par del gobierno y organismos internacionales, también debe destacarse el papel trascendental que juegan las compañías privadas (AT&T, Vodafone, Orange, etc.) quienes poseen el mayor porcentaje de la tecnología de IT y son los principales operadores que proporcionan el acceso a más del 90% de los actuales usuarios del ciberespacio (Winseck, 2017). Por último, otra componente que integra la infraestructura de telecomunicaciones incluye al *hardware*, es decir, a todas las partes físicas tangibles que integran un equipo de cómputo. Entre las cuales se pueden incluir *gadjets,* o instrumentos de acceso que permiten a los individuos hacer uso del internet y tener conexión a él, como Laptops, computadoras, *smartphones*, tabletas, etc. De hecho, se enfatiza que la capacidad y garantía de conexión, ya sea a través de posesión de IT o acceso a través de proveedores, será un factor crucial para que los Estados-Nación, o cualquier otro actor, puedan participar dentro del ciberespacio e influir en los hechos *ciberfísicos.*

De forma paralela a la IT, un componente trascendental para tener acceso, participación y dominio en el ciberespacio es la *electricidad* o *energía*. La IT, con las mejores conexiones satelitales y cables de fibra óptica, puede ser intrascendente si un Estado-Nación o actor con acceso a ella no posee los componentes energéticos para utilizarla e insertarse en la dinámica

del ciberespacio. Asimimo, los Estados-Nación y otros participantes inmersos en el internet deben poseer la *garantía de suministro de energía*[8] para poder formar parte de la dinámica del internet y los hechos ciberfísicos (Costigan y Lindstrom 2016; Eriksson *et al.*, 2009).

Por último, el tercer elemento clave de la parte física del ciberespacio está ligado a las *infraestructuras críticas* de los Estados, que comprenden a la infraestructura material vinculada a un espacio geográfico (local, nacional, regional o internacional) que suministra y presta servicios básicos o primordiales de los que depende el bienestar, progreso o modo de vida de un país y su población. De esta forma, la infraestructura crítica puede abarcar elementos como presas de agua, plantas eléctricas (de cualquier tipo, hidroeléctricas, nucleares, etc.), autopistas, puentes, rutas férreas que conecten ciudades o poblaciones, gasoductos o petroductos, satélites, cables de fibra óptica, etc. (Costigan y Lindstrom 2016; Johnson, 2009).

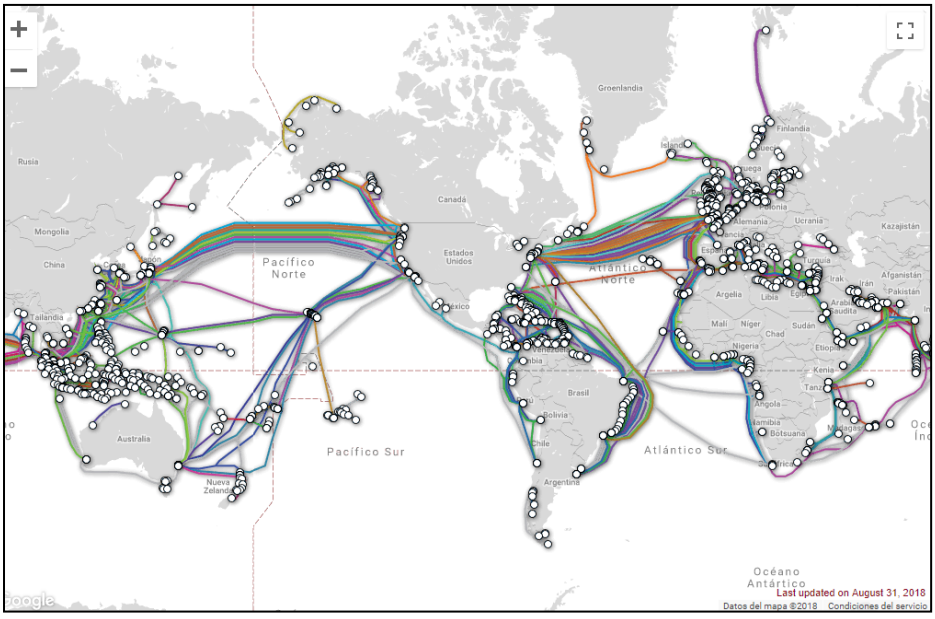
La importancia de este tipo de infraestructura oscila en el hecho de que la interrupción de su funcionamiento o suministro de servicios puede ocasionar severos efectos en el desarrollo de las actividades cotidianas de la sociedad. Esta característica hace que la infraestructura crítica sea considerada como uno de los componentes que integran las estrategias de seguridad nacional de diversos países y gobiernos alrededor del mundo. En la actualidad, el control y mantenimiento de la infraestructura crítica está bajo la responsabilidad de organismos públicos y militares (gobiernos u organismos internacionales y privados (principalmente empresas especializadas en cada rama de éstas). Asimismo, una gran cantidad de estas infraestructuras han empezado a utilizar sistemas informáticos o computadores para su funcionamiento, con aplicaciones ligadas a conexiones satelitales o redes de fibra óptica de internet (Hurwitz, 2012). En ese sentido, la afectación por parte de un ciberataque a cualquier infraestructura crítica de un país, con daños materiales, e incluso en costos de vidas humanas, puede ser considerada como el impacto más severo que puede presentar una ciber agresión.

[8] En esta parte de nuestro análisis, es importante destacar que utilizaremos más la categoría anterior, en vez de utilizar el concepto de seguridad energética, dado que ésta noción corresponde a un criterio más amplio que concibe el aval del suministro energético por parte del Estado de manera sostenible y económicamente viable, que formalmente forma parte de la doctrina de Seguridad Internacional que genera el gobierno de cada país (Yergin, 2006).

1.3.2.1 Un ejemplo de la parte física del ciberespacio: los cables marinos de fibra óptica

Para ejemplificar la importancia de la parte física del ciberespacio, utilizaremos la infraestructura de cables submarinos de fibra óptica de *Huawei. Technologie*s, empresa privada multinacional china, especializada en el desarrollo de tecnología de telecomunicaciones. A la fecha, Hauwei está incluida entre las cinco empresas más importantes a nivel mundial de telecomunicaciones, provee de espectro y conexión de internet y telefonía a un total de 35 empresas operadores de telecomunicaciones (entre los que están los más grandes de Asía y el Pacífico), y desde 2018, se ha posicionado como la segunda empresa productora y vendedora de *smartphone* a nivel mundial (Kaska, Beckvard y Minárik, 2019). La trascendencia de la red de telecomunicaciones de Huawei es la más importante de la República Popular de China, que proporciona conexión de fibra óptica de internet submarina a casi todos los países del mundo con litoral marino (casos excepcionales son el de Corea del Norte, que servirá más adelante para nuestro análisis), por lo que la infraestructura de Hauwei puede ser considerada también una parte importante de la *infraestructura crítica* del sudeste asiático y un vasto grupos de ésta zona del planeta (Frye, 2002), como se observa en la figura 3.

Figura 3. Cables submarinos de fibra óptica de Huawei Technologies.



Fuente: Submarine Cable Maps (2018)

Con base a la figura anterior, la infraestructura de Hauwei tiene conexiones en los cinco continentes del orbe, y centraremos nuestra atención en el caso de México (Figura 4). Si observamos las conexiones de cables de fibra óptica de México, se puede notar que tienen conexiones en cinco puntos de su litoral: cuatro en el Pacífico (dos ubicados en el Pacífico, en la costa de Tijuana y de Mazatlán, y dos en el mar de Cortés, en La Paz y Topolobampo) y dos en el Caribe (con conexiones en Cancún y Tulum).

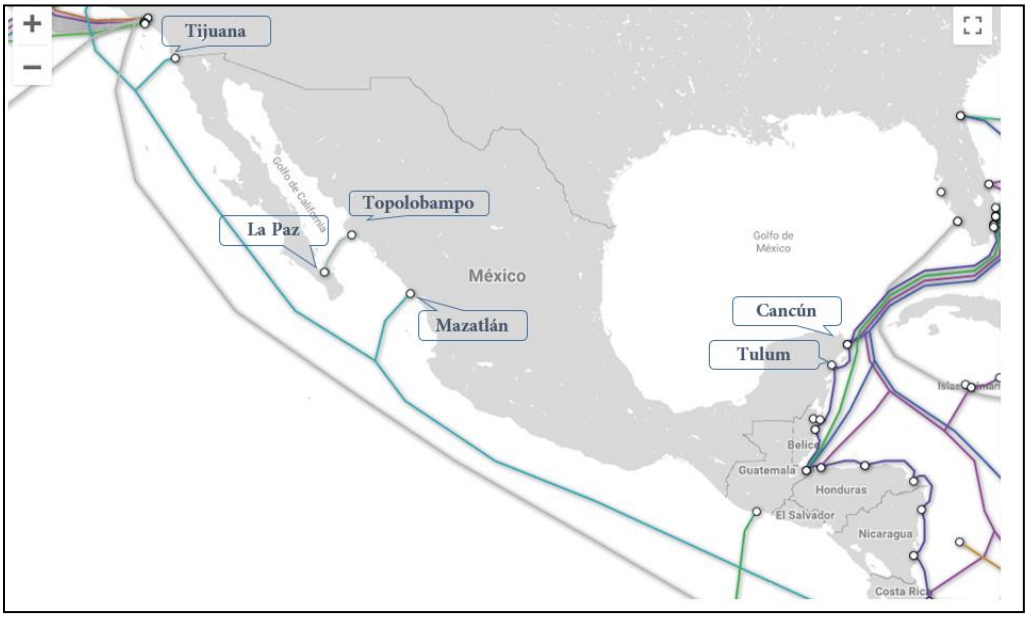
El cable de submarino que conecta con los litorales del Caribe es el ARCOS, esta infraestructura de fibra óptica conecta a Cancún y Tulum con otras 22 estaciones de telecomunicaciones asentadas en 18 países, tan sólo en el mar Caribe (Cable Map, 2018). No obstante, conexiones del cable ARCOS, en las Islas Británicas, Colombia, Venezuela, Costa Rica, hacen conexiones con más de cien estaciones en América del Sur, Europa y África. En el lado del pacífico el principal cable submarino de Hauwei es el *Pan American Crossiong (PAC)*, que conecta a México con toda la costa del Pacífico de América del Sur, y la costa Oeste de Estados Unidos.

Está conexión vincula las telecomunicaciones de México con más de siete regiones y más de ciento cincuenta estaciones en América, Asía y Oceanía. Los datos anteriores revelan la trascendencia de esta conexión de fibra óptica, la cual si sufriera algún tipo de daño, destrucción o inaccesibilidad causaría severos efectos en esta red. Dado que las conexiones de México, e interacciones de este país se verían interrumpidas con más de 250 estaciones en prácticamente todos los países del mundo (Cable Map, 2018). Escenario que puede tener severas repercusiones en el espacio *ciberfísico* para esferas como la economía, las finanzas, medios de comunicación, etc. Por lo que será un tema de seguridad, para el gobierno de México, y para la empresa de Hauwei, la integridad de las seis conexiones de fibra óptica, cómo un tema de *ciberseguridad* del Estado-Nación y de la empresa privada dueña de la infraestructura.

La necesidad del garantizar la protección y buen funcionamiento de este tipo de infraestructura lleva una reflexión. El suministro de internet de los cables de fibra óptica submarinos de Hauwei garantiza a múltiples gobiernos, así como a sus empresas y ciudadanos, la capacidad tener acceso al ciberespacio y da un potencial y margen de acción amplio para influir en los hechos *ciberfísicos*, esta condición está acompañada de uno de los

principales beneficios tangibles del ciberespacio: la prosperidad económica. No obstante, las conexiones con los cables ARCOS y PAC dan conexión a México con más de 500 estaciones, 190 países alrededor del mundo (Cable Map 2018). Lo anterior implica un margen alto del origen de ciberamenazas que pueden afectar algún sistema informático de este país y promover impacto en dinámicas sociales. La idea anterior lleva a deducir que un país sin acceso a estas conexiones de cables de fibra óptica vería afectada su condición de influir en el ciberespacio y los hechos *ciberfísicos.* Esta situación influiría en dos esferas: los beneficios económicos del uso del internet y el potencial de recibir ciberamenazas, que es visible en la figura 4.

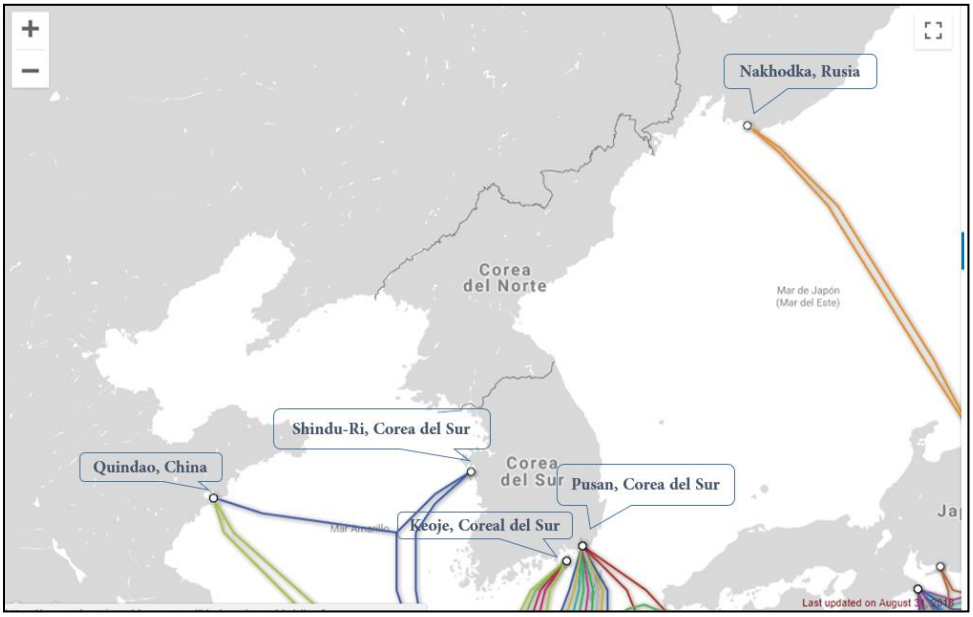
Figura 4. Conexiones de México a los Cables submarinos de Huawei Technologies.



Fuente: Submarine Cable Maps (2018)

Un ejemplo que puede verificar esta idea reside en el caso de la República Popular de Corea del Norte (lo que se observa en la figura 5). El *Submarine Cable Map* de Hauwei muestra que esté país no tiene ninguna conexión de fibra óptica submarina de esta empresa. Y las más cercanas se encuentran en Corea del Sur (las estaciones de Shindu-Ru, Pusam y Keoje), una en Rusia (Nakhodka) y una en China (Quindao).

Figura 5. Conexiones de Corea del Norte a los Cables submarinos de Huawei Technologies.



Fuente: Submarine Cable Maps (2018)

La información anterior nos lleva a la deducción de que los beneficios económicos y la participación de Corea del Norte en el comercio electrónico son muy bajos, o no se compara con la que pueden detentar sus países vecinos. En los hechos, la ITU tiene datos mínimos sobre los usuarios de internet de Corea del Norte, actualmente, se estima sólo hay 2 millones de usuarios en línea, de los 25 millones que habitan el país, y se contabiliza sólo existen 1,024 direcciones IP en todo el país (Warf, 2015). Si bien la anterior involucra una enorme brecha digital de este país con el resto del mundo, también existe un beneficio en cuanto a la seguridad nacional del Estado norcoreano. A razón, que este no formar parte de las redes de cables submarinos de fibra óptica hace que el potencial de origen de ciberamenazas para los sistemas computacionales norcoreanos se vean fuertemente limitados. Loque disminuye este origen de acceso a ciberamenazas, por el tipo de conexiones de internet que posee, que son vía satelital, en específico, con dos países, Alemania y China (con quien también cuenta con conexiones de fibra óptica vía cables terrestres).

1.3.3 La parte virtual del ciberespacio

El segundo componente de la narrativa del ciberespacio se refiere a la parte virtual vinculada al *internet,* ésta representará todas las esferas inmateriales que están inmersas en esta plataforma y que en conjunto conformaran al *ciberespacio* como arena de política. De esta forma, cabe aclarar que el concepto de ciberespacio es diferente al de internet, dado que el primero engloba al segundo y corresponde a una concepción más amplia de componentes, factores, dinámicas y actores.

Por internet se entiende al conjunto interconectado de redes de comunicación vinculadas a los protocolos IP (*Internet Protocol)* o ICT (*Transmission Control Protocol)* que permiten la conexión y tráfico de información a través de la red (Kello,2013). En conjunto, los protocolos en red se separan en cuatro tipos (aplicación, transporte, internet e interfaz) y tienen la finalidad de proveer una conexión para el flujo de información de punta a punta, es decir de un equipo o entorno a otro de semejantes características, con el paso integro de datos transferidos. En los hechos, la materialización del internet se observa en páginas web, sitios o blogs, redes de conexión *wi-fi* o alámbricas, aplicaciones, servicios bancarios o gubernamentales, etc. Cabe destacar que los protocolos de internet son diferentes de lo que se entiende como un *software* y se limitan a permitir el flujo de información a través del ciberespacio. En este sentido, será de importancia la indexación de información y la *superficie web* en la que es posible tener acceso a determinado tipo de datos, dado que se estima sólo una quinta parte de los sitios de internet son visibles a través de la *web superficial* (principalmente vinculados a buscadores en línea como *Google, Yahoo, etc.).* Mientras que la web profunda alberga más del ochenta por ciento de los sitios en línea y es de acceso restringido al gobierno, *hackers* o especialistas en programación, que poseen las capacidades para navegar a través de ella.

Otro elemento vital de la parte virtual del internet estará integrado por los *softwares,* que representan a los sistemas informáticos que crean los programas, sistemas operativos, lenguajes de programación, etc. En segunda instancia se encuentra el *hardware,* que permite que se puedan utilizar los equipos de cómputo que permiten el uso del ciberespacio a múltiples operadores. El concepto de software será de vital importancia para explicar los conceptos de *malware* y *ciber explotación* que se expondrán en el siguiente apartado, y que

se refieren a los programas informáticos diseñados y creados para extraer contenido de información de equipos informáticos, de acceso restringido, borrar los datos contenidos en ellos, interrumpir o modificar las funciones de sus programas o sistemas o bloquear el acceso a los usuarios legítimos.

Una vez aclarados los componentes del internet, procedemos a la conceptualización del ciberespacio. A la fecha, no hay una definición científica aceptada para este término y diferentes organismos internacionales, gobiernos, *think tanks* y teóricos han propuesto múltiples concepciones para alcanzar una resolución respecto a éste término. A escala global destacan las definiciones presentadas por la Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC) que describen al ciberespacio como:

> "*…el complejo ambiente resultante de la interacción de personas, software y servicios en el internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física"* (ISO/IEC, 2012, p. 9).

Por su parte, la ITU, prefiere utilizar el término de ciber ambiente, al que define como:

> "*los usuarios, redes, dispositivos, todo el software, procesos, información en almacenamiento o tránsito, aplicaciones, servicios y sistemas que se pueden conectar directa o indirectamente a las redes"* (ITU, 2012, p.7).

Por último, el CCDCOE, en su *Manual de Ciberseguridad*, presenta el siguiente concepto:

> "*El entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y espectro electromagnético, para almacenar, modificar e intercambiar datos utilizando redes informáticas."* (Klimburg, 2013, p. 14).

Las primeras dos definiciones (ISO/IEC e ISO) refrendan la importancia de los actores inmersos en la web y su interacción, para la creación del ciberespacio. Lo que denota, que más que sólo tráfico de datos e información, limitados al internet, el ciberespacio es una arena global en la que se desenvuelven fenómenos sociales. No obstante, ambas conceptualizaciones, limitan esta interacción a la narrativa virtual del internet. Noción que contrasta la definición del CCDCOE al aceptar que el ciberespacio no sólo detenta

componentes virtuales, sino también físicos, a la par de refrendar la importancia del control de datos e información en este campo. La visión de éste última institución, al ser un centro de investigación de la OTAN, acerca más el concepto de ciberespacio a las nociones de la seguridad nacional.

Respecto a los conceptos presentados por gobiernos nacionales, existen al menos veinticinco países que presentan su definición de ciberespacio, dentro de sus estrategias de seguridad, destacan las cercanas a la visión de la ISO y la ITU, que señalan las interacciones y fenómenos que vinculan a usuarios y portales de internet (Australia, Qatar, Países Bajos Japón, Alemania, etc.). Y las que definen al ciberespacio como un régimen híbrido, con parte física y virtual y con capacidad de impacto en hechos materiales de esferas como la economía, el comercio y política (Estados Unidos, Nigeria, Austria, Sudáfrica), con una concepción más emparentada al CCDCOE.

Para los teóricos de las relaciones y política internacional, como Joshep Nye (2010) el ciberespacio es:

> "*un régimen hibrido único de propiedades físicas y virtuales, en el que la capa virtual del ciberespacio se ajusta leyes económicas y costos marginales, leyes políticas de jurisdicción soberana y control gubernamental* (Nye, 2010, p.3)*".*

La definición de este autor se complementa con el concepto de *ciberpoder,* que presenta como "*la habilidad de usar el ciberespacio para crear ventajas e influenciar eventos en otros ambientes operacionales a través de instrumentos de poder".* Por lo que la perspectiva neorrealista de este autor da más énfasis a la consecuencia física y material que puede tener este campo informático. Por su parte, Lucas Kello (2013, p.10) describe al ciberespacio como:

> "*el conjunto de tres terrenos parciales de superposición, 1) el internet, que comprende a todas las computadoras interconectadas, 2) la "World Wide Web" consistente en los nodos de acceso a internet, 3) y el ciber archipiélago, que comprende todos los sistemas de computadoras que existen en seclusión teórica."*

Para Mayer *et al.* (2013, p. 3) el ciberespacio se define como:

> "*un dominio global y dinámico, sujeto a cambio constante, caracterizado por la combinación del uso de electrones y espectro electromagnético, que tiene la finalidad de crear, almacenar, modificar, intercambiar, compartir y extraer información, que incluye: infraestructura física y servicios de telecomunicaciones a los que es posible acceder por conexión de internet, sistemas computacionales, vinculados a software con operacionalidad y conectividad, redes dentro y entre sistemas computacionales, y constitución o almacenamiento de datos.*

Para esta propuesta de análisis, y una vez presentadas las diferentes conceptualizaciones de diferentes organismos y autores, el ciberespacio se entenderá como una arena de interacción compuesta por una parte virtual, integrada por una infraestructura web (protocolos de internet y softwares), y una parte física, (infraestructura de telecomunicaciones, critica y hardware), en que se suscitan dinámicas, fenómenos o hechos sociales en diferentes canales o esferas (política, económica, cultural, prensa, etc.), que poseen un potencial de transferencia o impacto de estos eventos al mundo material ,con repercusiones al contexto o integridad del Estado-Nación, gobierno o sociedad.

1.4 Conceptos claves para entender el ciberespacio

El contenido teórico y de ideas vertido hasta este punto de nuestro análisis puede aparentar que entender el problema del ciberespacio requiere de conocimientos en sistemas computacionales o algún margen de especialización técnica para analizar los temas de política internacional y seguridad nacional vinculados al internet. Para Lucas Kello (2013) esta falsa idea es uno de las principales limitantes actuales que impiden un desarrollo más amplio de los estudios de ciberseguridad por parte de las instituciones académicas, teóricos, gobiernos y creadores de políticas gubernamentales. En ese sentido, en este apartado introducimos dos clasificaciones de conceptos para entender los temas de análisis político internacional del ciberespacio (y que dan un gran margen de utilidad para estudio de casos) que denominaremos la *clasificación Kello y Klimburg.*

La *clasificación Kello* es realizada por el académico del mismo nombre y fue creada en su artículo *The Meaning of the Cyber Revolution,* de 2013. Los esfuerzos de Kello (2013) en

este documento están centrado en promover la difusión de los estudios de política desde el ciberespacio, y presentar un marco común técnico conceptual para el análisis de casos de estudio de la Ciencia Política y las Relaciones Internacionales, esta incluye:

a) *Ciberseguridad:* comprende a las medidas de protección de un sistema computacional o de la integridad de sus datos de una acción hostil. La ciberseguridad también se concibe como un estado de integridad, que es determinado por la presencia o ausencia de la intrusión dentro de un sistema computacional y sus funciones, además de que será de vital importancia para la seguridad y sobrevivencia de la información.

b) *Malware:* involucra el diseño de *software* para interferir con la funcionalidad o degradación de datos de un computador o red. Éste incluye una amplia gama de códigos dañinos (virus, gusanos, troyanos, *spyware, adware, ransomware,* etc.). La finalidad del malware es crear una avenida de acceso a un sistema computacional adversario u objetivo, por lo que el malware puede ser considera un instrumento de *ciber hostilidad.*

c) *Ciber crimen:* implica el uso de computadores para un objetivo ilícito bajo la existencia del código penal de una nación. Esto incluye fraudes bancarios, transmisión prohibida de datos, o pornografía infantil. Dado que la ley domestica no es aplicable en contra de Estados, el ciber crimen sólo involucra actores privados enjuiciables por jurisdicciones nacionales.

d) *Ciber ataque:* se refiere al uso de un código de interferencia con funcionalidad en un sistema computacional para un objetivo o estrategia política. Son caracterizados por el deseo y capacidad de los perpetradores por interrumpir operaciones informáticas o por destruir bienes físicos a través del ciberespacio. Pueden tener efectos directos (en infraestructura física) e indirectos (negar acceso a sistemas, operaciones o funciones, así como destruir información).

e) *Ciber explotación:* supone la penetración de un adversario en un sistema computacional con la finalidad de extraer (pero no destruir) información. Es considerada una actividad de extracción de inteligencia a un sistema anfitrión para extraer datos de carácter secreto o negar el acceso a los usuarios legítimos. Esto supone una acción de ciber espionaje para adquirir conocimiento crucial de un

sistema computacional adversario para planear futuros ciberataques o ciber operaciones.

Por su parte, la *clasificación Klimburg,* fue desarrollado el académico Alexander Klimburg, en el marco de su trabajo en el CCDCOE, en específico, para la creación del *National Cyber Security Framework Manual*, publicado en 2012 (Klimburg, 2012). Los conceptos que presentan son:

a) *Seguridad de información, TIC´s y ciberseguridad:* para esta clasificación es importante diferenciar los conceptos de seguridad de sistemas computacionales, protección de información y garantía de información, que son utilizados como términos intercambiables por diferentes gobiernos y estrategias de seguridad nacional, en la actualidad. Para esto es trascendental aclarar que la seguridad de la información se limita a la independencia de los datos y de dónde son tomados: medios electrónicos, impresos u otros. Mientras que seguridad de computadoras se refiere a asegurar la disposición y correcta operación de sistemas de computadoras con independencia de la información que resguardan o proceso. Finalmente, garantía de información corresponde al conjunto de información de seguridad, convenios y principios que determinan y evalúan qué información debe ser protegida.

   En ese sentido, la seguridad de las TIC's está más vinculada aspectos técnicos y la seguridad de computadoras, o con lo que define como la *cadena de suministro de seguridad* conectado a la IT y las Tecnologías de la Operación (TO´s) de las infraestructuras críticas. Mientras que los contenidos de información, su veracidad y responsabilidad de la utilización, se relaciona con la seguridad del internet o el contenido legal que hay en él. Por otra parte, para Klimburg la ciberseguridad es un concepto que va más allá de la seguridad de información y la seguridad de las TIC´s y TO´s, y define a la capacidad de proteger los secretos de un gobierno y permitir la defensa nacional, incluyendo la protección de la infraestructura crítica nacional, que impregna y maneja la economía global del siglo XXI.

b) *Ciber espionaje:* es la práctica de espiar, obtener información y generar inteligencia acerca de planes y actividades, de gobiernos extranjeros o empresas competidoras. La extracción de información se puede realizar por Estados o agentes privados. Los daños del ciber espionaje pueden afectar la integridad del gobierno y en el caso de las empresas, afectar la propiedad intelectual y causar riesgos, que en el tiempo, afecten el crecimiento tecnológico basado en el avance tecnológico, e innovación científica de otras naciones.
c) *Ciber guerra:* término académico, la referencia más cercana utilizada en documentos gubernamentales se refiere a guerra de información. Lo anterior, se refiere a las confrontaciones que existen entre las doctrinas de seguridad nacional de los diferentes Estados en torno a lo que es un ataque y una agresión. Por lo que esta noción se determina de acuerdo a la doctrina de seguridad nacional de cada país. No obstante, se refiere a actividades hostiles o amenazas en contra de la paz y seguridad internacional, que alcancen un grado de daño físico, y costos en vidas humanas.

Por último, se destaca que ambas clasificaciones tienen una connotación de securitización para el marco de análisis de casos de estudios o creación de documentos gubernamentales o académicos. Sin embargo, consideran a los actores privados como empresas u otros usuarios del internet, dentro del marco conceptual para análisis de eventos dónde hace interacción de éstos con Estados o gobiernos.

1.5 El ciberespacio como instrumento de poder

La emergencia del ciberespacio como nueva arena política internacional implica la posibilidad de su uso para fines políticos o para perseguir intereses particulares de Estados o individuos, actores públicos o privados al interior del internet. En la sección 1.3.3 se introdujo brevemente el término de *ciberpoder* que Joshep Nye (2012, p.3) define como: *"la habilidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en el ciber dominio".* Esta definición presenta al ciberespacio como un espacio de interacción, pero también de control y manipulación, en la que los actores inmersos pueden utilizar los recursos a su disposición, capacidades y ventajas cualitativas o cuantitativas para utilizar este dominio para influir en los hechos ciberfísicos,

y en consecuencia, en la realidad social que impacte o modifique las condiciones del contexto de la política internacional a su favor.

Para Sheldon (2012) el uso y aplicación del ciberpoder está orientado en aspectos tácticos, técnicos y operacionales en el ciber dominio, para quienes traten aplicarlo y utilizarlo. Lo anterior, está influenciado por la creación de un *objetivo estratégico*, el cual se puede perseguir, tanto en épocas de armonía o conflicto, y tiene la función de manipular el contexto de un ambiente estratégico, en este caso el ciberespacio, para ganar algún tipo superioridad por encima de los adversarios y degradar o limitar el desarrollo de capacidades semejantes por los competidores. En ese sentido, el ciberpoder es "*la suma de todos los efectos estratégicos generados por ciber operaciones en el mundo virtual*" (Sheldon, 2012). Por su parte, Kuehl (2009, p. 6) se refiere al concepto como:

> "[el] *centro de un conjunto nuevo de conceptos y doctrinas que son una palanca clave en el desarrollo y ejecución de política, ya sea contra el terrorismo, crecimiento económico o asuntos diplomáticos, etc."*

Mientras que para Starr (2012, p.4) es:

> *"*[un instrumento] *que a medida que evoluciona tiene el potencial de mejorar cada una de las palancas del poder nacional* [de un Estado], *en especial el militar y el informático".*

En vista de las múltiples definiciones que se tienen del concepto, sus capacidades y medios de impacto o influencia en torno al ciberpoder, a continuación presentaremos tres perspectivas teóricas que pueden ayudar a la comprensión de éste término y su capacidad de influir en eventos políticos del mundo material o hechos ciberfísicos, que son: 1) la teoría de la Guerra y el constructivismo, 2) el neorrealismo y el poder del Estado, y; 3) la teoría de la comunicación, visión de complejidad y teoría de sistemas.

1.5.1 La teoría de la guerra y la comprensión constructivista

El desarrollo de la Teoría de la Guerra Moderna, de Carl Clausewitz, ha marcado un fuerte énfasis en las características de los *campos o espacios de batalla* como un hecho crucial que puede determinar la superioridad de un Estado sobre otro en una confrontación bélica. En su obra clásica *De la Guerra* Clausewitz delinea los conceptos clave de las estrategias castrenses

del mundo contemporáneo, a la par que en su doctrina de la *Guerra Total* introduce un marco analítico que cimentó las características del poder terrestre de los Estados-Nación, con conceptos como el *espacio, tiempo, fuerza moral y material, teatro de guerra y operaciones* (Benítez, 1986). En específico, la categoría de *teatro de guerra* sirvió para la creación de esquemas bélicos semejantes en los años consecuentes a la publicación de los textos de Clausewitz.

Más tarde, en 1890 Alfred Tayer Mahan expandió la Teoría de la Guerra al espacio marítimo y determinaría los factores estratégicos para la superioridad del poder naval (Nye, 2012). Para 1921, Giulio Douhet publicaría su obra *El Dominio del Aire* y establecería los principios y ventajas del poder aéreo (Kuel, 2012). Posteriormente, el desarrollo del *poder espacial*, vinculado al desarrollo aeronáutico de cohetes y satélites, sería un tema de análisis recurrente y de amplia atención durante la segunda mitad del siglo XX para los teóricos de la guerra (Gray y Sloan, 1999). Asimismo, el desarrollo de las armas estaría determinado por el medio geográfico en que serían utilizadas –tierra, mar, aire, etc.- y debían de estructurarse para causar daño e impacto al enemigo en cada una de estas arenas (Kello, 2012).

Con relación a las ideas anteriores, de capacidades y factores individuales o contextuales, ligados a las características geográficas y físicas de cada teatro de guerra, presentan el hecho de que los cuatro campos de confrontación de la teoría clásica de la guerra ostentan dinámicas intersubjetivas ligadas al espacio físico, así como capacidad de influencia y poder para cada Estado-Nación. Dado que la confrontación bélica terrestre, con sus estrategias, técnicas y armamento (fusiles, tanques, morteros) eran completamente diferentes al espacio marítimo (submarinos, buques) o aéreo (jets o bombarderos). También, las cualidades intersubjetivas del Estado-Nación (como su territorio y poderío bélico) determinan su margen de acción para influir en las diferentes arenas de batalla, como fue el caso de Estados insulares, que necesitaron de transportarse a otras zonas para realizar guerra terrestre (Japón o Inglaterra), o países que no poseen litoral y por lo tanto se vieron limitados a desarrollar un amplio margen de poder marítimo, aunque no quedaron excluidos de él (Bolivia, Bielorrusia, Suiza, Kenia, etc.). La misma condición aplica para el campo aéreo o espacial, en los que el poderío de un Estado es determinado por la cantidad de arsenal (aeronaves) o desarrollo tecnológico (programa espacial) para desarrollar superioridad en estas esferas.

Esta visión de la intersubjetividad de los teatros de Guerra y capacidades del Estado-Nación nos acerca al concepto de *identidad*, desarrollado dentro del constructivismo. La identidad del Estado-Nación o actor internacional es un concepto que sirve como un puente entre la estructura de las normas o el régimen internacional y los intereses de los actores. En sí, la identidad supone una categoría dentro del análisis constructivista que sirve para señalar que en el sistema internacional existe una estructura normativa que determina el papel y grado de importancia de sus diferentes miembros (Estados protagonistas o no protagonistas) y crea una noción en torno a lo que es correcto (cooperación, alianzas) y lo que es incorrecto (conflicto, disuasión) derivado de las interacciones que se dan entre los actores. Por otra parte, las interacciones entre los actores del sistema internacional y las capacidades intersubjetivas de cada Estado, u otros actores, ayudaran a delimitar su interés nacional o particular, así como su papel dentro de la estructura.

En relación a lo anterior, estas ideas presentan al ciberespacio como un nuevo *campo o espacio de batalla*, en el que se miden los Estados-Nación a través de la confrontación, para alcanzar sus objetivos e intereses particulares. Éste supuesto nos obliga a discutir elementos de la Teoría de la Guerra tradicionales como: a) aceptar el ciberespacio como espacio de batalla, b) la naturaleza estado céntrica del análisis bélico y la posibilidad de aceptar otros actores en este marco de análisis. c) las características de las ciber armas desde las categorías de espacio, tiempo y fuerza, y; d) el señalar si el ciberespacio es un *teatro de guerra* o un *teatro de operaciones.*

a) Respecto a la primera noción, centrada en debatir si el ciberespacio es un espacio de batalla, se expresa que esta idea es difícil de aceptar a cabalidad en nuestro análisis dado que el concepto de *ciber guerra* es una categoría no abiertamente aceptada por varios teóricos. En ese sentido, en vez de señalar al ciberespacio como una arena de batalla, nos referiremos a él como un campo de interacción, en el que pueden existir dinámicas de conflicto entre diferentes Estados.

b) Por otra parte, la Teoría de la Guerra señala a los Estados-Nación como los actores fundamentales del análisis del conflicto bélico. Ante esto, se argumenta que de la misma manera que en el análisis clásico de la Teoría de la Guerra, los conflictos más trascendentales en el internet están representados por el choque entre dos o más países. No obstante, el marco

analítico del constructivismo permite ampliar el margen de consideración a otras entidades que tienen un papel de importancia dentro del campo virtual y construyen una identidad e intereses particulares para tratar de utilizar o poseer ciber poder, como las empresas privadas, los *hackers, o grupos criminales.* Está visión, es cercana al análisis de Van Creveld (1991), que en su libro *The Transformation of War,* indicó que en el futuro la guerra no se limitará a choques entre Estados-Nación, sino entre:

> "*…grupos a los que hoy llamamos terroristas, guerrilleros, bandidos y ladrones, pero que sin duda recurrirán a títulos más formales para describirse a sí mismos* (Van Creveld, 1991, p.17)."

La descripción anterior permite englobar a *hacktivistas* o *cibercriminales,* y de hecho, el mismo Van Creveld (2002) señaló a los *hackers* como parte de estos nuevos actores emergentes en los conflictos posteriores a la visión tradicional de la guerra.

c) La tercera cuestión es atender las características de las ciber armas en comparación a las categorías clásicas de Clausewitz: espacio, tiempo y fuerza. En relación al *espacio*, se expresa que este elemento se desvirtúa completamente dentro de la parte virtual del ciberespacio (software, protocolos IP o ICT), a razón que esta esfera carece de componentes materiales para que exista un grado de daño o amenaza. En todo caso, el máximo grado de daño que podría alcanzarse sería la interrupción o negación de un servicio derivado del saboteo por un actor rival inmerso en el mundo virtual. Respecto a la parte física del ciberespacio, esta se vuelve vital cuando se señala las *infraestructuras críticas* de un Estado-Nación.

En ese sentido, el daño a una INC es uno de los márgenes más grandes que puede presentarse en esta arena. En relación con el *tiempo,* a diferencia del concepto anterior, esta categoría maximiza su grado de afectación e impacto, en el campo virtual, en contraste con el espacio físico. Porque el lapso de planificación de una agresión en contra de un adversario puede operacionalizarse en un plazo más breve. Asimismo, si un Estado es víctima de un ciber ataque o ciber explotación, se vuelve de vital importancia resolver la agresión por la extracción de información o daño que es capaz de sufrir. Por último, la categoría de *fuerza* crea un esquema de interpretación cercano a los *hechos ciberfísicos,* dado que al interior del ciberespacio la diferencia de fuerzas se vuelve asimétrica, y permite a un individuo o grupo de personas, equiparar su nivel de acción al de un Estado, al menos dentro del internet. Sin

embargo, esta condición se verá superada si las interacciones o conflictos saltan al espacio material, ya que en el mundo físico los Estado-Nación detentan más poder coercitivo que cualquier otro actor.

d) El resolver si el ciberespacio es un *teatro de guerra* o de *operaciones* se externa que este se encuentra más ajusta más a un *teatro de operaciones,* que se anexa a los otros campos de confrontación de la Teoría Clásica de la Guerra. Además, se expresa que esta condición se establece a razón que los hechos ciberfísicos derivados de la utilización de ciberpoder por algún actor no modifican completamente la naturaleza de la guerra, aunque se acepta que si crean una nueva dinámica en el desarrollo de los conflictos que se desenvuelve en el dominio del ciberespacio.

1.5.2 La visión neorrealista y el poder del Estado

El paradigma neorrealista de las Relaciones Internacionales atendió el problema del ciberespacio y el concepto del ciber poder desde 2010, a tres años del primer caso trascendental de análisis de los estudios de ciberseguridad (Estonia, 2007) y en vísperas de otros eventos que reforzarían los estudios de esta nueva arena de influencia dentro de la política internacional (Stuxnet, 2011; Wikileaks, 2011; Primavera Árabe, 2011).

Con la publicación del artículo *Cyber Power*, Joseph Nye (2010) generó un esquema teórico que desentrañara a este nuevo campo de influencia y acción política desde la perspectiva del poder del Estado-Nación. Para este autor, la emergencia del ciber espacio como campo para ejercer el ciber poder se asocia más a un proceso de *difusión de poder* que a una *transición de poder* (Nye, 2014). Esta transición está vinculada a la posesión o manipulación de información por parte de los gobiernos, función para la que está prácticamente diseñada el internet y permite modificar la polaridad del poder en la estructura internacional, al menos en el ciberespacio. En ese sentido, los rápidos y vertiginosos avances de las TIC´s, TO´s y la tajante disminución del costo, procesamiento y transmisión de información hacen necesario que el Estado regule y controle la arena del internet, así como que construya doctrinas que consideren a éste como un elemento crucial para salvaguardar la integridad de la soberanía, interés y seguridad nacional y política exterior en el ciberespacio (Nye, 2010; 2014).

Por otra parte, Nye acepta que si bien la categoría de poder es elusiva y difícil de medir, en el espacio material, está se complica más al interior del internet. No obstante, destaca que

una característica del ciber poder, semejante al poder físico, es su alcance para que un Estado pueda realizar una acción por encima de otro. De esta forma, el ciberespacio es un campo de dominio en el que se pueden ejercer *los tres rostros del poder*, que corresponden a la capacidad de influir en el comportamiento y voluntad de otro actor (Dahl, 1961), la capacidad de enmarcar o ajustar agenda (Bachrach y Baratz, 1963), y la distinción entre el poder suave (*softpower),* que reside en la enmarcación, atracción y persuasión de la agenda política, y el poder duro (*hardpower),* que se determina por esquemas de coerción y pago, desarrollados por el mismo Nye durante la década de los noventa. Asimismo, ajusta ambas categorías a las dimensiones físicas y virtuales del ciber poder con las nociones de *intra*-ciberespacio y *extra*-ciberespacio, como se muestra en la figura 6.

Figura 6. Ciber poder en capacidades intra y extra-ciberespacio.

	Intra ciberespacio	**Extra ciberespacio**
Instrumentos de Información	***Hard power***: Ataques de Negación de servicio (DDoS) ***Soft power:*** Crear conjunto de normas y estándares del internet	***Hard power:*** Ataques a sistemas de supervisión, control y adquisición de datos. ***Softpower:*** Campaña de diplomacia pública para influenciar la opinión.
Instrumentos Físicos	***Hard power:*** Control gubernamental sobre compañías. ***Soft power:*** Infraestructura para apoyar a activistas de derechos humanos.	***Hard power:*** Enrutar bombas o cortar cables vitales. ***Soft power:*** Protestar para señalar o evidenciar a ciber proveedores.

Fuente: Nye (2010)

Un aspecto vital del análisis neorrealista es que éste destaca que el ciber poder no reemplaza al espacio geográfico, además de que no anula la soberanía del Estado-Nación. No obstante, acepta que éste es un régimen de componentes físicos y materiales que coexisten con el ejercicio del poder estatal y complican este concepto en la arena virtual, perspectiva que se acerca a nuestro análisis anterior centrado en la Teoría de la Guerra y el constructivismo. Del mismo modo, el enfoque del poder estatal expresa que el ciberespacio es una arena que debe ajustarse al dominio y control del régimen jurídico de los Estado-Nación, para su contexto local, además de que se aboga por la creación de una *gobernanza del internet* (Choucri *et al.*, 2013; Singer y Friedman, 2013) o la creación de un *Tratado del Ciberespacio* en el que los actores hegemónicos claves regulen este campo y creen normas para la delimitar el comportamiento de las partes interesadas (Hughes, 2010). En este sentido, un elemento clave del neorrealismo es su consideración del papel vital de las empresas privadas, promotoras o

creadores de softwares, como entidades de suma importancia para la consolidación de un régimen internacional de normas del internet. No obstante, deja en claro que los Estados-Nación son los mandamases de la regulación y control del internet (Nye, 2010).

Esta visión Estado-céntrica del enfoque neorrealista en torno al ciber poder crea conflictos con el concepto de soberanía. Porque esta idea emana de la integridad territorial y de la creación de fronteras geográficas cimentada en la Paz de Westfalia de 1648. Esta discusión señala que a diferencia del espacio terrestre, marítimo o aéreo, el ciberespacio no detenta ninguna frontera. Lo que hace que se describa al ciberespacio como una arena de características *post-westfalianas* (Hughes, 2010, Kello, 2013), discusión que atenderemos en el segundo capítulo de esta investigación. Por otra parte, entre los principales componentes físicos de los que carece el internet, se encuentran la conquista o control total, dado que la estructura del ciberespacio lo hacen más un espacio de construcción o manipulación, que lo diferencian de los campos señalados anteriormente.

Por último, se destaca que la visión del ciber poder neorrealista, centrada en la manipulación del ciber espacio como arena de expansión del poder estatal a través de la consolidación de doctrinas de seguridad nacional y política exterior, así como la creación de normas internacionales para la regulación del internet, será la perspectiva principal que desarrollará esta investigación, a razón que se considera es la que más se ajusta a las dinámicas de interacción entre los Estados-Nación, y otros actores de la política internacional, implicados en el análisis y estudio de los hechos ciberfísicos.

1.5.3 La visión de la teoría de la comunicación, teoría de sistemas y la complejidad

Una tercera perspectiva para entender al ciber poder se encuentra en el papel del internet como un medio masivo de comunicación e intercambio de información. Atender esta visión nos obliga a acércanos a esquemas de pensamiento como la *teoría de la comunicación, la teoría de sistemas y la complejidad,* para centrarnos más en el proceso de socialización de los actores en el ciberespacio y los efectos del flujo de información en el mundo físico, más allá del control del internet (visión neorrealista) y las características intersubjetivas de esta arena y las capacidades de sus partes (teoría de la guerra y constructivismo), tratados en los apartados anteriores.

De esta forma, la primera perspectiva que sirve para nuestro análisis de los *hechos ciberfísicos* y los efectos materiales del flujo de información nos acerca al pensamiento de Marshall McLuhan, su famosa frase "*el medio es el mensaje"* y sus clasificaciones de los medios de comunicación. Para McLuhan los medios representan tecnología que se concebían como una extensión del cuerpo humano, en ese sentido, un medio podía entenderse como cualquier herramienta diseñada por el hombre para extender su cuerpo o cerebro, por ejemplo, las bicicletas o automóviles representaban extensiones de las piernas, una pala o un martillo extensiones de los brazos, o los libros eran extensiones de la voz y mente. McLuhan aclaraba que estos medios no podían existir sin la participación de los individuos y las interacciones o procesos de socialización. Del mismo modo, externo que los medios, al volverse vehículos de interacción e intercambio de información, podían modificar el curso o funcionamiento de la sociedad, cultura o costumbres, a la par de crear una interacción dual de la operacionalidad entre el medio y los mensajes (McLuhan y Powers, 2020).

Con esta postura dividió a los medios de comunicación en dos ramas, 1) medios *calientes*, que presentaban características como información clara, precisa y accesible, alta definición y participación escasa del público en la construcción del mensaje. Y, 2) medios *fríos,* que se caracterizaban por presentar información escasa o incompleta, baja definición y requerían de una alta participación de los individuos para completar los mensajes a través de su capacidad cognitiva (Islas, 2004). Para ejemplificar los dos tipos de medios, Mcluhan se refirió a la prensa o la fotografía como medios calientes, y a la televisión o cine como medios fríos. Asimismo, Mcluhan externo que cada tipo de medio creaba y moldeaba *ambientes* de interacción que determinaban los cambios en la estructura social. Lo anterior, tenía que ver más con los efectos sociales visibles que generaban el intercambio de mensajes, más que con su contenido (Vilardo, 2021).

Los postulados anteriores tienen algunos elementos que sirven a nuestro análisis, a la par de particularidades que deben derogarse en la categorización de los hechos ciberfísicos. 1) En primera instancia, la noción de entender a los medios de comunicación como extensiones del cuerpo humano es plausible para individuos o grupos de personas al interior del ciberespacio, pero se complica para otro tipo de actores como Estados, Empresas y Organismos Internacionales. De esta forma, debemos aclarar que el internet, su uso y manipulación,

también debe entenderse como una extensión de las facultades e intereses de este otro tipo de entidades que tienen un papel trascendental en internet y en la consolidación del ciber poder, tal como es el caso del concepto de *interés nacional* del Estado-Nación. 2) Abordar la capacidad de los medios para transformar o modificar la realidad nos sirve para explicar eventos de casos de estudio más allá de los daños o ataques a la *parte física* del ciberespacio (infraestructura crítica o la IT), de hecho, el marco de análisis de McLuhan nos permite atender e interpretar otro tipo de manifestaciones sociales, en el mundo material, que se derivan del tráfico de información en el ciberespacio y se vinculan con el *comportamiento social*, como los disturbios asociados al traslado del *Soldado de Bronce* en el cibera taque de Tallin, en 2007, o la organización civil en contra de los regímenes autoritarios en Medio Oriente, durante la *Primavera Árabe.* También, este marco nos sirve para analizar casos más recientes en que el uso del internet ha tenido influencia de empresas privadas, como *Cambridge Analytica*, en procesos políticos que competen a gobiernos nacionales, como fue el caso de la elección presidencial de Estados Unidos, de 2016, o el *Brexit*, y que se vuelven temas de seguridad nacional o política internacional.

Después, la categorización de medios *fríos* o *calientes* nos lleva a entender el internet como un medio frío, debido a que el intercambio de información es la mayoría de las veces poco claro al interior del ciberespacio y requiere de la participación de los individuos u otros actores para completar los mensajes. En esta perspectiva, la experiencia de Estonia o la Primavera Árabe sirven para ejemplificar cómo la escasez de información determinó las acciones y respuestas tanto de la sociedad civil, como de las autoridades. También, los ejemplos de *Stuxnet* o Wikileaks, así como sus implicaciones en las dinámicas sociales apoyan los postulados de McLuhan, que expresan que son más trascendentes los efectos del intercambio de mensajes, que su contenido, como fue el daño causado al Programa Nuclear Iraní o los roces diplomáticos y la vulneración de información restringida por el Departamento de Estado, de Estados Unidos, derivada del *cablegate.*

Por otra parte, respecto a la categorización del internet como un medio que produce y crea su propio *ambiente,* este postulado nos acerca a una discusión semejante a la que realizamos desde la teoría de la guerra o el constructivismo sobre el ciberespacio como una arena de interacción y conflicto delimitada por la identidad y capacidades de los actores. No obstante,

la aportación de la teoría de la comunicación de Mcluhan es el señalar que el aumento de las *interfaces* entre los actores del ciberespacio promueve una multiplicidad de innovaciones que alteran los acuerdos o estructuras normativas para analizar cada caso o unidad de estudio (Vilardo, 2021). Dado que si algo distingue al análisis de los hechos ciberfísicos es la relativa facilidad de acceso al ciberespacio de miles o millones de actores potenciales y las diferencias cualitativas que presenta un caso como el de *Stuxnet,* a los ciber ataques de Tallin. Es precisamente el concepto de *ambiente* el que nos permite crear un puente entre la *teoría de la comunicación* y la *teoría de sistemas* y la *complejidad*, ya que debemos entender al internet como un medio masivo de comunicación que funciona como un sistema social complejo y adaptativo. En el que las características de los actores son las que establecen su funcionamiento, agencia o distintas agendas (Barron, 2017).

En ese sentido, la visión holística de la teoría de sistemas ayuda a la comprensión de los hechos *ciberfísicos* con relación a las diferentes fuentes o actores que pueden poseer o utilizar ciberpoder al interior del internet, contemplar a una entidad, como un Estado, o un individuo con intereses particulares, más allá de las ideas del control o regulación del internet o el conflicto. En ese sentido, se argumenta que el ciber espacio se puede entender como un *sistema social*, en el que interactúan múltiples subsistemas sociales -económico, cultural, religioso, científico- (Luhman, 1996), además de que su grado de complejidad aumenta debido que el internet es la plataforma tecnológica más grande actual que incorpora la mayor cantidad de actores sociales en el mundo. Y en teoría, permite a un amplio sector de la humanidad estar inscrita en un entorno o espacio temporal en el que sus partes interactúan constantemente.

Ante esto, una gran parte de los hechos ciberfísicos deberán ser abordados desde la visión de la complejidad, perspectiva que implica estudiar un fenómeno desde una representación de una totalidad organizada, cuyos elementos no pueden ser estudiados en forma separada o individual (García, 2006). Esto a razón de que los casos en que el ciber poder es utilizado para causar un efecto o impacto en la sociedad, este se mueve en esferas multidimensionales o transdisciplinarias, que pueden abarcar dualidades que antes se consideraban excluyentes, como lo público de lo privado, lo económico de lo político, etc. Asimismo, es notable que el estudio y análisis de determinados hechos ciberfísicos puede verse limitados desde la visión

del poder estatal neorrealista, o desde el conflicto de la teoría del Guerra, ante este condicionamiento, la visión de complejidad promueve un nivel de análisis más amplio para desentrañar cada caso de estudio. Aspecto del pensamiento complejo que permiten presentar al ciberespacio como uno de los sistemas sociales más contradictorios e inciertos del mundo contemporáneo.

1.6 Actores de la política internacional y *stakeholders* del ciberespacio

El último apartado que desarrollaremos en este capítulo es la necesidad de delimitar o señalar a los actores que sean susceptibles de participar en la arena del ciberespacio. Para atender esta discusión, recurriremos a los paradigmas clásicos de las teorías de las relaciones internacionales, que, con el esquema del realismo, durante la década de las cincuenta, presentaron al Estado-Nación como el actor clave del análisis de la política internacional. Visión acotada y Estado-céntrica que se transformó en la década de los setenta y comenzó a incluir nuevos protagonistas en el debate y quehacer de la política global que siguen modificándose hasta nuestros días.

Ante esto, abordaremos dos delimitaciones de los actores capaces de influir en la política internacional, la primera se vincula a los paradigmas clásicos, que denominaremos los *actores clásicos* y son capaces de influir en los hechos políticos del mundo físico. Posteriormente, utilizaremos la categoría de *las partes interesadas,* presentada por Klimburg y Healey (2012), para señalar a aquellos otros actores que pueden utilizar ciberpoder para alcanzar intereses políticos, y en consecuencia, influir en los hechos ciberfísicos. Por último, contrastaremos algunos de puntos de interés entre la primera categorización y la segunda, para delinear a las partes interesadas del ciberespacio.

1.6.1 Actores clásicos de la política internacional

El paradigma realista de las Relaciones Internacionales es el primer esquema de la disciplina que utiliza la noción de actor para referirse a los protagonistas de la política internacional. Influida por los sucesos y conflictos internacionales de la primera mitad del siglo XX, como la Gran Guerra, el fracaso de la Sociedad de Naciones y la II Guerra Mundial, el realismo político pone énfasis en el egoísmo humano y el interés individual como los elementos promotores del conflicto de la política entre las naciones. En ese sentido, en el primer principio del realismo político, Hans Morgenthau expresa que las leyes que rigen las

relaciones entre los países y la política global emanan de la naturaleza humana, por lo cual el conflicto y egoísmo que existe entre los individuos se traslada también al nivel entre Estados (Scheuerman, 2009). Asimismo, en el segundo principio, indica que los Estados-Nación definen y desarrollan la noción de *interés nacional* para perseguir sus objetivos particulares en el contexto internacional, mientras que en el tercer principio especifica que ésta noción es de *validez universal* y *atemporal*. Por lo que indica que todos los Estados detentan y persiguen sus propios intereses a través de la construcción de poder, de manera indefinida, en la política global.

En lo general, Morgenthau (2008) indicó que la multiplicidad de actores (Estados-Nación) implicaba que éstos desarrollaran procesos de *rivalidad*. Por lo que los Estados necesitan poseer poder como un medio para su participación en la política internacional y como un fin para garantizar la defensa y sobrevivencia. Ante esto, debe entenderse que la visión de Morgenthau pone énfasis en que el conflicto y la anarquía es la norma de la política entre las naciones, idea que fue de gran éxito y aceptación desde el fin de la II Guerra Mundial hasta la década de los setenta del siglo XX, dada la magnitud que alcanzaron los conflictos multinacionales y el amplio desarrollo del poderío militar como principal medio de disuasión por potencias como Estados Unidos y la Unión Soviética.

No obstante, se debe aclarar que el análisis del realismo emanó de la experiencia internacional acontecida en la primera mitad del siglo. Sin embargo, tras treinta años de vigencia, y una considerable disminución de la magnitud y trascendencia de las confrontaciones bélicas, el realismo empezó a verse superado por múltiples factores que mostraron transformaciones cualitativas en el proceso de acción de la política global. Ya que, en el curso de la década de los sesenta, de siglo XX, entidades como la Organización de las Naciones Unidas se volvieron más influyentes en los procesos de pacificación o resolución de conflictos globales, la cooperación económica multilateral se transformó en la norma del continente europeo y las empresas se volvieron actores de relevancia en las relaciones bilaterales entre los países.

En este contexto, acontecería un debate paradigmático al interior de la disciplina de las Relaciones Internacionales que culminaría en el desarrollo de nuevas vertientes teóricas que se acoplarían a explicar las nuevas dinámicas de la sociedad global, entre los que destacan el

liberalismo, marxismo, realismo estructural y la *teoría de sistemas.* De la parte del liberalismo, es importante mencionar su énfasis en que, si bien el conflicto y rivalidad es una de las principales dinámicas que existen entre los Estados, la cooperación también se presenta como una opción viable para múltiples países en aras de la construcción de influencia global (Keohane y Dunn, 2002). En ese sentido, esta visión resaltó la importancia de la creación de un marco institucional que servía como promotor de la cooperación internacional, que comúnmente se asociaba a entidades supranacionales, por lo que abrió la puerta a la inclusión de los *organismos internacionales* como actores de la política internacional. También, el incremento paulatino del comercio internacional y su cada vez mayor importancia entre la agenda bilateral o multilateral de los Estados definió que las *empresas trasnacionales* fueran considerados actores capaces de enmarcar la agenda política global desde la visión liberalista. Por otra parte, el *marxismo* puso énfasis en las asimetrías de desarrollo económico que existían entre los países del norte y el sur, u occidente y oriente. Por lo que el componente del desarrollo industrial de los países desarrollado y los subdesarrollados se acercó a señalar de igual forma a las empresas trasnacionales como actores que detentan poder hegemónico en el orden internacional (Maclean, 1988).

A pesar de que estos enfoques abrieron espacios para otro tipo de protagonistas de la política, el posicionamiento de los Estados-Nación se refrendó por concepciones como el *neorrealismo* y la *teoría de sistemas* de las relaciones internacionales, aunque estos esquemas aceptaron la existencia de otros canales de comunicación entre la política internacional más allá del poder estatal y la búsqueda de intereses particulares de los gobiernos. En ese sentido, el *neorrealismo* introdujo el concepto de estructura para especificar que el orden o estabilidad del sistema internacional era generado por los Estados, a la par que los principales mecanismos de dialogo e interacción más desarrollados en la política global eran generados por los países y por lo tanto se les daba primacía (Waltz, 2004). Por otra parte, la teoría de sistemas se acercó a esta visión al presentar los diferentes tipos de *balances de poder* o *sistemas internacionales* que podían emanar de la creación de un orden internacional por parte de los Estados, como sistema bipolar, bipolar libre, universal, jerárquico y unidad de veto. Visiones que retomaron fuerza con el recrudecimiento de la Guerra Fría y el conflicto ideológico entre la URSS y Estados Unidos en el periodo de los gobiernos de Mijaíl Gorbachov y Ronald Reagan en la década de los ochenta (Wendt, 1987).

En ese sentido, la discusión en torno a los protagonistas de las relaciones internacionales tendría que esperar hasta el tercer debate paradigmático de la disciplina, promovido por los cambios en el orden internacional durante la década de los noventa, como el fin de la Guerra Fría, el auge de las políticas neoliberales a nivel global y el inicio del proceso de globalización, para ampliar el margen de los actores internacionales. En este contexto, teorías como *trasnacionalismo, cosmopolitismo, gobernanza global* y la *sociedad de la información*, señalarían a entidades subnacionales (ciudades, urbes, provincias, localidades, etc.), movimientos globales u Organizaciones No Gubernamentales (ONG´s) como nuevos protagonistas con capacidad de enmarcar agenda política. Por su parte, el constructivismo con la categoría de identidad, y la construcción intersubjetiva de los actores y sus intereses, también permitió englobar a otro tipo de actores de difícil clasificación dentro de la categoría de actores internacionales como los grupos terroristas, crimen organizado o guerrillas o grupos de choque.

Respecto a esta breve revisión teórica, se expresa que los actores clásicos de las relaciones internacionales fueron identificando en la sucesión de los debates teóricos, entre los cuales podemos ubicar tres grupos vinculados a cada época del desarrollo de la disciplina que se presentan en la tabla 2 referente a los actores clásicos de las relaciones internacionales.

Tabla 2. Actores clásicos de las Relaciones Internacionales

Actores o protagonistas de las RR.II.	**Debate paradigmático**	**Teorías o Esquemas que lo contemplan**
Estado-Nación	Primer Debate Segundo Debate	Realismo Neorrealismo Teoría de Sistemas
Organismos Internacionales o Regionales Empresas Trasnacionales	Segundo Debate Tercer Debate	Liberalismo Marxismo Cosmopolitanismo Trasnacionalismo

Actores o protagonistas de las RR.II.	Debate paradigmático	Teorías o Esquemas que lo contemplan
Movimiento Globales Gobierno subnacionales ONG's Grupos Terroristas Crimen Organizado Guerrillas	Tercer Debate	Constructivismo Cosmopolitismo Trasnacionalismo Gobernanza Global Sociedad de la Información

Fuente: Elaboración propia.

1.6.2 Las partes interesadas del ciberespacio

El recuento de la sección anterior en torno a la delimitación de los protagonistas de la política internacional nos sirve para discutir la categoría de *actor* en la arena del ciberespacio y en los hechos ciberfísicos. De esta forma, se explica que la necesidad de las diferentes teorías de las relaciones internacionales por enmarcar o señalar a los actores de las relaciones internacionales surge de la necesidad de encontrar unidades de análisis que permitan aplicar los preceptos o principios desarrollados por cada teoría, ya sea *realismo, constructivismo, liberalismo,* etc., en casos concretos de estudio.

Asimismo, con independencia de la naturaleza conflictiva o cooperacionista del enfoque, la utilidad de señalar actores permite localizar las fuentes de las que emana el poder, cooperación o agendas de la política global, promovida por los intereses de los actores y las interacciones que estos generan de acuerdo con las condiciones imperantes en el contexto internacional de cada época (Guerra Fría, Neoliberalismo, Globalismo, etc.). En ese sentido, la necesidad de identificar a los actores que influyen en los hechos ciberfísicos y el ciberespacio sirve a los teóricos para crear y operacionalizar estrategias en aras de la construcción del ciberpoder, dado que ésta permite consolidar significados y metas de los intereses de un actor al interior de este dominio, que le sirven para identificar a sus potenciales adversarios o aliados.

Para Klimburg y Healey (2012) la comprensión de los protagonistas del ciberespacio es vista desde la óptica de la ciberseguridad nacional, que compete a una visión que tiene al Estado-Nación como centro del análisis, pero acepta que el control y dinámicas del internet no están

restringidas a entidades gubernamentales e incluye actores no estatales e internacionales. Lo anterior se relaciona con los actores clásicos de las relaciones internacionales, ya que todo ellos pueden tener participación al interior del internet, a razón que las barreras de ingreso al ciberespacio son relativamente mínimas y no obstaculizan o condicionan a ninguno para acceder a este campo. No obstante, categorizar la acción de cada uno de estos actores en el espacio virtual puede ser problemático al señalar categorías como *ciber guerrero, ciber terrorista* o *ciber activistas,* etc., que no son necesarias para un análisis estratégico y pueden causar conflicto al momento de delinear qué características o elementos definen a cada una de estas entidades, por lo que se denota que la categoría de *actor* es impopular desde los estudios de ciberseguridad (Klimburg, 2013).

Frente a este escenario, se propone un marco conceptual que sirva de ayuda y para el entendimiento de los *stakeholders* o partes implicadas del ciberespacio, que Klimburg y Healey (2012) dividen en tres categorías, que se describen a continuación:

a) *Actores Estatales:* señala en específico a los Estados-Nación, representados por instituciones gubernamentales. Por lo general, son las entidades con los mejores y más sofisticados recursos para influir en el ciber espacio, dado que los gobiernos pueden componer grandes equipos de seguridad informática y poseen infraestructura en telecomunicaciones propia para utilizar internet y promover sus intereses

   Asimismo, una ventaja que poseen este tipo de actores es que al ser entidades de tan gran magnitug abarcan desde gobiernos locales, regionales o nacionales, así como diferentes esferas de influencia (política, económica, comercial, educativa, financiera, etc.), es muy complicado que sean susceptibles de sufrir ataques que contemplen a la totalidad de sus componentes, ya sea unidades de gobierno o infraestructura nacional crítica. Por lo que es más común que los ciber ataques u operaciones de ciber espionaje o ciber operación estén vinculados a un solo objetivo de la gran estructura del Estado.

   Otra superioridad que detentan es que al detectar una agresión a través del ciber espacio es viable que pueden someter en alguna medida a los perpetradores a un marco de normas legales y repercusiones políticas. No obstante, de estas ventajas cualitativas, el Estado también sufre desventajas vinculadas a su gran cantidad de

recursos (presupuesto, equipamiento o gente entrenada), que se refleja en su falta de agilidad y respuesta frente a las ciber agresiones, aspecto que se dificulta más si éstas agresiones se mueven a través de entidades privadas y no se tiene un marco de acción estructurado para la confrontación de ciber amenazas (Klimburg y Healey, 2012, p. 68).

b) *Actores no Estatales Organizados:* comprende a las entidades fuera del Estado-Nación y de carácter privado con un nivel de organización mínima en alguna esfera social (empresarial, criminal, política, etc.). Los actores no estatales son responsables de prácticamente todo *hardware* y *software* que se utiliza en el ciber espacio, y también, son las principales víctimas de este tipo de actividades. Destaca que este grupo de actores ejecutan la mayoría de las ciber operaciones, ya sea para sus intereses particulares o para apoyar operaciones de los gobiernos. Los estudios del ciberespacio y ciber seguridad deben poner especial atención en este tipo de actores, dado que la dinámica del internet muestra cada vez más que la ciberseguridad en un asusto vinculado principalmente a actores no estatales. Por último, se menciona que lo grandes actores no estatales son vitales para la construcción de ciber poder e influencia en el internet, con énfasis especial para las empresas de software (como Microsoft, Linux, etc.), empresas de seguridad (McAffer, Norton) o portadores de telecomunicaciones (At&T, Vodafone), a la par que tienen una capacidad de movilización más ágil que la de la mayoría de los gobiernos del mundo (Klimburg y Healey, 2012, p. 69).

c) Actores no Estatales no Organizados: representan a los actores que realizan ciber operaciones o campañas del más bajo nivel al interior del internet, como pequeños ciber criminales o *hacktivistas.* Normalmente este tipo de acciones son conducidas por pequeños grupos de individuos, sin nivel de jerarquía, o incluso por actores individuales. La ausencia de algún nivel de autoridad o cadena de mando limita seriamente su nivel operación y capacidad de daño que pueden causar. Se resalta, que a diferencia de las grandes organizaciones criminales o grupos delictivos bien estructurados, éste tipo de actores no desempeñan actos de ciber crimen de alto valor,

> robo de propiedad intelectual, y por lo tanto no juegan un papel decisivo en el ciberespacio. También, se destaca que el nivel de recursos que tienen para emprender ciber operaciones es muy limitado por lo cual sus campañas en el internet son comúnmente de corta duración. No obstante, de estas características, detentan ventajas frente a los actores estatales y no estales, como un margen de acción y reacción más ágil y rápida, a la par de habilidad y un capital humano más competitivo que muchos gobiernos o empresas (Klimburg y Healey, 2012, p. 70).

La anterior delimitación de Klimburg y Healey (2012) permite conjuntar a los diferentes actores clásicos de las relaciones internacionales en los tres grupos sugeridos por estos autores, con la finalidad de crear un análisis estratégico más concreto que permita englobar a cada uno de ellos. También, la ventaja de conjuntar ambas clasificaciones nos permite presentar qué enfoques teóricos pueden tener cercanías o vínculos para la promoción de un análisis y estudio estratégico de los múltiples hechos ciberfísicos que deseemos abordar, como se presenta en tabla 3. De esta forma, se expone que los estudios del ciberespacio, ciber poder y hechos ciberfísicos que partan de la óptica de análisis de los actores estatales, se vincularán con perspectivas como el realismo, realismo estructural o la teoría de sistemas desarrollada al interior de las relaciones internacional. De esta forma, no sorprende que los autores que se desenvuelvan en ésta perspectiva vinculen al ciberespacio con elementos como la seguridad nacional, política exterior o soberanía estatal, y que abogan por la construcción de un régimen del ciber espacio y su control por parte de los Estados-Nación.

Por otra parte, el análisis de esquemas teóricos que se vinculan a actores no estatales organizados, amplía su margen de acción a una serie de enfoques como liberalismo, marxismo, cosmopolitanismo o la teoría de sistemas desarrollada al interior de la teoría de la comunicación. En ese sentido, estas perspectivas indagarán en temas más allá del poder y sobrevivencia del Estado, para centrarse en actores o fenómenos como las empresas privadas, movimientos sociales, flujos de trasnacionales de mercancías o individuos o prácticas ilícitas del crimen organizado de gran envergadura, que puedan tener materialización en los hechos ciberfísicos. Por último, se destaca que la clasificación de actores no estatales no organizados permite englobar una serie de nuevos

entes que han sido de difícil clasificación para los analistas de la política internacional en la última década, pero que han enmarcado agenda en el contexto internacional.

Tabla 3. Clasificación Klimburg y Healey, actores de las RR. II. y enfoques teóricos.

Clasificación Klimburg y Healey	Actores clásicos de las RR. II	Perspectivas Teóricas
Actores Estatales	Estados Nación Organismos Internacionales o Regionales Gobiernos subnacionales	Realismo Realismo Estructural Teoría de Sistemas (RR.II.)
Actores no Estatales Organizados	Empresas Trasnacionales Empresas de Software Firmas de Seguridad Portadores de Telecomunicaciones ONG's Grupos Criminales Movimiento Globales Grandes grupos Terroristas	Liberalismo Marxismo Cosmopolitanismo Trasnacionalismo Gobernanza Global Teoría de Sistemas (Teoría de la Comunicación) Sociedad de la Información
Actores no Estatales no organizado	*Hackitivistas* Pequeños grupos criminales Individuos autónomos.	Trasnacionalismo Constructivismo Teoría de Sistemas (Teoría de la Comunicación) Sociedad de la Información

Capítulo 2. Ciberseguridad: nexos entre la soberanía y seguridad nacional

Introducción

La ruta crítica de este capítulo es encontrar los nexos entre el concepto de soberanía y la seguridad nacional, y consecuentemente, con la ciberseguridad. La discusión está orientada en reforzar la hipótesis principal de esta investigación, que define al ciberespacio como una nueva arena de la política internacional en la que es posible vulnerar la soberanía de un Estado-Nación, a través de la ciber explotación de sus sistemas informáticos (TIC´s), ya sea por el robo o manipulación de información de carácter de seguridad nacional, o por la afectación a sus sistemas operativos (TO´s) que adminsitran Infraestructura Nacional Crítica, en ese sentido, la ruta del capítulo es la siguiente.

Figura 7. Vínculo entre la soberanía, seguridad nacional y ciberseguridad.

Fuente: Elaboración propia.

Para sustentar este argumento, utilizamos el diagrama anterior, en el que se presenta el postulado de que la creación de una política de seguridad nacional es la consecuencia de la idea de la soberanía. Si bien la definición de este concepto ha sido y es objeto de polémica dentro de los debates teóricos al interior de la ciencia política y las relaciones internacionales, se considera que se cuentan con los recursos académicos suficientes para sostener este planteamiento. Una vez realizada esta discusión, se procede a realizar un análisis sobre la

creación de una estrategia y doctrina de seguridad nacional, dentro de la cual debe estar incluida la ciberseguridad. Es importante mencionar que la interpretación de los conceptos de seguridad nacional y soberanía se hace desde una óptica constructivista, dado que se considera que cada Estado-Nación edifica una estrategia de seguridad nacional y ciberseguridad como una entidad intersubjetiva, que proviene de su identidad, intereses y nociones de securitización según sus necesidades de sobrevivencia como Estado. Posteriormente, se hace una pequeña diferenciación del términp de la ciberseguridad, desde la visión de los Estados-Nación y los actores no estatales organizados, provenientes del sector privado o económico, a razón que es importante marcar las diferencias de protección que presenta cada una de estas esferas. Por último, se realiza una discusión en torno a la capacidad de resiliencia y ciber disuasión que debe poseer un Estado para garantizar su capacidad de defensa al interior del ciberespacio, desde diferentes métricas internacionales.

2.1 El concepto de soberanía desde la visión Estado-céntrica

Según Eisenhut (2010, p. 4): "*la seguridad es el núcleo de la existencia del Estado*". El origen de este precepto se remonta al pensamiento de Thomas Hobbes, que en su obra *Leviatán*, definió al Estado como el protector contra las amenazas externas (Hobbes, 2013). Entre múltiples autores, esta base teórica de la ciencia política es el principal sustento de la noción soberanista que adoptaron las potencias europeas durante el siglo XVII. En los hechos, esta idea se materializa con sucesos históricos como la firma de la Paz de Westfalia, en 1648, evento que dio inicio a la creación de los Estados-Nación modernos e influyó fuertemente en la obra de Thomas Hobbes, que se publicó en 1651. En ese contexto, más que comprender a la Paz de Westfalia como el episodio que representó el fin de la religión como instrumento de control político en la Europa moderna, es importante ser consciente de otros eventos que ocurrieron en torno a este evento y las consecuencias que cimentaron los antecedentes de lo que sería la seguridad nacional.

Previo al inicio de la Guerra de los Treinta Años (1618), el cisma protestante y la expansión del luteransmo y calvinismo debilitaron la estabilidad y el poder político de los imperios católicos, principalmente el Sacro Imperio Romano Germánico. El conflicto entre las dos vertientes del cristianismo sirvió como pretexto para que múltiples reyes o señores feudales de la Europa medieval intentaran hacerse con la conquista de otros territorios y la dominación

política de múltiples ciudades con el fin de utilizar la religión como la base para legitimar incursiones bélicas. Si bien, se señala a la secularización de la política como el principal éxito alcanzado en la Paz de Westfaliana, otros factores tienen mayor trascendencia para la noción soberanista del Estado y su vinculación con la seguridad nacional.

El primero es que dicho evento constituyó a la integridad territorial como la base de la existencia del Estado, desde una perspectiva teórica se señala que esta capacidad, definida como *la responsabilidad de proteger*, supuso el cese de la libertad de actuar violentamente de los individuos para centralizar la capacidad de ejercer la violencia en una autoridad -un príncipe o monarca, y posteriormente, un gobierno (Stahn, 2007). Por otra parte, en el plano del pragmatismo, la Guerra de los Treinta Años, fue un evento bélico en el que resaltó el uso de mercenarios para las labores bélicas, trasunto que impactó en la necesidad de poseer un ejército por parte de las nacientes potencias de Europa para garantizar su seguridad (Triandafillov, 2013). En ese punto, la necesidad de poseer una armada permanente, lista para defender el territorio del Estado-Nación y a la población que formaba parte él, fue uno de los elementos clave para garantizar la sobrevivencia estatal. Posteriormente, la creación de los ejércitos modernos, con capacidad de defensa nacional, fue una de las principales secuelas de la idea soberanista que cimentaba los fundamentos de la seguridad nacional (Altinay, 2004).

En esta fase del desarrollo del Estado-Nación, Davies (2016) expresa que de la salvaguarda del territorio emanó otra característica vinculada a la noción soberanista: *la autonomía política o determinación del Estado*. La perspectiva de la autonomía política recibió importantes aportes desde las teorías de las relaciones internacionales, en esta visión destacan dos paradigmas que otorgan elementos al debate que son el realismo y el liberalismo económico. Para los realistas la soberanía se entiende en el entorno de la anarquía del sistema internacional –en el que existe una ausencia de autoridad central- y existe un permanente balance de poder y búsqueda de la hegemonía entre los Estados, por lo que Morgenthau definió a la "*soberanía como la autoridad suprema que puede alcanzar una nación*" (Moses, 2012). De esa forma, los realistas entienden a la autonomía política como la capacidad de decisión y acción vinculada al poder estatal.

El poder del Estado puede medirse y comprenderse desde múltiples esferas; por ejemplo, para Robert Gilpin (2010) el poder de los Estados-Nación se comprende desde su capacidad económica, militar y tecnológica. Mientras que para John Mearsheimer (2001), este se debe entender desde la innovación de la doctrina militar, seguridad nacional y política exterior, la capacidad de desarrollo de armas y la creación de una estrategia inteligente para aplicar en los hechos. Por último, destaca la definición sobre soberanía que realizó Kenneth Waltz (2010) a la que define como:

> "…*la capacidad de un Estado de operar independientemente de otras naciones…un Estado soberano es aquel que decide por sí mismo como va hacer frente a sus problemas internos y externos, incluso, si decide cooperar con otros…"* (Waltz, 2010).

En contraposición, el pensamiento liberal abordó la concepción soberanista desde los principios de la economía de mercado, que son: 1) el interés individual, 2) el orden natural que emana de la interacción del interés de los individuos y el bienestar social, y 3) la capacidad innata del mercado de autorregularse por sí mismo. Estos preceptos ponen por encima al intercambio económico, de la actividad política, e incluso, de la militar y de defensa. A pesar de esta visión, el mismo Adam Smith (2015) reconoció en la *Riqueza de las Naciones* que el deber de la soberanía es:

> "*proteger a la sociedad de la violencia y la invasión de otras sociedades independientes, lo cual debe hacerse a través de una fuerza militar"* (Smith, 2015).

No obstante, aunque Smith aceptó que frente una amenaza bélica era necesaria la capacidad de defensa militar para la sobrevivencia del Estado, el liberalismo económico señaló a la soberanía – desde los términos de la integridad territorial- como un costo que afectaba el intercambio y la economía de mercado. Ante esta perspectiva, el pensamiento de David Ricardo sobre la ventaja comparativa y el libre intercambio entre naciones de bienes y productos sentaron la base de las ideas cooperacionistas que desarrollaron los Estados-Nación de occidente, después de la segunda mitad del siglo XX.

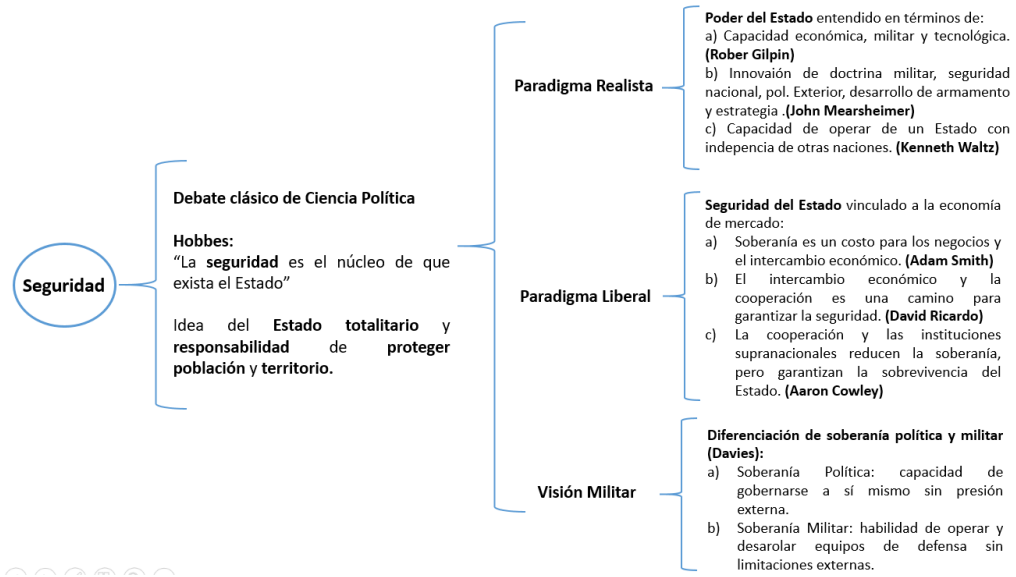
En esta discusión, Cowley (2011) destaca que la cooperación implicó una transformación de la noción tradicional de la soberanía que tenían los realistas, dado que hizo explicito que los caminos para la sobrevivencia del Estado podían alcanzarse desde la cooperación, como mostró la creación de organismos como la Comunidad Europea del Acero y el Carbón (CECA), en 1950, que desafiaron la idea de la integridad territorial y el poder del Estado, al dejar en la jurisdicción de una institución supranacional, integrada por seis naciones, la explotación de dos recursos clave: el acero y el carbón, los cuales fueron vitales para acrecentar el poderío bélico de las naciones europeas durante las dos guerras mundiales. En ese sentido, Davies (2016) expresa que la transformación de la CECA en la Unión Europea, implicó una reducción de la capacidad de decisión soberana de los países que integran este organismo internacional, en esferas como la administración de justicia, la política económica y la defensa. Sin embargo, sus miembros obtuvieron beneficios, como la disminución de conflictos armados, que potencializaron el intercambio económico a su máximo nivel hasta transformarse en uno de los bloques comerciales más importantes del mundo. Tomando en cuenta este caso, se argumenta que la actividad comercial y el intercambio de mercado resultaron una alternativa eficiente para garantizar la seguridad de las naciones, aunque esto implicaría para las naciones sacrificar soberanía y autonomía de decisión en diferentes esferas.

Otra aproximación de interés, que vincula a la soberanía con la seguridad nacional, es también señalada por Davies (2016), al hacer una diferenciación de la soberanía estatal, desde los términos políticos, y delimitar la comprensión de una *soberanía militar*. A la primera la define como: "[la capacidad] *de autoridad de un Estado para gobernarse a sí mismo y operar libre de control externo*". Mientras que sobre la segunda expresa que es "*la habilidad para desarrollar y operar equipos militares y de defensa libres de las limitaciones de externos".* Por lo que denota, que más allá de la visión realista y liberal, la soberanía de los estados también se vincula a su capacidad real y autónoma de defensa y protección.

Por último, en la figura 8 se indican los vínculos señalados en este apartado entre la soberanía y la seguridad nacional. Además de presentar las diferencias entre el concepto para los realistas y los liberales, en el que se observa que para los primeros supone la capacidad de construcción y manutención de poder militar y político en la esfera internacional. Mientras

que para los liberales, representa un elemento con nexos a la sobrevivencia del Estado, que puede vincularse al mercado y la cooperación económica, para garantizar la seguridad y permanencia del Estado, con beneficios para la economía y el libre intercambio de bienes, aunque esto suponga el sacrificio de autonomía de decisión y actuar.

Figura 8. Nexos seguridad, soberanía y paradigma realista, liberal y militar.



Fuente: Elaboración propia.

2.2 El debate Post-Wetsphaliano de la soberanía

En el apartado anterior se presentó una contextualización de la noción soberanista de los Estados y su comprensión desde los fundamentos de la Ciencia Política y las Relaciones Internacionales. Del mismo modo, se expuso la visión del realismo político, neorrealismo, liberalismo económico y pensamiento militar en los términos que estos paradigmas entienden dicho concepto. Para Glanville (2013), fundamentos como la salvaguarda de *la integridad territorial* y *la responsabilidad de proteger* cimentaron la idea tradicional o *westfaliana* de este término. A dichas características, McFarlane y Sabahdze (2013) añaden otras como *la autodeterminación* –vinculada a la capacidad de decisión de un Estado- y *la no intervención* –en asuntos internos de un país, en el plano político, económico, etc. No obstante, ambos autores señalan que durante la segunda mitad del siglo XX el concepto de soberanía entró en un proceso de transformación que dejó sin vigencia a la noción westfaliana.

En torno a este debate, Krasner (2010) y McFarlane y Sabahdze (2013) categorizan a la soberanía en cuatro diferentes épocas, que son:

1) Paz de Westfalia (Siglo XVII y XVII)
2) Congreso de Viena (1815 a 1945)
3) Guerra Fría (1945 a 1991)
4) Post Guerra Fría (1991 – actualidad)

En las dos primeras fases de esta clasificación, la idea de soberanía está fundamentada en el principio de protección de la integridad territorial y la responsabilidad de proteger. Por lo que la idea de la seguridad nacional se asocia a la salvaguarda del territorio y la protección de la población por parte del monarca o gobierno, en nombre de la soberanía estatal. Este paradigma está vinculado en el contexto histórico de Europa desde el siglo XVII y a la consolidación como naciones de los grandes imperios como Francia e Inglaterra. En el pensamiento de los siglos XVII, XVIII, XIX y la primera mitad del XX, la noción soberanista se acerca más a la visión realista, entendida por las potencias europeas como la capacidad de decisión, sustentada en su poder bélico. Y las consecuencias de esta forma de entender al concepto, vinculada a la búsqueda de los intereses particulares de los Estados-Nación, de forma individualista, que llevó al continente europeo a su máximo hecatombe, en la Segunda Guerra Mundial.

Para la segunda mitad del siglo XX, gran variedad de autores expresa que la noción westfaliana pierde su vigencia e inicia una época de comprensión post-westfaliana en torno al concepto (Granville, 2013; McFarlane y Sabahdze, 2013; Cowley, 2011; Davies 2016). Esta transformación se vincula al auge del liberalismo económico en la política entre las naciones, a razón que esta perspectiva amplió el margen de los canales de comunicación entre los Estados más allá de la dualidad de la paz y el conflicto. Entre los que destacó el intercambio comercial y la cooperación internacional. En este ambiente, la evolución de la CECA a la Comunidad Económica Europea es uno de los principales eventos históricos que denota el inició de la era post-westfaliana (Falk, 2002). Dado que los mecanismos y políticas multilaterales que desarrolló este proceso de integración cuestionaron en la realidad a los fundamentos de la visión tradicional del término, tales como la eliminación de barreras arancelarias al comercio, la libre circulación de personas en mercados laborales, la creación

de políticas de seguridad alimentaria compartida y la edificación de instituciones supranacionales. En ese sentido, Europa conoció una época de paz y bonanza económica, cimentada en la cooperación y en la cesión de su capacidad de decisión autónoma y soberana a cambio de estos beneficios (Davies 2016; Schmidt, 2011).

Una segunda ola que cuestionó la idea tradicional de la soberanía se dio durante la década de los ochenta, impulsada por los cambios en el modelo económico de los postulados de la economía neoclásica para redinamizar el crecimiento en Europa, Estados Unidos, América Latina, y más tarde, en las naciones del sudeste asiático. Este tipo de reformas, basadas en el pensamiento teórico de la Escuela de Chicago y el Consenso de Washington, presentó una serie de cambios estructurales al modelo económico del Estado de Bienestar, hegemónico a nivel mundial hasta ese entonces en las economías de libre mercado, que crearon una tendencia de desestatización de la economía que redujo gran cantidad de derechos laborales y sociales, vinculados a la figura de ciudadanía, que poseían las personas en múltiples países del mundo (Marchetti, 2009).

Lo anterior, trajo una nueva era de crecimiento modesto a las naciones de los países desarrollados y en vías de desarrollo, también estuvo acompañado de un fuerte malestar social, que incrementó de las desigualdades y procesos de marginación. En ese punto, el concepto de soberanía se ve cuestionado desde la raíz de la *responsabilidad de proteger*, que tiene su origen en la idea de la soberanía westfaliana, en el marco de la reducción del Estado de Bienestar, éste se había vinculado a nociones culturales como la identidad nacional, y jurídicas, como la ciudadanía (Stacy, 2002; Gans, 2001). El cambio del modelo del Estado Bienestar al Estado de la Liberación Económica separó por completo los términos de identidad nacional, ciudadanía y soberanía. Dado que las últimas dos décadas de siglo XX se vieron marcadas por el señalamiento, surgimiento y activismo político de grupos sociales marginados de parte de la estructura del Estado, tales como los indígenas, migrantes, grupos religiosos, comunidad LGBT, etc. (Grotenhuis, 2016; Sassen, 2000)

Esto se da a razón de que el principio de la *responsabilidad de proteger*, que argumentaba que correspondía al Estado el salvaguardar la integridad de la población y el proporcionar una serie de garantías y derechos que poseían sus ciudadanos, se transformó por completo. E incluso, algunos estudios dentro del paradigma de la globalización demostraron que múltiples

sectores de la sociedad con diferencias étnicas, culturales, lingüísticas, etc., no se sentían incluidos y representados en la conceptualización de la identidad cultural hegemónica de los Estados (Hafner-Fink, Malnar, & Uhan, 2013; Shevel, 2009). A la par, se consideraban que ostentaban derechos ciudadanos incompletos o de segunda categoría, por lo cual los gobiernos no cumplían en todos los sectores de la población este principio, haciéndolo parte del paradigma westfaliano. Esto derivó en que se repensara la categoría de los Estados-Nación, y se empezara a hablar cada vez más de países, con múltiples nacionalidades representadas por diferentes grupos sociales, según su importancia en la estructura y cultura del gobierno, aportaban elementos a la identidad nacional, dependiendo de sus características étnicas, sociales y culturales, accedían a derechos ciudadanos completos o incompletos (Krasner 2001; Sassen, 2000).

Por último, la tercera ola que sustenta el paradigma de una soberanía post-westfaliana se localiza en la reducción de las fronteras físicas, territoriales, económicas y tecnológicas a nivel global. Esto está relacionado con dos acontecimientos importantes de la década de los noventa, que son: el final de la Guerra Fría y el avance de las nuevas tecnologías de comunicación, trascendentes dentro del proceso de globalización. Respecto al primero, se destaca que la conclusión de la Guerra Fría, con la desintegración de la URSS, fue un golpe a la visión realista de la soberanía, que tenía como uno de sus más grandes fundamentos a la integridad territorial. Lo anterior derivó que la idea de seguridad nacional[9] se empezara a alejar de este fundamento, a partir el surgimiento de las amenazas no convencionales en las diferentes regiones y zonas del mundo. Ya que nuevos fenómenos que afectaban la integridad del Estado-Nación como el crimen organizado, narcotráfico, migración, cambio climático o terrorismo, ya no estaban atados o inmersos en la dinámica de las fronteras territoriales.

Por otra parte, el avance de las tecnologías, en la que jugó un papel protagónico el internet, aceleró el flujo de interacciones políticas, económicas y culturales. Las economías se integraron más a razón de la velocidad de los intercambios comerciales y financieros. Al mismo tiempo que los fenómenos políticos se interconectaban más, dada la capacidad de

[9] Los vínculos entre soberanía, seguridad nacional y ciberseguridad se tratan a profundidad en el punto 2.4 de este capítulo de investigación. En este apartado se cita el concepto de seguridad nacional sólo para demostrar que incluso este concepto, insertó a profundidad en la idea de la soberanía, se transformó radicalmente con el surgimiento de las amenazas no convencionales en el contexto internacional.

acceso a información de primera mano de lo de lo que pasaba en cada país, principalmente proporcionada por usuarios de internet y medios de comunicación. De hecho, tendencias como la Primavera Árabe, el auge del populismo y las recientes protestas de América Latina, en 2019, muestran esto. También, se puede argumentar que el internet y sus múltiples aplicaciones, como las redes sociales y medios de comunicación, crearon una unidad cultural que permite convivir a cualquier persona, con sus semejantes, en cualquier otra latitud del mundo (Peters, 2005).

Con base en la recapitulación anterior, este trabajo de investigación refrenda la hipótesis de que vivimos en la era de la soberanía post-westfaliana, dado que existen tres épocas que cuestionan los fundamentos básicos de la soberanía tradicional: *la autodeterminación, la responsabilidad de proteger* y *la integridad territorial*.

La primera se remonta al proceso de integración de la Unión Europea, en donde los Estados de la CECA sacrificaron su capacidad de decisión soberana en aras de la creación de una comunidad, hoy unión, que les brindó beneficios económicos, políticos y laborales. La segunda, se da en el cambio del modelo económico del Estado de Bienestar al Estado de la Liberalización Económica. En que los derechos civiles de la ciudadanía se desprenden del principio de la responsabilidad de proteger y la identidad nacional. Por último, la tercera época se enmarca en el fin de la Guerra Fría y la prescripción de la integridad territorial en el marco de la concepción de la seguridad nacional. Época que estuvo acompañada del auge y viralización de la tecnología del internet, instrumento que redujo las barreras y fronteras en todas las esferas de la sociedad.

2.3 ¿Soberanía en el ciberespacio? De qué estamos hablando

¿Podemos hablar de soberanía en el ciberespacio? Nuestra discusión en torno a la era post-westfaliana de la soberanía nos acerca a las características de este dominio, dado que está plataforma carece de múltiples elementos que definieron al Estado-Nación desde su creación. En ella, variables como *las fronteras territoriales* no existen. Sin embargo, nuestra explicación de los hechos ciberfísicos presentada en el primer capítulo de esta investigación, denota que las dinámicas del ciberespacio pueden tener impacto en el espacio físico o material. Asimismo, partimos de la hipótesis central de esta tesis, la cual expresa que las dinámicas surgidas en el ciberespacio pueden tener alcances en la soberanía, seguridad

nacional y política exterior de los Estados-Nación, a través de los hechos ciberfísicos. Por lo que nos compete analizar cómo los diferentes elementos que definen a dicho concepto se vinculan en este dominio.

En ese sentido, empezaremos con el principio de la *responsabilidad de proteger*, el cual, en el caso del ciberespacio, está relacionado a la doctrina de seguridad nacional de cada país. Por ejemplo, los países democráticos conciben al internet como un instrumento que sirve como canal de comunicación para la expresión de opiniones políticas o ideológicas, por parte de su población, a la par de ser una plataforma económica capaz de traer beneficios en las dinámicas comerciales, en el cuál se debe salvaguardar y garantizar la privacidad, integridad y libertades de las personas. Sin embargo, para las naciones con regímenes autoritarios, cómo es el caso de la República Popular China, Corea del Norte, o con democracias débiles, tales como Rusia o Venezuela, el internet se transforma en un medio a través del cual el Estado puede vigilar a la población para garantizar la seguridad y sobrevivencia del régimen, visión que pone por delante la seguridad del Estado, por encima de las personas.

Respecto al principio de *autodeterminación,* este es quizás el fundamento de la soberanía tradicional que más puede empatarse con la noción del *ciberpoder* que se abordó en el capítulo pasado, desde la perspectiva del constructivismo y la Teoría de la Guerra, el neorrealismo y el poder del Estado, y finalmente, la Teoría de la Comunicación, Teoría de Sistemas y la Complejidad. Las primeras dos perspectivas tienen en el centro a los Estados-Nación y en ambas se hace explícito que la finalidad de los países, en el contexto internacional, es garantizar su sobrevivencia, defensa e integridad, y posteriormente, utilizar las características de los diferentes dominios (tierra, aire, mar, espacio y ciberespacio), así como las tres caras del poder, para alcanzar una posición privilegiada en el concierto de las naciones. Si bien, la superioridad en los *teatros de guerra,* de Clausewitz, y la creación de un *régimen* o *tratado del ciberespacio* se concentran en la visión de que los Estados son entidades que buscan la creación y posesión de ciber poder, la visión liberal abordada en nuestra discusión en torno a la soberanía nos demuestra que no todos los países del mundo poseen los medios y capacidades para ser actores de trascendencia en este campo.

En la actualidad, la creación de tecnología de vanguardia vinculada al internet, centrada en nuevos sistemas como la *inteligencia artífica, machine learning, big data o internet de las*

cosas, está limitada a un puñado de naciones. Por lo cual, los países que no sean capaces de desarrollar este tipo de capacidad tecnológica se verán en la circunstancia de tener que contratar los servicios de entidades del sector privado (con origen en los países que sí detenten estas competencias), para poder tener presencia en el dominio del ciberespacio y las capacidades mínimas de defensa en esta arena. No obstante, mientras no creen una política de seguridad nacional, que tenga como eje central incrementar y mejorar sus fortalezas del ciberespacio, este grupo de países estarán condenados y rezagados en la creación de ciberpoder a diferencia de los países de vanguardia. De igual manera, el tema de la autodeterminación se vuelve central cuando se aborda el tema del uso y control de la Infraestructura Nacional Crítica de los Estados, ya que los sistemas de energía, agua, gas, electricidad o manejo y administración de vías de comunicación requieren de un importante nivel de ciber defensa y capacidad soberana para garantizar la seguridad de la población y la sobrevivencia del Estado. Esta situación, llega incluso a sistemas que no están completamente en la esfera del Estado, y están más en la zona de influencia del sector privado, como los sistemas bancarios, financieros o de medios de comunicación e información. Lo que denota, que en efecto como considera el paradigma liberal, los países que están rezagados y no cimenten en el futuro esfuerzos por reducir la brecha tecnológica con las potencias del ciber espacio, tendrán menor capacidad de autodeterminación en sus decisiones como Estados (Cowley, 2011). En ese sentido, se concluye que el internet, al igual que las dinámicas económicas y comerciales derivadas de la integración europea, así como las consecuencias socioculturales, derivadas del cambio del modelo de Estado de Bienestar al Estado de la Liberalización Económica, son parte de las fuerzas a nivel internacional que han enmarcado la era post-westfaliana que se vive en la actualidad.

En el marco de las ideas y los debates en torno a la soberanía y su comprensión en el dominio del ciber espacio, diversos teóricos, autores civiles y militares, e incluso países, han abordado el tema. Una de las primeras concepciones de interés es la expresada por Franzese (2009), un militar de la fuerza aérea norteamericana, que expresa que a inicios del siglo XX dos teorías operaban en la Ciencia Política en torno a esta discusión. La primera argumentaba que el ciberespacio es inmune a la soberanía del Estado y la segunda definía al ciberespacio como un bien común. Esta noción se dio en el periodo de popularización del internet entre las empresas y la sociedad civil, en que se exaltaban las fortalezas de este medio de

comunicación como su capacidad de supervivencia – a diferencia de otras tecnologías-, flexibilidad y alto rendimiento, más centrados en los objetivos comerciales -como bajo costo, simplicidad o atractivo para el consumidor (Carroll, 200). También, aspectos como su colegialidad, descentralización de la autoridad e intercambio abierto de información se consideraba crearían nuevas dinámicas sociales en temas de opinión pública, libertad de expresión, elección política y poder de la sociedad frente al Estado (Brate 2002).

Para refutar la primera teoría, Franzese (2009) expresa que el ciberespacio no es inmune a la soberanía del Estado por cinco concretas razones:

1) El ciberespacio debe ser controlado por al menos una entidad para que exista y funcione[10]. Esto se vincula al hecho de que el ciberespacio tiene una parte física -que abordamos en el capítulo de esta investigación y se expresa en elementos como la infraestructura en telecomunicaciones y capacidad de conectividad, acceso a energía e Infraestructura Crítica- y sin ella los usuarios no pueden acceder a él. Esta parte física del ciberespacio recae en un espacio terrestre, marítimo, aéreo o espacial, dominios dónde los fundamentos de la soberanía estatal se han establecido desde hace ya varios siglos o décadas, por lo cual el ciberespacio debe sujetarse a la regulación y supervisión de los Estados-Nación.
2) La segunda razón es que el ciberespacio está sujeto a relaciones financieras que requieren de leyes para el control de las transacciones y actividades económicas. En ese sentido, el ciberespacio no es inmune a la soberanía del Estado, dado que las decisiones comerciales en el dominio están fuertemente influenciadas por las leyes de un país respectivo.
3) La tercera razón se vincula al hecho de que el contenido enviado a través del ciberespacio tiene importancia en el mundo físico o material. Ya que, si bien el internet fue creado para mejorar el flujo libre de información, ésta plataforma no protege o resguarda la información de interés válido para el Estado, así como a dónde se envía, recibe o almacena, esto aplica a información vinculada a actividades ilícitas

[10] Franzese (2009) hace referencia en su texto a la Corporación de Internet para la Asignación de Nombres y Números (ICANN por sus siglas en inglés) como una de las entidades reguladoras del internet. En la actualidad organismos como la ITU, la Organización Europea de Entidades Gestoras de Dominios de Primer Nivel con Código de País (CENTR) y la Asociación de Dominios de Niveles Superiores Geográficos de Latinoamérica y el Caribe (LACTLD) también juegan este papel.

que son definidas como ciber crimen, tales como la pornografía infantil, robo de identidad, rodo de información personal o robo financiero. Y es verdad que cada uno de estos delitos están sujetos a las leyes y códigos de los respectivos países dónde se efectúan. De igual manera, los Estados tienen capacidad coercitiva en encarcelar, enjuiciar e imponer las respectivas sanciones a quienes cometan estos delitos.

4) La cuarta razón es que los Estados-Nación, con el paso del tiempo, se han visto más obligados a afirmar su presencia en el ciberespacio como una cuestión de seguridad nacional. Y en los hechos, cada vez más elementos del gobierno están conectados y son operados a través del ciberespacio. Asimismo, en la última década, la necesidad de crear una Estrategia Nacional de Ciber Seguridad[11] (ENCS) se ha vuelto un elemento clave para la Seguridad Nacional.
5) La última razón es que, si bien en sus inicios el internet se presentó como un medio para promover la libertad de las personas, con el pasar de los años se ha visto como también sirve para explotar intereses individuales, crear caos, obtener ventajas sobre un competidor o difundir un mensaje específico de odio o violencia. Ante esas condiciones, el ciberespacio requiere del poder coercitivo de la soberanía Estatal para regular, controlar y castigar a los actores que utilicen el internet para estos fines. También, la perspectiva del ciberpoder también denota la influencia de la soberanía en el ciberespacio, dado que múltiples explotan el dominio como un campo para ganar ventajas estratégicas y militares sobre otros Estados o competidores.

Respecto a la segunda teoría mencionada anteriormente, se contrasta que el ciberespacio no tiene características que definen a un bien común, tales como un tratado internacional que lo rija, establecimiento de usos y prohibiciones específicos permitidos, límites y definición (Stern, 2011; Hurwitz, 2012). A la par de que los bienes comunes detentan características como el hecho de que las naciones han acordado renunciar a determinados reclamos de soberanía exclusiva sobre cualquier parte de estos y ningún Estado es capaz de controlar en su totalidad. Con lo que se argumenta que los estos bienes globales representan la ausencia

[11] Más adelante se abordará la concepción de ciberseguridad desde diferentes ENCS de múltiples países del mundo.

de soberanía, sino más bien la presencia mundial de una soberanía compartida (Chertoff, 2014; Falkner, 2012).

La discusión anterior se centra en relacionar a la idea de la soberanía en el ciberespacio con su parte física y con la ausencia de la creación de un *tratado del ciberespacio* para su regulación global. Sin embargo, autores como Demchak y Dombrowski (2013) expresan que si bien las ideas de la soberanía westfaliana no aplican en el contexto del internet, la autonomía de decisión y acción, expresada en la capacidad de resiliencia y disrupción, serán el principal elemento que en futuro definan la capacidad soberana de un Estado en el ciberespacio. En este sentido, Lewis (2009) comparte los fundamentos de esta visión al expresar en un futuro cercano los países líderes del internet serán aquellos que en el futuro cercano consoliden fronteras defendibles en este dominio ante sus oponentes y adversarios, a través de una política efectiva de Seguridad Nacional, promovida por el gobierno, que considere crucial para la defensa del Estado-Nación a la ciberseguridad.

En los hechos, más de cien países en la actualidad poseen y han generado avances en aras de la creación o consolidación de una *Estrategia Nacional de Ciberseguridad* (ENCS), las cuales consideran aspectos como construcción de capacidades en el ciberespacio, creación de un marco legal adecuado para el dominio, cooperación internacional y capacidad de resiliencia y reacción frente a ciber amenazas (Libicki, 2009). Por otra parte, el CCDCOE de Tallin, que es parte de la OTAN, expresa que todos sus miembros cuentan al menos con una primera versión de su ENCS, que es considerada una subrama o parte complementaria de una estrategia de seguridad nacional, en las que han establecido sus propias definiciones de ciberespacio, ciberseguridad y han delimitado las ciberamenazas a su seguridad, a la par de implementar protocolos de acción y reacción frente a ciber incidentes.

Del mismo modo, se destaca que incluso los países autoritarios son conscientes de la importancia del ciberespacio, e incluso naciones como la República Popular de China han promovido en la comunidad internacional los fundamentos para la creación un concepto de ciber soberanía. Sobre este asunto, Lindsay (2015) destaca que este país comprende a la soberanía en ciberespacio como:

> "*la capacidad de evitar y bloquear la influencia no deseada en el ciberespacio de un actor extranjero, con la finalidad de evitar que los*

ciudadanos sean expuestos a ideas y opiniones consideradas perjudiciales para el régimen."

Concepción que denota que, para este país, está en un primer orden la seguridad del Estado-Nación, y en segundo, la seguridad de las personas. Asimismo, se destaca que la República Popular de China pone énfasis en que es necesario cambiar la estructura del régimen internacional de la gobernanza del internet de la actualidad – que engloba a empresa privadas, organismos internacionales, empresas de telecomunicación y académicos- a un foro internacional como la Organización de las Naciones Unidas, que transfiera el poder y regulación del ciberespacio de las compañías e individuos, sólo a los Estados, con lo cual este país promueve uno de los esfuerzos más insistentes en dejar la regulación del internet en la completa esfera de los Estados-Nación, y en consecuencia, bajo la influencia de los intereses de estos actores (Schia, & Gjesvik, 2017; Iasiello, 2017b).

2.4 Puntos de encuentro en la soberanía y seguridad nacional

A pesar de que la noción post-westfaliana se posicionó en la comunidad internacional desde mediados del siglo XX, en el marco de la Guerra Fría, la noción tradicional de la soberanía tuvo vigencia en la era el mundo bipolar, al menos en lo que compete a la esfera de la seguridad nacional. Posterior a la caída del bloque socialista, el auge de la liberalización económica, la globalización y el surgimiento de las amenazas no convencionales, los teóricos de la seguridad ajustaron la comprensión de la seguridad a las características de estos nuevos fenómenos sin renunciar a posicionar al Estado-Nación en el centro de la discusión de la seguridad nacional e internacional. Lo anterior, se debe a que las raíces de este precepto se encuentran en el hecho de que la principal aspiración y razón de existir de una estrategia y doctrina de seguridad nacional es la sobrevivencia del Estado. En ese sentido, el presente apartado, sirve para presentar los vínculos entre los conceptos de soberanía y seguridad nacional, como un preámbulo para establecer dónde se encuentra la ciberseguridad dentro de esta doctrina del Estado-Nación.

El primer precedente de la creación de una doctrina de seguridad se dio en Estados Unidos, en los años inmediatos al fin de la II Guerra Mundial. Al mismo tiempo que el país buscaba consolidarse como la principal potencia militar y económica del mundo, así como su

influencia internacional y hegemonía en el continente americano. De acuerdo a Rivas y Rodríguez (2010), es con la promulgación de la *National Security Act* o Acta de Seguridad Nacional, de 1947, que Estados Unidos crea su primera doctrina vinculada a mantener su seguridad como Estado-Nación. Para estos autores, la doctrina de los años cuarenta está fuertemente influenciada por el pensamiento político de Thomas Hobbes y la Teoría de la Guerra de Clausewitz. En ese sentido, ésta abarca y mezcla conceptos de defensa militar, seguridad pública e interior. A la par, establece que para garantizar la seguridad e intereses de Estados Unidos es necesario proteger su integridad territorial, seguridad interior, estabilidad de instituciones y defensa de valores (Mardones, 2005).

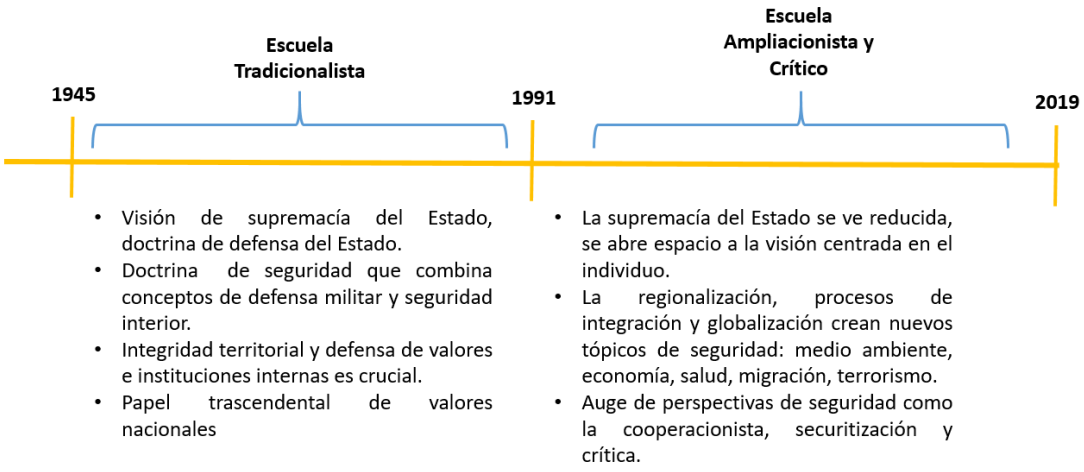
De esta forma, se observa que la doctrina tiene una doble función, una que se proyecta hacía el interior del país y se vincula a combatir las amenazas y reducir factores de riesgo cómo un todo de la sociedad, salvaguardando la identidad, valores y cultura estadounidense de la amenaza comunista, así como su zona de influencia continental (las américas) e influencia ideológica (Europa, y puntos de Asía como Corea del Sur o Japón). Y una función con proyección hacía el extranjero, que en el marco de la confrontación del modelo capitalista-democrático contra el socialista-dictatorial, tenía tres características: 1) defensa de valores de occidente -democracia y economía de libre mercado-, 2) defensa y promoción de la idiosincrasia estadounidense en el mundo; y 3) defensa de territorio y autodeterminación para Estados Unidos y sus aliados (Rivas y Rodríguez, 2010),. De esta forma, la proyección de la doctrina de seguridad nacional fuera de las fronteras del Estado-Nación tiene un nexo concreto con la política exterior, a tal punto que es considerado un documento estratégico del poder nacional (Klimburg, 2012). En ese sentido, se observa como la influencia de la seguridad nacional también tiene una implicación en la política entre las naciones[12].

Desde su origen, es posible detectar como tres fundamentos de la soberanía westfaliana están incluidos en la doctrina de seguridad nacional de Estados Unidos –la integridad territorial, responsabilidad de proteger y autodeterminación del Estado-Nación-, los cuales pasan a formar parte de la *escuela tradicionalista* de la seguridad nacional que surge con el Acta de Seguridad Nacional. Para Barcena-Coqui (2000), este primer paradigma se define por ideas

[12] El tema de los vínculos entre la soberanía, política exterior y ciberseguridad es un tema que se desarrollará a profundidad en el capítulo 3 de esta investigación.

como la visión de la supremacía del Estado por encima de la población -incluso en los países democráticos y de occidente-, la unión de la defensa militar y seguridad interior con tal de garantizar la salvaguarda de las instituciones de gobierno, a la par de contener un importante contenido ideológico cimentado en los valores nacionales. Posteriormente, con la caída el bloque socialista, en 1991, un nuevo núcleo de temas en torno a la seguridad se insertaría en el seno de la seguridad nacional, con lo que surgirían dos nuevas escuelas: la ampliacionista y la crítica, como se muestra en la figura 9. Ambas escuelas se vieron influenciadas por el reposicionamiento del individuo como núcleo de la seguridad nacional y por el surgimiento de las amenazas no convencionales. Por su parte, las dos escuelas se definieron por compartir ideas como la reducción de la supremacía del Estado en el nuevo entorno global de finales del siglo XX, el surgimiento de complejos de seguridad y su regionalización a razón de los procesos de integración y globalización, así como pasar a englobar nuevos tópicos de seguridad como la protección del medio ambiente, economía, salud, migración, terrorismo, etc.

Figura 9. Evolución de la Doctrina de Seguridad Nacional 1945-2019.



Fuente: Elaboración propia con base en Barcena-Coqui (2000) y Rivas y Rodríguez (2010).

Un aspecto de importancia en torno a la evolución de la doctrina de seguridad nacional de Estados Unidos se encuentra en que para varios autores existen dos puntos de referencia para entender cómo evolucionó este concepto, que se dan durante los gobiernos de los presidentes Harry Truman y George W. Bush (Van Vugt, 2015). Respecto al primero se establece que el Acta de Seguridad Nacional (1947) estableció los fundamentos de una primera concepción

en torno a la seguridad nacional, la cual se cimentó en defender el hemisferio occidental de la creciente influencia del mundo comunista, el cuál puso énfasis en que, para garantizar la seguridad nacional de Estados Unidos, este país debía volverse un mediador, garante y protector de los estados democráticos. En ese sentido, nociones como la teoría de la contención, cimentada en los preceptos de George F. Kennan, y en la superioridad bélica frente a la Unión Soviética, permearon la idea de la integridad territorial y la responsabilidad de proteger en la doctrina. Asimismo, es importante destacar que de acuerdo con el Artículo 5 de la OTAN, esta garantía se hizo extensiva no sólo al territorio de la unión americana, sino a todos los países que eran miembros de la alianza militar que compartían los valores de occidente. En ese sentido, la discusión inaugural que se hizo al inicio de este capítulo demuestra un fuerte impacto de estos fundamentos clásicos de la soberanía en el surgimiento de la doctrina de seguridad nacional.

Posteriormente, el segundo punto se da con la reestructuración que sufrió la Estrategia de Seguridad Nacional durante el gobierno del presidente George W. Bush, que terminó con el relanzamiento de esta en 2002. Y la estructuración del documento más acorde a las necesidades de seguridad de Estados Unidos, que se habían transformado después de los atentados terroristas del 11 de septiembre de 2011, en Nueva York y Washington D.C. En este punto, vale la pena señalar que, si bien la noción postwefaliana de la soberanía empezó a imperar durante la década de los cincuenta en la comprensión de la política exterior en diferentes países, pero principalmente en Europa, con el inicio de la integración europea, se resalta que la formación de este bloque comercial no supuso una amenaza para la sobrevivencia de los Estados-Nación desde la comprensión de la seguridad nacional. Por lo cual, si bien es cierto que el debate postwestfaliano empezó a impactar durante las décadas de los sesentas, setentas y ochentas en esferas como la economía, política y cultura, esta no tuvo impacto en la doctrina de seguridad nacional.

De esta forma, con el fin de la Guerra Fría la simetría del enemigo se desdibujó por completo para Estados Unidos, ya que durante los años de conflicto contra la URSS éste era materializado por un Estado-Nación enemigo, que era fácilmente identificable y se ajustaba a los preceptos clásicos de la Teoría de la Guerra y el realismo político. Sin embargo, con los atentados terroristas del 9/11, la noción en torno a las amenazas y los adversarios se

transformaron radicalmente, ya que grupos terroristas como Al-Qaeda vulneraron la seguridad y soberanía de los Estados Unidos de una forma atípica a como se consideraba a una amenaza desde la visión del Acta de Seguridad Nacional. Dado que este enemigo no tenía intenciones de conquistar el territorio de este país, o limitar su capacidad de decisión soberana, pero sí dañar a su población y causar terror entre ella.

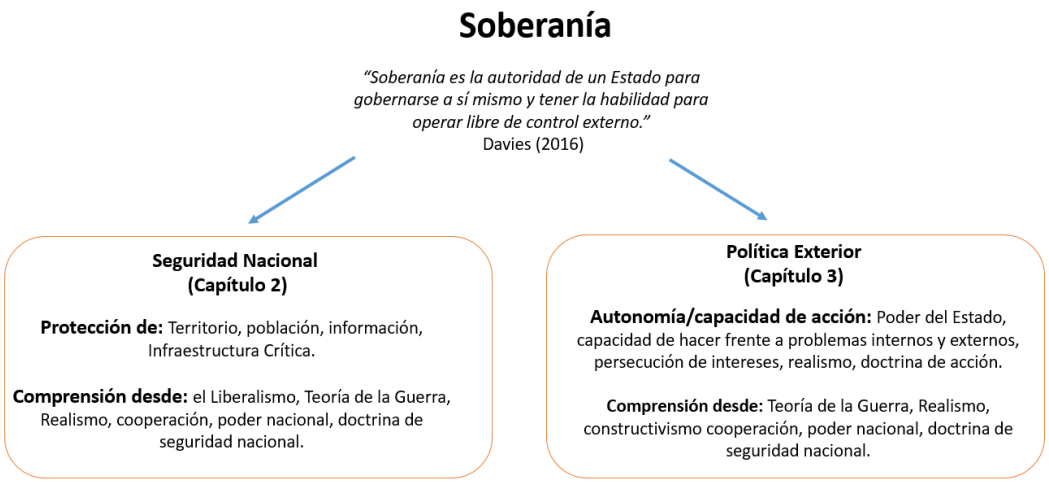
De esta forma, el conflicto y la conceptualización de la guerra sufrieron un cambió en el contexto de las nuevas amenazas, que se ajustan a los preceptos de Van Creveld (1991; 2002) ya que se hizo tangible que los nuevos enemigos de la seguridad nacional e internacional eran adversarios de capacidades asimétricas, con líneas de acción de baja intensidad y dónde características como superioridad a través del tiempo y el espacio no podían ser determinadas. En este punto, es que los fundamentos de la soberanía postwefaliana alcanzaron la dimensión de la doctrina de seguridad nacional en Estados Unidos.

Esto se vio reflejado en la nueva versión del documento de 2002, que incluyó aspectos como la promoción de los derechos humanos, fomento de alianzas contra el terrorismo, atención de conflictos regionales y la transformación de las instituciones de seguridad nacional de EE. UU., más en sintonía a los retos de la seguridad del mundo post-westfaliano (Tarzi, 2014; Jervis, 2003)

Con la discusión anterior se señalan los nexos que existen entre el concepto de soberanía – ya sea en su visión tradicionalista y postwestfaliana, con la doctrina de seguridad nacional, objetivo central de este capítulo. No obstante, también quedan visibles los vínculos que existen entre estos dos conceptos y la política exterior. Asunto que se tratará a detalle en el capítulo tres de esta investigación.

En la figura 10 se presenta la vinculación y comprensión entre esta triada de conceptos. También, aún queda pendiente presentar el papel que ocupa la ciberseguridad dentro de la doctrina y estrategia de seguridad nacional.

Figura 10. Nexos entre soberanía, seguridad nacional y ciberseguridad.



Fuente: Elaboración propia.

2.5 El papel de la ciberseguridad en la estrategia y doctrina de Seguridad Nacional

La ciberseguridad es un tema que empezó a hacer presente su importancia en la seguridad nacional y política internacional a finales de la década de los noventa del siglo XX. Como se mencionó anteriormente, desde su creación, durante la década de los sesenta, hasta el año 2000, se pensó que el internet era un espacio libre de la injerencia del Estado e inmune a la soberanía que transformaría el flujo de información, democratizaría el conocimiento y cambiaría las dinámicas de participación ciudadana. Este periodo -que abarca los años de 1960 a 2000-, es definido por Palfrey (2010) como la *fase de acceso abierto* del ciberespacio y comprende su popularización en la sociedad y uso cada vez más constante en la economía, medios de comunicación, temas de gobierno y demás esferas de la sociedad. No obstante, las dinámicas derivadas de este proceso lo hicieron un campo en que la injerencia del Estado-Nación fue inevitable y necesaria. En ese sentido, se resalta que, al momento de su popularización e inclusión en la vida cotidiana de las personas, a finales del siglo XX, la era postwefaliana de la soberanía llevaba más de cuarenta años de desarrollo.

Asimismo, la creación de la doctrina de seguridad nacional tenía más de medio siglo de existencia y los debates en torno a la comprensión de las nuevas amenazas a la seguridad nacional e internacional se discutían en el núcleo teórico de la academia en los años inmediatos a la Guerra Fría. Sin embargo, es precisamente en el proceso de globalización y liberalización económica, que aconteció en el sistema internacional a finales del siglo pasado,

que el internet se vuelve uno de los instrumentos clave para acelerar y consolidar este proceso. Por lo cual la necesidad de su control y regulación se empieza a hacer presente por parte de los gobiernos de los diferentes países del mundo.

En ese sentido, la primera penetración del Estado-Nación en la esfera del internet se da durante los años 2000- 2005, que es definida como la *fase del acceso negado* (Palfrey, 2010; Deibert y Rohozinski, 2010). Esta inmersión de los gobiernos en el ciberespacio se da a razón de que los gobiernos empezaron a considerar que existen actividades y expresiones en el internet que deben ser reguladas, administradas, e incluso bloqueadas. Respecto a esto, Zitrain y Palfrey (2007) en el informe *Access Denied: The Practice and Policy of Global Internet Filtering,* documentaron que durante ese período alrededor de 70 países y 289 proveedores de servicio de internet crearon legislaciones para el control de actividades en el dominio, o implementaron filtros para controlar su contenido o bloquearlo. El primer conjunto de legislaciones de este tipo se dio en el campo económico, dado que el internet mostró su gran potencial para acelerar las dinámicas comerciales, por lo cual los gobiernos tuvieron que avanzar en el desarrollo de legislaciones y códigos que regularan las actividades comerciales.

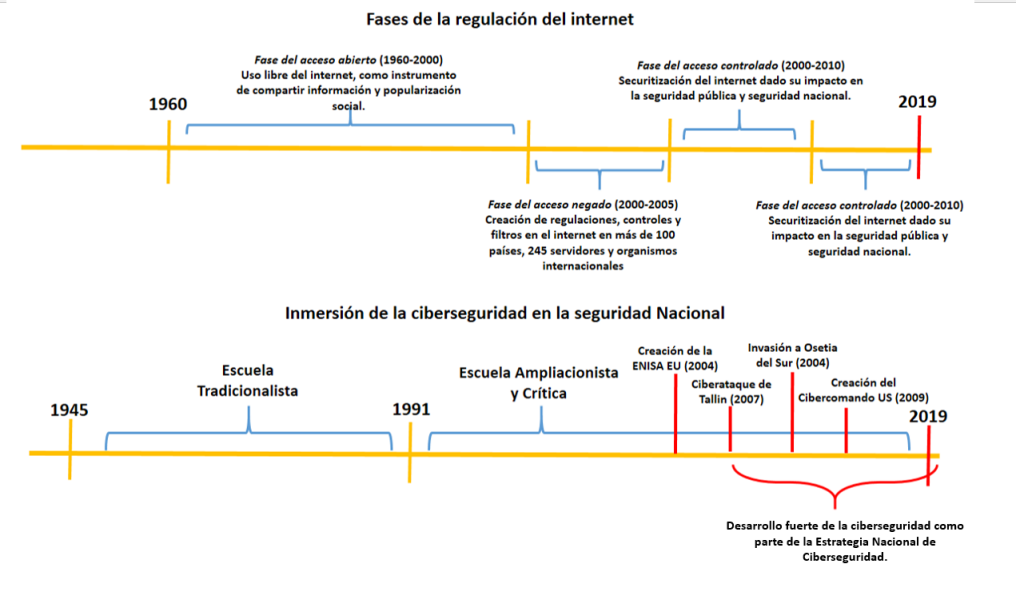
Posteriormente, la segunda etapa de la injerencia del Estado se da en el control de los contenidos legales e ilegales y regulación del flujo de datos e información. Esta aplicación de controles coercitivos en el internet se dio tanto en los países democráticos, como autoritarios. Las diferencias oscilan en que naciones como la República Popular de China, la Federación Rusa y Arabia Saudita, crearon filtros de control de contenido y prohibieron el flujo de información o acceso a sitios en línea que se consideró que podrían crear dinámicas negativas o contra el gobierno. Mientras que en las naciones democráticas los países redactaron leyes y códigos de justicia que se aplicaron en las actividades económicas, políticas y de medios de comunicación en el internet.

También, es importante destacar que fue durante estos años, que el internet sufrió un proceso de securitización, en que los países pusieron énfasis en crear nuevas definiciones para delimitar delitos o actividades ilícitas que se realizaran a través de esta plataforma o utilizaran este para su consolidación. En los hechos, más de cien países establecieron en sus códigos de justicia y sistemas penales definiciones sobre los ciber crímenes que debían ser juzgados y

castigados por el Estado. De igual manera, organismos internacionales como la Organización para la Cooperación Económica (OCDE), la Unión Europea (UE), o la Unión Internacional de Telecomunicaciones (ITU), crearon convenios y acuerdos para la regulación de estas actividades, hasta la creación del Convenio de Budapest en 2004, que fue el primer intento de una armonización sobre ciber delitos para su investigación y persecución (Palfrey, 2010; Klimburg; 2012, Take, 2012).

Es en este punto que el ciberespacio mostró su capacidad de injerencia en la seguridad pública y se empezó a evaluar su capacidad de impacto en la seguridad nacional. Por lo que se considera que la *fase del acceso negado* no creó como tal bordes y barreras reales en el internet, pero sí empezó a delimitar las líneas geopolíticas de contacto entre los diferentes países en su tendencia política, modelo económico e intereses nacionales. Posteriormente, sería en la *fase de acceso controlado*, que abarca de los años 2005 a 2010, que el proceso de securitización del ciberespacio alcanza a la seguridad nacional. Esto se dio a través de la creación de marco instituciones que previnieran ciber incidentes y eventos concretos a nivel global, entre los primeros destaca que tanto la Agencia Europea de Seguridad de las redes y de la información (ENISA por sus siglas en inglés), como el Cibercomando de Estados Unidos, consideraron que el uso del ciberespacio, por grupos terroristas islámicos era una acción que podía vulnerar la seguridad nacional del Estado (Newmeyer, 2015; Samaan, 2010). Sin embargo, en los hechos, eventos como el ciberataque de Tallin, Estonia (2007), o el hackeo a la red gubernamental de Georgia, durante la invasión de Osetia del Sur (2008) mostraron el potencial que tenía el ciberespacio para vulnerar a un Estado-Nación. Sería a razón de sucesos como estos que la ciberseguridad pasa a ser un apartado necesario en toda doctrina y estrategia de seguridad nacional de un país, para garantizar su seguridad y capacidad de decisión soberana. Y es precisamente a raíz del hecho de Tallin que todos los países de la OTAN, y posteriormente el resto del mundo, comenzaron a crear sus primeras versiones de una Estrategia Nacional de Ciberseguridad (ENCS), cómo se muestra en la figura 11.

Figura 11. Fases de regulación del internet e inclusión de ciberseguridad en seguridad nacional



Fuente: Elaboración propia con base en Palfrey (2010), Barcena-Coqui (2000), Rivas y Rodríguez (2010).

Por último, Palfrey (2010) expresa que desde 2010 nos encontramos en la *fase de la contienda*, que se define por la confrontación entre las diferentes partes interesadas al interior del ciberespacio y su capacidad para crear consensos y la gobernanza dentro de este dominio. Para Aguilar-Antonio (2020), lo anterior se refleja en el hecho de los gobiernos del mundo han avanzando en una amplia y necesaria inclusión de actores para consolidar el régimen del ciberespacio y el desarrollo de políticas y ENCS de ciberseguridad, como parte fundamental de la estrategia de seguridad nacional.

2.6 La construcción de una Estrategia Nacional de Ciberseguridad

A raíz del ciberataque de Tallin, Estonia (2007), la necesidad de crear una ENCS que forme parte de la estrategia global de Seguridad Nacional se volvió una exigencia para todas las naciones miembros de la OTAN. Para 2011, un total de veinte países, de los 29 que conforman esta alianza, ya contaban con su primera versión de este documento, en el que se presentaba su definición de ciberseguridad y una delimitación de las ciber amenazas consideradas con capacidad de vulnerar la seguridad nacional.

Por su parte, la Unión Internacional de Comunicaciones, en 2013, realizó la primera medición del *Índice Global de Ciberseguridad* (*GCI* por sus siglas en inglés), dicho organismo definió

a esta medida como "*una referencia confiable que mide el compromiso de los países con la ciberseguridad a nivel mundial, para crear conciencia sobre la importancia y las diferentes dimensiones del problema*" (GCI, 2013). En su primera medición, el GCI contó con la participación de 105 países, de un total de 193 naciones miembros de este organismo. Sin embargo, para la cuarta aplicación de su metodología, englobó a un total de 153 países. A nivel internacional es considerada uno de los referentes más importantes que permiten delinear las ciber capacidades de defensa de un país, dado el conjunto de campos de aplicaciones, industrias, y actores, que evalúa en sus cinco pilares (medidas legales, medidas técnicas, medidas organizativas, desarrollo de capacidades y cooperación y se encuentran a la vanguardia de la agenda global de ciberseguridad.

Del mismo modo, en 2018 la *E- Governance Academy* presentó la primera versión del Índice Nacional de Ciberseguridad o (*National Cyber Security Index* o *NCSI* en inglés), dicho documento fue financiado por el Ministerio de Relaciones Exteriores de Estonia y la Agencia de Cooperación para el Desarrollo del mismo país. Su trascendencia radica en que esta medida reconoce que la ciberseguridad es un desafío global que no puede ser garantizado por un sólo país. Con lo cual el NCSI proporciona una visión general de la ciberseguridad y las capacidades de defensa de 100 diferentes naciones, a través de cuatro esferas del gobierno, que se traducen en 3 categorías de ciberdefensa, 12 capacidades y 46 indicadores, en los que se señalan las buenas prácticas y muestran los aspectos a mejorar de cada uno de estos países.

En los hechos, estas mediciones sirven a los gobiernos para la estructuración o mejora de sus ENCS. Sin embargo, en muchos aspectos los retos de la ciberseguridad avanzan más rápido que la capacidad de acción de los gobiernos. Tan sólo en 2017, se presentaron 1,579 brechas de información en el sector financiero de Estados Unidos, las cuales aumentan a una tasa promedio de 44.6% anual (GBA & ITRC, 2018). Al momento que se escribe este texto, de acuerdo con *T-Sec Radar* de *Deutsche Telekom* se dan 60,312[13] ciberataques cada minuto, lo que representa 3, 712, 960 por hora, y 79,390, 302 en un solo día (Sicherheitstacho, 2019). Por su parte, la plataforma Digital Attack Map (2019) lleva el registro diario de los ataques DDoS en el mundo, que son accesibles a cualquier individuo, empresa o gobierno por tan

[13] Las visualizaciones de mapas en torno a ciber incidentes de *T-Sec Radar* de *Deutsche Telekom* es una de la aplicaciones más impresionantes que permite tecnologías de vanguardia como el *internet of things* (IoT) y el Big Data, una visualización rápida puede verse en este link: https://sicherheitstacho.eu/start/main

sólo 150 dólares[14]. Por lo que este sitio se encarga de detectar su origen y país destino, los cuales alcanzaron cifras de más 8,000 diarios durante el último año. A la par que el *Cyberthreat Real-Time Map,* de la empresa Kapersky (2019) contabiliza minuto a minuto ocho[15] diferentes tipos de ciber incidentes alrededor del mundo, además de contabilizar los cinco países con más infecciones cibernéticas, a través de sus sistemas y aplicaciones antivirus. Datos como los anteriores, implican que las ENCS estén en la necesidad de constante actualización.

En ese sentido, el BID y la OEA (2018) expresan que muchas naciones deben aún alcanzar la madurez en sus ENCS para poder encarar los retos que implica la ciberseguridad en la actualidad. De esta forma, para poder abordar nuestra hipótesis vinculada a qué el ciberespacio es un nuevo campo de la política internacional a través del cual se puede vulnerar la seguridad nacional y la soberanía de un Estado-Nación, debemos comprender qué entienden los diferentes países por ciberseguridad y ciber amenazas, así como las partes interesadas del sector privado, en torno a este dominio.

2.6.1 Ciberseguridad y ciber amenazas: la visión de los actores estales

En el apartado 1.4 del capítulo 1, de esta investigación se presentó una serie de conceptos clave para la comprensión del ciberespacio desde el análisis político y las relaciones internacionales. En ese sentido, sirvió para conceptualizar una noción académica de lo que entiende por ciberseguridad desde autores de la ciencia política como Kello (2012) o Hughes (2010). No obstante, nuestra discusión en torno a la doctrina de seguridad nacional, su comprensión desde la soberanía y los intereses del Estado-Nación, nos llevan a entender a la ciberseguridad como una construcción intersubjetiva que edifica cada país, en torno a sus intereses nacionales, valores, cultura, ideología y aspiraciones en torno a cómo se ven a sí mismos como nación y el papel que desean ocupar en el contexto internacional. Basta revisar los conceptos de ciberseguridad de diferentes ENCS, para observar esto en los hechos. De esta manera, este apartado se centra en una discusión en torno a la compresión de la

[14] Los ataques DDoS son de los más accesibles y baratos, y los que más éxito tienen en vulnerar seguridad informática, la plataforma de *Digital Attack Map* muestra la profundidad y utilización diaria de esta modalidad de ciber agresión: https://bit.ly/2qPHqCe

[15] Las amenazas que mide el *Cyberthreat Real-Time Map* día a día son: en 1) en escaneo de acceso, 2) escaneo de baja demanda, 3)virus a través de e-mail, 4) escaneo de detección de intrusos, 5) antivirus en páginas web, 6) escaneo de vulnerabilidad, 7) Lapersky anti-spam, 8) actividad de detección *botnet.*

ciberseguridad y amenazas, desde las ENCS, así como entender los perfiles de ciber amenazas desde diferentes ópticas que permitan sustentar nuestra hipótesis de investigación. Para lo anterior, se revisó el apartado de *Estrategia y gobernanza,* de la biblioteca del CCDCOE Tallin (2021), que presenta estrategias de seguridad y defensa nacional, ENCS, legislaciones nacionales –vinculadas al ciberespacio-, y declaraciones de derecho internacional, de un total de 77 naciones, entre las que se incluyen miembros de la OTAN, aliados estratégicos de esta alianza, así como de múltiples países de África, América Latina, el Caribe, Asia y Oceanía. En ese sentido, se clasificó el total de documentos elaborados en torno a la ciberseguridad, que alcanzaron una cifra de 210, y se agruparon en cuatro diferentes grupos de países: 1) países y aliados de la OTAN y otros países de Europa, 2) países de América Latina y el Caribe, 3) países de Asia y; 4) países de Medio Oriente y África.

Posteriormente, se extrajo la definición de ciberseguridad y ciber amenazas de una selección de países para una discusión en torno a la comprensión del concepto y amenazas a la seguridad nacional desde el ciberespacio. También, un aspecto de importancia que se realizó fue calcular el promedio de documentos, estrategias y legislaciones en torno al tema de la ciberseguridad que han elaborado los cuatro diferentes grupos de países. Lo anterior, se realizó en torno a que los cuatro indicadores[16] del GCI ITU (2018) consideran que el avance de construcción de capacidades, mejoramiento tecnológico y organizacional y consolidación de cooperación entre instituciones estatales y privadas es visible través del número de documentos que cada país ha elaborado para mejorar sus capacidades de defensa y acción en el ciberespacio, así como avanzar en la gobernanza de este dominio con el apoyo de las partes interesadas. De esta forma, la redacción cada vez más constante y mayor de documentos vinculados a la construcción de capacidades en el ciberespacio refleja dos cosas:

1) La importancia que dan los países y sus gobiernos al ciberespacio como un instrumento del poder nacional y dominio de defensa vital para garantizar la seguridad nacional y la promoción de los intereses nacionales, y;

[16] La descripción completa de la métrica del GCI (2018) se da en el apartado 2.7.3 de este capítulo de investigación.

2) el grado de experiencia, reformulación de objetivos, integración y organización entre los actores estatales y los actores no estatales, para crear la gobernanza del ciberespacio y la construcción de la ciberseguridad.

En ese sentido, en la tabla 4 se presentan los resultados obtenidos de este análisis, en el que se observa que los países que más han abordado el tema de la ciberseguridad a través de estrategias y legislaciones nacionales han sido las naciones miembros de la OTAN sus aliados estratégicos y países de Europa, con un promedio d 3.8 ENCS por país en la región. También, se destaca que hay países que han dado un peso vital al dominio del ciberespacio como dominio de la seguridad y poder nacional, en el proyecto de nación. Entre estos destacan naciones como Estados Unidos, que desde 2014 ha creado un total de trece documentos vinculados a la construcción de capacidades como Estado-Nación en el ciberespacio. O Países Bajos, con un total de siete documentos. Sin embargo, es importante mencionar que la creación de una gran cantidad de documentos vinculados al tema no siempre se refleja en la consolidación de una ENCS bien estructurada, tal es el caso de Israel, que cuenta sólo con tres documentos, o de Estonia, con un total de cinco.

De igual manera, es importante observar que países de otras regiones del mundo se encuentran rezagados en torno al desarrollo de su ENSC. Por ejemplo, en América Latina son contados los países que han creado al menos dos documentos vinculados a la construcción de capacidades nacionales en el ciberespacio –Brasil y Colombia-, lo que denota que el país tenga un promedio de 1.12, muy semejante al de Medio Oriente y África. Por otra parte, Asia es una región que presenta una visión muy dispar, dado que países como China y Japón han dado una importancia vital al ciberespacio como instrumento para garantizar la seguridad nacional, con un total de cinco documentos cada uno. Mientras el resto de los países de la región sólo han elaborado una ENCS, no obstante, los datos muestran que se encuentra mucho más aventajada que América Latina con un promedio de 2.3. Asimismo, se destaca que Medio Oriente y África son los países que menos importancia han dado al uso de la arena del ciberespacio en la elaboración de una ENCS y creación de legislaciones para la construcción de capacidades. Lo anterior, muestra una brecha geopolítica en temas de proyección del Estado-Nación en el ciberespacio, construcción de ciberpoder y ciber capacidades. Dónde hay un claro rezago de otras regiones del mundo frente a los países de

occidente. Esta situación se refleja en las definiciones de ciberseguridad de las naciones de la OTAN y Europa, que están mejor estructuradas que las de otros países. También, es importante destacar que la delimitación de ciber amenazas con capacidades de vulnerar la seguridad nacional del Estado-Nación, están más establecidos en éste primer grupo de países, que en el resto del mundo. Sin embargo, también existen polos en otras zonas del planeta que buscan una proyección a futuro en el ciberespacio.

Tabla 4. Promedio de documentos y estrategias sobre el ciberespacio.

Grupos de países	Promedio de documentos y ENCS.
Países y aliados de la OTAN y otros países de Europa.	3.8
Países de América Latina y el Caribe.	1.12
Países de Asía.	2.3
Países de Medio Oriente y África.	1.11

Fuente: CCDCOE Tallin (2021).

2.6.1.1 Anatomía de la ciberseguridad de los países de la OTAN, sus aliados estratégicos, y otros países de Europa.

En cuestiones de seguridad los países de la OTAN, y sus aliados estratégicos, representan el conjunto de naciones que más importancia han dado al dominio del ciberespacio como una esfera esencial para garantizar la seguridad nacional y proyectar el poder e intereses del Estado. En ese sentido, destaca que este conjunto de naciones fueron las primeras en crear ENCS en conjunto y de forma paralela, durante el periodo 2008-2014, en aras de consolidar un régimen de estatutos, definiciones, marcos legales y desarrollo de capacidades para construir una gobernanza del ciberespacio, que garantizara su seguridad como Estados individuales y como conjunto de países que forman parte de esta alianza (CCDCOE Tallin, 2021). Asimismo, la dimensión doctrinaria es concretamente más visible en estos países que en los de otras regiones del mundo. De esta forma, se destaca que esto se ve reflejado de dos formas, 1) en la materialización de los intereses nacionales a través de la construcción del poder nacional-más vinculado a los Estados-Nación que se asumen como potencias o protagonistas de la sociedad internacional, 2) aquellos países que optan por la promoción de

un multilateralismo para la construcción de un *Tratado del ciberespacio* en las diferentes ENCS. Por último, se señala que ambas categorías – definición de ciberseguridad y ciber amenazas- se encuentran en la tabla 5, que engloba a un total diez naciones. De este análisis Aguilar-Antonio (2020) presenta las siguientes conclusiones en torno a la concepción de ciberseguridad:

a) El ciberespacio es un componente del poder nacional: la importancia del ciberespacio para la seguridad nacional es visible en cada una de las ENCS. No obstante, es importante diferenciar la forma en que cada Estado entiende el ciber poder. Para casos como Estados Unidos, la EOTPW (2017) muestra la definición de un país que se asume como una potencia internacional. Por su parte, Estados como Israel (NCD, 2017) o Australia (AAGD, 2009) develan que la construcción de ciber capacidades como un factor de relevancia dentro de su política de seguridad nacional, sus intenciones de contribuir a la consolidación de la gobernanza y securitización multilateral del ciberespacio, mas no expresan sus intenciones de ser las entidades reguladoras de un régimen global.

b) La presencia del multilateralismo y cooperación: el conjunto de países asume que la regulación del ciberespacio es una tarea conjunta que debe realizarse entre diferentes naciones. No obstante, existen países con una marcada tendencia más abierta a la cooperación internacional – como es el caso de Alemania (FG, Germany, 2016) y Países Bajos (DMSJ, 2011; MFA, 2018)- a los que buscan garantizar su capacidad de decisión soberana, con independencia de estar abiertos al multilateralismo – Turquía (MTMAC, 2016), Reino Unido (UK Cabinet Office, 2011), e Israel (NCD, 2017).

c) El ciberespacio es un instrumento de proyección internacional: países con modesta o menor participación en esferas globales o regionales, a las potencias tradicionales del contexto internacional, utilizan al ciberespacio como un instrumento para posicionarse como potencias en este dominio. El caso más representativo de esto se da en Estonia, país que tiene una importancia relativamente baja en temas culturales, financieros o políticos en la región europea, pero que en el ciberespacio representa a una de las naciones de vanguardia, con intenciones de crear aportes a la construcción de la seguridad internacional en este campo (MSJ, 2017; MEAC, 2019).

Tabla 5. Definición de ciberseguridad y ciber amenazas según los países y aliados de la OTAN y otros países de Europa.

País	Definición de Ciberseguridad	Ciber amenazas
Canadá	"*La ciberseguridad es la protección digital de la información y la infraestructura que reside en direcciones de seguridad cibernética, atender los desafíos y amenazas del ciberespacio para asegurar los beneficios y oportunidades de la vida digital* (CDPS, 2010, p. 4)."	Ciber crimen en dos categorías según CDPS (2010): 1. *Tradicional:* fraude, abuso, acoso y explotación sexual a través del internet. 2. *Crimen de objetivos tecnológicos:* hackeo, esquemas de fraude de ramsonware, ataques DDoS, etc. Ciber amenazas avanzadas: • Espionaje y ciber explotación, robo de información confidencial, seguridad nacional o propiedad intelectual del Estado, ataque a Infraestructura Crítica Nacional.
Turquía	"[ciberseguridad es la]…p*rotección de los sistemas de información que forman el ciberespacio de ataques, asegurando la confidencialidad, integridad y disponibilidad de la información y datos procesados en este entorno, detectar de ataques e incidentes de seguridad cibernética, activación de mecanismos de contra-respuesta y sistemas de recuperación a las condiciones antes de incidente de seguridad cibernética* (MTMAC, 2016, p. 3)."	Cuatro tipos de amenazas según MTMAC (2016): . 1. Interrupción de transporte, suministro de energía o INC a través del ciberespacio. 2. Robo, divulgación, modificación o destrucción de información personal e información confidencial de propiedad del gobierno o de INC (*ramsonware* o ciber explotación, hacktivismo). 3. Daño material o de reputación a compañías, instituciones, empresas, medios de comunicación o sistemas de servicios. 4. Ciber crimen, robo de datos o información, fraude, realización de actividades ilícitas, delitos financieros.

País	Definición de Ciberseguridad	Ciber amenazas
Alemania	*"…* [la] *ciberseguridad global se conforma de la ciberseguridad civil y militar, esta es el objetivo deseado de la situación de seguridad informática, en la que los riesgos del ciberespacio global se han reducido a un mínimo aceptable. Por lo tanto, la seguridad cibernética en Alemania es el objetivo deseado de la situación de seguridad de TIC´s, en la que los riesgos de Alemania en el ciberespacio se han reducido a un mínimo aceptable* (FG Germany, 2016, p. 4)*."*	Ciber amenazas de dos tipos según FG Germany (2016): 1. Civil: uso fraudulento de datos, espionaje industrial, daño a de sistemas informáticos de rutas de comercio y transporte, ciber crimen. 2. Militar: daños a INC, amenazas hibridas, afectación de sistemas de comunicación, cadenas de suministro o suministro de materias y energía.
Países Bajos	*"La ciberseguridad es liberarse del peligro o daño debido a la interrupción, avería o mal uso de las TIC´s. El peligro o daño resultante de la interrupción, desglose, o el mal uso puede consistir en limitaciones a la disponibilidad o confiabilidad de las TIC´s, violaciones de la confidencialidad de información almacenada en medios de comunicación o daños a la integridad de esa información* (DMSJ, 2011, p. 3)*."*	4 tipos de amenazas según (MFA, 2018): 1. *Interrupción o disrupción no deseada extranjera:* hackers, países o grupos organizados que busquen desestabilizar la influencia política y económica de Países Bajos, engloba desinformación, ciber espionaje y terrorismo. 2. *Amenazas militares:* daños al territorio nacional o de aliados a través del ciberespacio, por INC, amenazas hibridas, vulneración del espacio aéreo o naval, amenazas nucleares o de armas de destrucción masiva. *3. Amenazas vitales al proceso económico:* ciber espionaje industrial, daño a rutas de comercio físicas (rutas marítimas) o digitales (cables en mar profundo), aseguramiento de materias primas y energía, protección de inversiones. *4. Amenazas de armas químicas, biológicas, radiológicas y nucleares (CBRN):* protección del uso o posesión de este tipo de armas, por parte de Estados o grupos organizados, contra

País	Definición de Ciberseguridad	Ciber amenazas
		la seguridad de Países Bajos, Europa, o los aliados de la OTAN.
Estonia	*"La ciberseguridad nacional es un término amplio que abarca muchos aspectos de la información, los datos y los medios electrónicos, servicios que afectan los intereses y el bienestar de un país. Garantizar así la seguridad del ciberespacio de un país comprende una gama de actividades en diferentes niveles. Con este fin, los dominios de políticas más importantes deben reducir la vulnerabilidad del ciberespacio, prevenir los ciberataques en primera instancia y, en caso de un ataque, asegurar una rápida recuperación del funcionamiento de los sistemas de información. Por lo tanto, una estrategia de defensa cibernética debe evaluar la vulnerabilidad de la infraestructura crítica de un país, diseñar un sistema de medidas preventivas contra ataques cibernéticos y decidir sobre la asignación de tareas relacionadas con la gestión de la seguridad cibernética a nivel nacional. Además, también es importante mejorar el marco legal contra los ataques cibernéticos, para mejorar cooperación institucional, y para sensibilizar al público y desarrollar programas de capacitación e investigación sobre ciberseguridad* (MSJ, 2017, p. 4)*."*	Tres tipos de amenazas según MEAC (2019): 1. *Amenazas a la sociedad digital y el Estado:* protección de datos e información personales y del Estado, protección de INC, protección de ransomware, ataques DDoS, seguridad frente a ciber crimen. 2. *Amenazas a la industria, investigación y desarrollo:* protección de propiedad privada de start-ups en el sector seguridad, protección de investigaciones en torno a ciberdefensa y propiedad intelectual. Protección de cadenas de suministro, comercio y exportación. 3. *Contribución internacional a la ciberseguridad:* aporte de Estonia a la gobernanza del ciberespacio y solución de amenazas contra la OTAN, la ONU, la OSCE y la Unión Europea.
Reino Unido	*"[*ciberseguridad son las*] acciones tomadas para reducir el riesgo y asegurar los beneficios de un entorno digital confiable para empresas e individuos* (UK Cabinet Office, 2011, p. 5)*."*	4 grupos de ciberamenazas según la HM Government (2016): 1. Ciber criminales: extorsión, fraude, *ramsonware*, ataques DDoS, actividades ilícitas de internet. 2. Amenazas estatales y patrocinadas por los Estados: ciber espionaje, ciber explotación, ramsonware y destrucción de información.

País	Definición de Ciberseguridad	Ciber amenazas
		3. Terroristas: uso de ciberespacio para atentados terroristas y reclutamiento de miembros. 4. Hacktivistas: ataques DDoS, *insiders* a sistemas críticos o bases de datos de información de seguridad del Estado. 5. *Script Kiddies*: individuos que utilizan programas o malwares creados por otras personas para realizar ciber ataques.
Estados Unidos	*"la política de ciberseguridad incluye estrategia, política y estándares con respecto a la seguridad y las operaciones en el ciberespacio, y abarca el rango completo de reducción de amenaza, reducción de vulnerabilidad, disuasión, compromiso internacional, respuesta al incidente, resistencia y políticas de recuperación y actividades, incluidas red de computadoras operaciones, aseguramiento de la información, derecho aplicación de la ley, diplomacia, militar y misiones de inteligencia y como se relacionan éstas con la seguridad y estabilidad de la infraestructura global de información y comunicaciones. Esta no incluye otro tipo de política de información y comunicación no relacionado con nacional seguridad o aseguramiento de la infraestructura* (EOTPW, 2017, p. 2)."	4 tipos de amenazas según (EOTPW, 2017): 1. Amenazas a las redes e información federales: 2. Amenazas a las infraestructuras críticas: 3. Combate al ciber crimen y mejora de notificación de incidentes: 4. Amenazas a la economía digital y propiedad intelectual:
España	*"*[ciberseguridad es] *el uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques que afecten al estado español, a este fin debe servir la Política de Ciberseguridad Nacional* (PG España, 2013, p. 6)*."*	Según la DSN (2019) Entre las amenazas se encuentran: • Estados extranjeros, causas técnicas, fenómenos naturales, hacking, conflictos, crimen organizado, amenazas internas, terrorismo, sabotaje, hacktivistas, individuos aislados, delincuencia, espionaje, organizaciones terroristas.

País	Definición de Ciberseguridad	Ciber amenazas
Australia	*"*[ciberseguridad son las] *medidas relacionadas a la confidencialidad, disponibilidad y integridad de la información, que se procesa, almacenado y comunicado por medios electrónicos o medios similares* (AAGD, 2009, p. 8)*."*	Entre las amenazas se encuentran (AAGD, 2009): • Amenazas a la seguridad nacional, amenazas a la seguridad pública y privacidad de los individuos (ciber crimen), amenazas a la economía y comercio, amenazas a la seguridad internacional.
Israel	*"[*ciberseguridad son las*] acciones directas del Estado para confrontar ciberamenazas y esfuerzos indirectos destinados a alentar y apoyar actividades de seguridad en el sector privado y colaborando con él. El concepto de operaciones define tres capas operativas: fortalecer la robustez cibernética, resistencia cibernética sistémica y defensa cibernética nacional. El enfoque de tres capas se deriva de la naturaleza única de las ciberamenazas y el papel central de las organizaciones privadas para lograr ciberseguridad nacional Las tres capas difieren entre sí en sus objetivos, en el papel del Estado y en las relaciones entre el Estado y organizaciones privadas* (NCD, 2017, p. 5)*."*	Tres tipos de amenazas según la (NCD, 2017): • Amenazas a la ciberseguridad de los mercados y el sector privado. • Amenazas a la información del Estado, disposición y generación. • Amenazas a la seguridad nacional.

Fuente: Elaboración propia con base en CCDCOE (2019)

Lo anterior, aplica también a naciones como Países Bajos –que tienen una importancia económica, política o temas de seguridad, mediana en la Unión Europea o la OTAN, pero que ven proyectadas sus capacidades de injerencia en el ciberespacio (DMSJ, 2011; MFA, 2018)-, o en países que se distinguen por utilizar el *soft power* tales como Canadá (CDPS, 2010) o Australia (AAGP, 2009).

d) *La ciberseguridad tiene una dimensión civil, militar y estatal:* el conjunto de Estados demarca de forma concreta los diferentes niveles que engloba la ciberseguridad y el tipo de ciber amenazas que existen en cada nivel. Para el caso de Estonia, esta nación marca una diferencia entre amenazas a la *sociedad digital* -claramente de carácter civil o de seguridad pública-, a las *amenazas al Estado* -de connotación militar (MEAC, 2018). Esta misma situación se ve reflejada en el caso de Alemania[17] y Canadá[18]. Por otra parte, destaca la clasificación que utiliza Países Bajos al hablar de amenaza militares y amenazas CBRN[19], que se encuentran en la esfera de responsabilidad de la seguridad nacional. La combinación de la dimensión civil con la militar corresponde a un enfoque integral de cooperación civil-militar para la seguridad nacional (Klimburg, 2012).

e) *Vinculación actores estatales-actores no estatales o privados:* la importancia de la construcción de nexos entre las partes interesadas está presenten en este grupo países, principalmente en actores estatales y actores no estatales organizados. Esta asociación estratégica se presenta en al menos tres dimensiones: 1) Se reconoce la necesidad e interdependencia del Estado-Nación con la iniciativa privada, principalmente instituciones de creación de tecnología de vanguardia en internet o sistemas informáticos, para la construcción de ciber capacidades. 2) Se incentiva y considera vital la creación de conocimiento para consolidar capacidades de resiliencia y

[17] Alemania utiliza la clasificación civil y militar para diferenciar amenazas del ciberespacio para la seguridad pública y la seguridad nacional.
[18] Canadá utiliza la clasificación de amenazas tradicionales para describir a actividades como el ciber crimen, mientras que habla de amenazas avanzadas para hablar de amenazas a la seguridad nacional como ciber espionaje, ataques a INC, amenazas hibridas, terrorismo, etc.
[19] Son las letras del acrónimo en *inglés Chemical, Biological, Radiological* y *Nuclear*. Es decir amenazas que se realizan a través de armamento no convencional o armas de destrucción masiva.

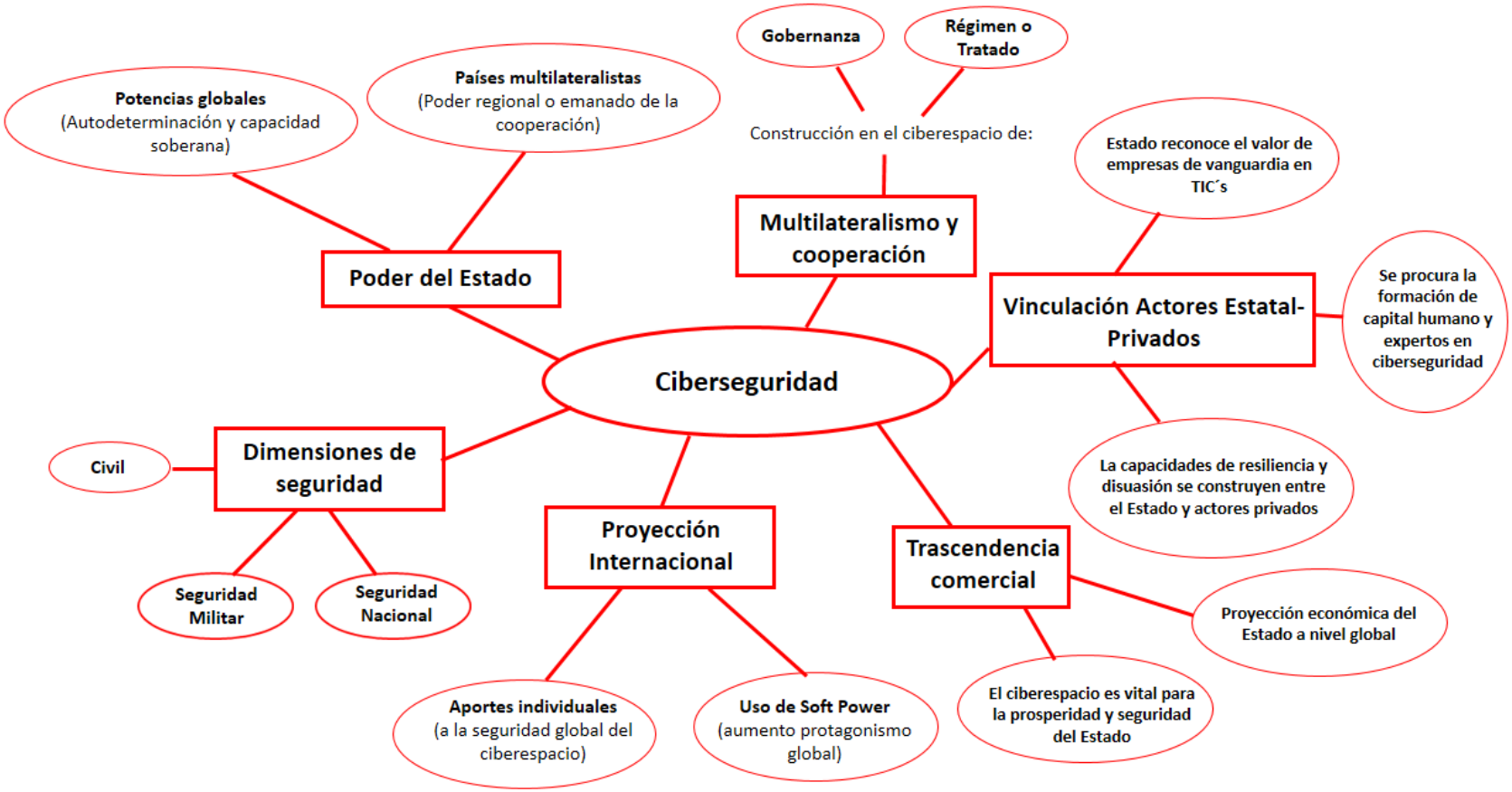
disuasión en el ciberespacio, en ese sentido, países como Estonia promueven la creación de posgrados o programas académicos o científicos vinculados al tema de la ciberseguridad (MEAC, 2019). 3) Se expresa la necesidad de contar con capital humano o profesionales expertos en ciberseguridad frente a los retos emanados en el ciberespacio, como es el caso de Israel (NCD, 2017)

f) *Se comprende y diferencia la parte física y virtual del ciberespacio:* las estrategias hablan de las diferencias entre las tecnologías de la información (TIC´s), vinculadas a sistemas informáticos, bases de datos, etc., y relacionadas a la parte virtual del ciberespacio. Y las tecnologías de la operación (OT´s), relacionadas a infraestructura nacional crítica, cadenas de suministro, rutas de transporte y comercio, etc., Asimismo, establecen las amenazas que pueden presentarse a la seguridad nacional desde el ciberespacio en la esfera civil, militar y nacional.

g) *Se reconoce la trascendencia comercial y económica del ciberespacio:* los documentos generados por el Estado, tales como Estrategias de Seguridad Nacional, ENCS, legislaciones nacionales o declaraciones de derecho internacional, contienen apartados en los que se aborda la importancia de la dimensión económica y comercial del ciberespacio. Así como el papel que juega este en la prosperidad del Estado, la seguridad nacional y la proyección del país hacia el exterior.

Para concluir se destaca que la figura 12 presenta una anatomía de la concepción de ciberseguridad de los países de la OTAN, sus aliados y otras naciones de Europa.

Figura 12. Anatomía de la ciberseguridad de países y aliados de la OTAN.



Fuente: Elaboración propia.

2.6.1.2 Tipos y clasificaciones de ciber amenazas y vulnerabilidades de países de la OTAN

De acuerdo con Lindstrom y Luiijf (2012) la delimitación de las ciber amenazas y vulnerabilidades, por parte de un Estado-Nación, debe tener una fuerte convergencia con la Estrategia de Seguridad Nacional (ESN). En ese sentido, estos autores especifican que existen tres elementos en la actualidad que son importantes en la estructuración de una ESN para la definición de amenazas:

I. Debe ser posible para un gobierno trasladar la visión de seguridad nacional del Estado-Nación en una política coherente y con viabilidad de ser implementada. Lo anterior, en vista de que esta condición genera la facilidad de producción de subestrategias de seguridad a través de diferentes dominios –combate al terrorismo, ciberseguridad, seguridad energética, pública o ambiental- consistentes con la ESN global.

II. El Estado debe implementar la ESN en consonancia con sus relaciones diplomáticas e internacionales. En ese sentido, la creación de objetivos a alcanzar por parte de la ESN, como la definición de amenazas, sirven para comunicar el pensamiento estratégico que tiene una nación a otros países y a la comunidad internacional en el largo plazo.

III. La ESN no debe existir en un vacío estratégico, debe tener vínculos con estrategias nacionales e internacionales, o con dinámicas globales o regionales, para alentar un conjunto de políticas con objetivos afines. En el plano nacional esto promueve la coordinación, cooperación y colaboración entre agencia gubernamentales y las partes interesadas. En el marco internacional, promueve alianzas estratégicas y refuerza acciones conjuntas contra amenazas regionales o globales.

La coherencia aplicada de los tres fundamentos citados anteriormente es visible en las ESN o *Libro Blanco* de una gran cantidad de países de OTAN, como se presenta en la selección de la tabla 6.

Tabla 6. Amenazas y vulnerabilidades de según ENS y *Libros Blancos* de la OTAN.

País	Tipo de documento	Año	Ejemplos de amenazas y vulnerabilidades
Francia	Libro Blanco	2008	Armas de Destrucción Masiva (ADM), terrorismo, proliferación de misiles balísticos, ciber ataques, espionaje, redes criminales, riesgos a la salud, riesgos a ciudadanos en zonas vulnerables del extranjero.
Alemania	Libro Blanco	2006	Terrorismo, proliferación de ADM, regiones inestables y Estados Fallidos, conflictos regionales, tráfico de armas ilegales, Estados y gobiernos frágiles, rutas de transporte, seguridad energética, bienes globales, peligros creados por el hombre, amenazas a la salud, desafíos regionales, cambios internos.
Hungría	Estrategia de Seguridad	2012	Terrorismo, proliferación de AMD, regiones inestables y Estados fallidos, migración ilegal, inestabilidad económica, retos de la sociedad de la información, bienes globales, peligros creados por el hombre, amenazas a la salud, desafíos regionales, cambios internos.
Países Bajos	Estrategia de Seguridad	2007	Brechas internacionales de paz y seguridad, amenazas CBRN, terrorismo internacional y crimen organizado, vulnerabilidades de la sociedad, falta de seguridad digital, falta de seguridad económica, cambio climático y desastres naturales, enfermedades infecciosas y de animales.
Polonia	Estrategia de Seguridad	2007	Terrorismo organizado internacional, crimen organizado internacional seguridad energética, debilidad de vínculos transatlánticos, conflictos congelados o regionales, bajos niveles de integración de la vida económica y mercados financieros, amenazas ambientales, desafíos nacionales (cambios de población, infraestructura, suministro de energía).

País	Tipo de documento	Año	Ejemplos de amenazas y vulnerabilidades
España	Estrategia de Seguridad	2011	Conflictos armados, terrorismo, crimen organizado, inseguridad financiera o económica, vulnerabilidad energética, proliferación de ADM, ciber amenazas, flujos migratorios no controlados, emergencias y desastres, infraestructuras críticas, cadenas de suministro y servicios.
Reino Unido	Estrategia de Seguridad	2010	Terrorismo internacional, ataques hostiles en el ciberespacio de Reino Unido, riesgos naturales, accidentes o ataques a territorios de ultramar, riesgos de inestabilidad, crimen organizado, disrupción severa a satélites de telecomunicaciones, disrupción a todos los suministros de gas, disrupción de corto o mediano plazo a recursos esenciales de suministro internacional.
Estados Unidos	Estrategia de Seguridad	2010	ADM, vulnerabilidades en el espacio y ciberespacio, dependencia energética, cambio climático, enfermedades pandémicas, Estados fallidos, terrorismo, redes criminales globales.

Fuente: Lindstrom y Luiijf (2012).

En ese sentido, se destaca que la ciberseguridad pertenece a un Enfoque Integrado de Administración de *Todos los Riesgos*[20], que fue posicionado en la agenda de seguridad de la OTAN por Estados Unidos y Reino Unido, a finales de la primera década del siglo XXI. La importancia de un análisis de todos los riesgos oscila en que permite examinar e identificar la mayor parte de las vulnerabilidades del Estado-Nación, ayuda a calibrar las consecuencias de las amenazas a la seguridad nacional, y permite buscar vías innovadoras para proteger a la sociedad. También es importante resaltar que dicho enfoque reconoce que garantizar el cien por ciento de seguridad no es viable o realista, pero hace énfasis en la coordinación intra

[20] *Integrated All-Hazards Risk Management Approach* por su nombre en inglés.

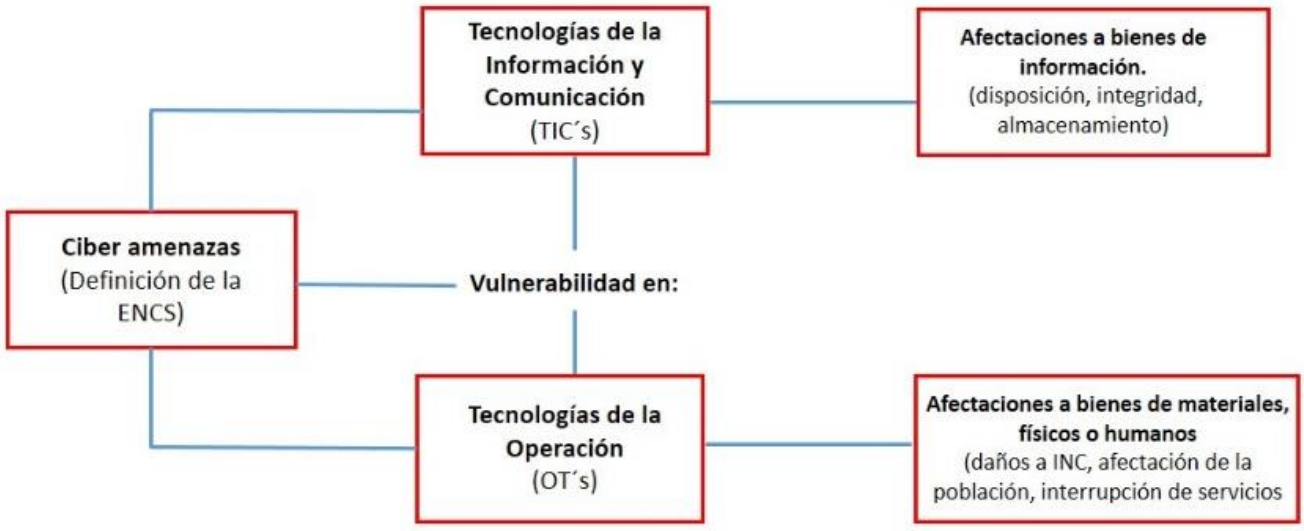
e interestatal, así como las actualizaciones a la amenazas no convencionales o complejas definidas por Buzan *et al.* (1998) a finales del siglo pasado.

Por otra parte, respecto al contenido doctrinario de la ENCS, la definición de ciberamenazas puede ser interpretada en dos perspectivas. Para Goodman (2010) esto expresa las actividades no toleradas en el ciberespacio que se considera pueden tener un impacto en sectores como la economía, vida política, sistemas financieros, privacidad y derechos fundamentales, e infraestructura nacional crítica. Lo anterior, es complementado por Lewis (2014), quien argumenta que la delimitación de ciber amenazas por parte de la ENCS marca las prioridades del Estados, su visión en torno al ciberespacio, así como su nivel de integración con las tendencias globales en torno a ciberseguridad.

Asimismo, se destaca que existe una brecha diferenciada entre la comprensión de amenazas y vulnerabilidades a la seguridad nacional por parte de Estados autoritarios, -entre las que se incluyen control y prohibición de contenidos, discusión política o libertad de expresión-, y los Estados democráticos, que se centran en proteger de una forma comprensiva la integridad del Estado y los derechos de los ciudadanos.

El segundo enfoque se refiera a la vinculación directa que existe entre ciber amenazas y vulnerabilidades por parte de Von Solms y Van Niekerk (2013). Esta conexión oscila en que el Estado debe ser el primero en reconocer las vulnerabilidades que posee la seguridad nacional en la parte virtual (TIC´s) y en la parte material del ciberespacio (OT´s). En relación a lo anterior, el enfoque permite clasificar los diferentes tipos de ciber amenaza en relación a la medición del alcance y grado de profundidad que puede tener las implicaciones de un ciber incidente en la seguridad nacional del Estado-Nación. Este modelo se presenta en la figura 13, en ese sentido, esta propuesta permite vincular las estrategias de reacción, disuasión y respuesta del Estado en los dos campos, frente a un ciber incidente.

Figura 13. Vínculos entre ciber amenazas y vulnerabilidades en ciberseguridad.



Fuente: Elaborado con base en Von Solms y Van Niekerk (2013)[21].

Para cerrar esta sección, se presentan dos propuestas de comprensión de ciber amenazas y vulnerabilidades para la seguridad del Estado-Nación. La primera corresponde al *esquema clásico* más aceptado en los estudios de ciberseguridad y seguridad nacional, en torno a esta perspectiva se posicionan autores como Bendovschi (2016), Tabansky (2011) y el sitio web Hackmageddon (Pessiri, 2019), que recaba estadísticas y líneas de tiempo en torno a ciber agresiones alrededor del mundo. Dicho esquema presenta cuatro tipos de ciber agresiones que se exponen en la figura 14.

[21] Se aclara que el modelo de Von Solms y Van Niekerk (2013), solamente contempla la variable de TIC´s en vulnerabilidades. Sin embargo, su investigación trata el impacto en la esfera material y humana de una ciber amenaza. En ese sentido, se anexa la variable de las OT´s dado que esta permite señalar el grado de afectación que puede sufrir la parte material del ciber espacio.

Figura 14. Clasificación clásica de ciber amenazas y vulnerabilidades de la seguridad nacional.

Fuente: Elaboración con base en Pessiri (2019), Bendovschi (2016) y Tabansky (2011).

La descripción a cada clasificación se presenta a continuación:

- *Ciber crimen:* corresponde a actividades ilícitas realizadas a través del ciberespacio. Estas dinámicas se entienden como una amenaza a la seguridad pública, económica y civil dentro de la esfera global de la seguridad nacional. Se distinguen por ser ejecutadas por grupos organizados que operan fuera del Estado y su objetivo es obtener ganancias o bienes derivadas de éstas (Bendovschi, 2016).

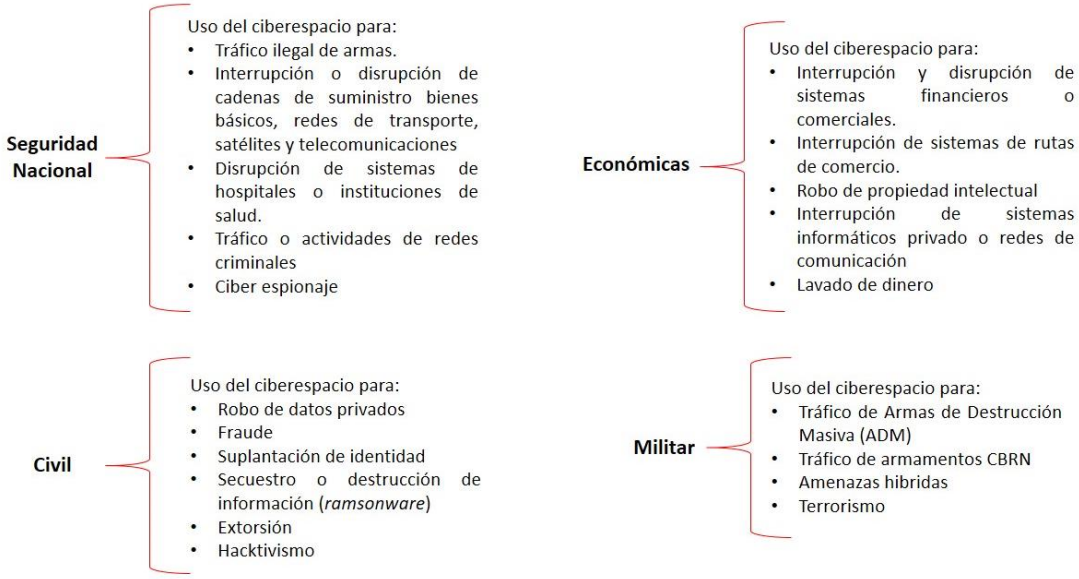
- *Hacktivismo:* actividades de explotación, disrupción, interrupción, secuestro o destrucción de información de bases gubernamentales o que pertenecen al Estado-Nación, el gobierno o sus operadores. A diferencia del ciber crimen, estas actividades no tienen la finalidad de generar ganancias económicas, sino afectar la reputación o estabilidad política del gobierno, a través de la manipulación de información reservada o clasificada que puede ser utilizada en contra del Estado, sus operadores y dirigentes para afectar su imagen pública (Tabansky, 2011).

- *Ciber espionaje:* explotación o robo de información de otros Estados o gobiernos, con el fin de recopilar datos que sirvan para inteligencia y creación de un diagnóstico de vulnerabilidades que den supremacía para efectuar una agresión por parte de un Estado oponente o adversario (Weissbrodt, 2013).

- *Ciber guerra:* disrupción o daño físico o material a elementos que estén bajo la protección o la autoridad soberana del Estado, aplica objetivos civiles, infraestructura nacional crítica, militares, etc. (Kello, 2013, Hughes, 2010)

Por otra parte, derivado del análisis de la definición de ciberseguridad y delimitación de amenazas a la seguridad nacional por parte de los países de la OTAN, realizado en la figura 15, se presenta una *propuesta alterna* de clasificación de ciber amenazas a la propuesta tradicional, centrada en la cual engloba cuatro tipos de ciber amenazas y vulnerabilidades.

Figura 15. Propuesta alterna de ciber amenazas y vulnerabilidades.



Fuente: Elaboración propia.

La delimitación y descripción que se da en cada una de ellas es:

- *Seguridad Nacional:* Amenazas que pueden comprometer la seguridad del Estado-Nación y se vinculan con otras esferas de la seguridad nacional –civil, económica,

militar-, responde a un nivel de amenaza global que involucra a más de una dimensión y esfera del gobierno y necesita de una coordinación intraestatal e internacional.

- *Económicas:* Dimensión centrada en los actores no estatales organizados, en ella se reconoce el uso del ciberespacio como medio para garantizar la prosperidad del Estado y su proyección al exterior. Asimismo, se centra en definir ciber amenazas y vulnerabilidades que pueden afectar la dimensión privada, económica y financiera del Estado-Nación.
- *Civil:* corresponde a la definición del grado de afectación o capacidad de acción de actores individuales en el ciberespacio. En ella se contemplan derechos civiles como la privacidad y protección de datos y ciber delitos centrados en afectar a individuos. Asimismo, se engloba aspectos, como el hacktivismo que representan la actividad de individuos organizados para dañar el prestigio de una autoridad gubernamental, o funcionario público, ya sea con el fin de alcanzar objetivos políticos, o con el fin de dañar su prestigio.
- *Militar:* ciber amenazas que requieren un nivel de especialidad en temas de seguridad que no corresponde a las instituciones de seguridad pública o civil, y comprometen la integridad soberana de los componentes del Estado-Nación, por lo cual se requiere de la atención de las Fuerzas Armadas, en conjunto con otras agencias e instituciones del gobierno.
-

2.6.1.3 La brecha de ciberseguridad en otras regiones del mundo

En la actualidad existe una brecha en torno a la comprensión de la ciberseguridad en múltiples países de otras regiones el mundo fuera de la OTAN y Europa, como América Latina, Asia, África y Medio Oriente. Esta condición se vincula a que una gran cantidad de naciones, en estas zonas, no han dado un papel protagónico dentro de su plan de gobierno al ciberespacio y su comprensión. En ese sentido, tampoco la ciberseguridad ocupa un papel vital en la política de seguridad nacional y en la política exterior. Lo anterior, también tiene un nexo con la penetración del internet, que aún detenta cifras precarias en estas regiones. De acuerdo con la IWS (2019) Norteamérica y Europa son las zonas con el mayor número de usuarios de internet y utilización de esta tecnología en la aplicación de su vida diaria, con cifras de 88.1% y 86.8%, respectivamente. No obstante, regiones como América Latina (59.6%),

Medio Oriente (56.7%), Asia (45.2%) y África (27.7%), muestran una distancia aún muy amplia para empatarse con los países que se encuentran a la vanguardia en temas del ciberespacio.

De esta forma, las ENCS de estos países poseen una marcada distancia en su nivel de integración con las tendencias globales de ciberseguridad a las naciones de la OTAN, como puede observarse en la tabla 7, en el que se presenta la definición de ciberseguridad y ciberamenazas. En ese sentido, el estudio de BID/OEA (2017) marca una distinción entre la creación de una ENCS, y la consolidación o madurez en torno a la comprensión de la ciberseguridad por parte de este mismo documento. Esto se refleja en la tabla 7 que presenta las definiciones de ciberseguridad en una selección de países de América Latina y Medio Oriente, naciones que están en un nivel equiparable a su penetración del internet. De esta forma, se puede observar que, si bien cada definición de ciberseguridad se ajusta a parámetros internacionales, existen ambigüedades en diversas esferas. Dichas lagunas pueden describirse con los opuestos de nuestro análisis derivado de las ENCS de la OTAN y otros países de Europa, en ese sentido los principales elementos que marcan la brecha que existe entre este conjunto de países y la selección de países de la tabla 7 son:

a. No se considera la construcción de ciber poder como mecanismo de proyección nacional. Y la vinculación con la ENS y la política exterior no está bien establecida.
b. El marco de cooperación internacional es ambiguo, dado que no existe una institución internacional que lo coordine –caso OTAN-, además que no se han establecido mecanismos de coordinación para atender problemáticas afines o comunes que afecten a más de un país en el marco regional e internacional, al menos desde el dominio del ciberespacio.
c. No se diferencianlas dimensiones o niveles de amenazas (civil, militar, seguridad nacional). De hecho, el conjunto de ENCS que están en el cuadro 7 utilizan el término de *ciber amenaza,* pero no define cuáles son éstas en el ciberespacio o su impacto en la seguridad nacional de forma concreta.

Tabla 7. Definición de ciberseguridad y ciber amenazas de países de otras regiones del mundo.

País o Gobierno	Región	Año	Definición de Ciberseguridad
Colombia	América Latina y el Caribe	2011 y 2014	"[ciberseguridad es la] *capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética* (CONPES, 2011)*."* *"*[ciberdefensa es la] *capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional* (CONPES, 2011)*."*
Brasil	América Latina y el Caribe	2018	"*La protección del espacio cibernético abarca un gran número de áreas, como la capacitación, inteligencia, investigación científica, doctrina, preparación y uso operativo y gestión de personal. Incluye también la protección de sus propios activos y la capacidad de actuación en red. La instalación del Sector Cibernético tiene como propósito conferir confidencialidad, disponibilidad, integridad y autenticidad a los datos que trafican en sus redes, que son procesados y almacenados* (LBDN Brasil, 2012)."
México	América Latina y el Caribe	2017	*"Es el conjunto de acciones encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad, que permitan a la sociedad, academia, sector privado e instituciones públicas contar con los recursos para la gestión de riesgos y amenazas en el ciberespacio, así como el incremento de la resiliencia nacional* (ENCS México, 2017)*."*
Chile	América Latina y el Caribe	2017	"[ciberseguridad implica] *Proteger la seguridad de las personas en el ciberespacio, llevar a cabo sus actividades personales, sociales y comunitarias normales en el ciberespacio, así como ejercer sus derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad personal. Para proteger la seguridad del país, promover la seguridad de las redes y sistemas de información pertenecientes al sector público y privado, especialmente los que son esenciales para el buen funcionamiento del país, asegurando la continuidad de los servicios básicos. Promover la cooperación y coordinación entre instituciones, mejorar las acciones de comunicación, coordinación y cooperación entre instituciones, organizaciones y empresas, tanto en el sector público como privado, a nivel nacional e internacional, con el propósito de fortalecer la confianza y brindar una respuesta única a riesgos del ciberespacio. Gestionar los riesgos en el ciberespacio, tener en cuenta el desarrollo de procesos de análisis y gestión para el uso, procesamiento, almacenamiento y transmisión de información, así como la creación de capacidades para prevenir y recuperarse de los incidentes de seguridad cibernética que puedan surgir, para para lograr un ciberespacio estable y resistente* (PNCS Chile, 2017)*."*

País o Gobierno	Región	Año	Definición de Ciberseguridad
Costa Rica	América Latina y el Caribe	2017	"[Ciberseguridad es el] Conjunto *de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio* (ENCS Costa Rica, 2017)*."*
Afganistán	Medio Oriente	2014	"[Ciberseguridad es la] *protección de los sistemas de información que protegen el ciberespacio de los ataques, garantizar la confidencialidad, integridad y accesibilidad de la información que se procesa en este espacio, detección de ataques e incidentes de ciberseguridad; poniendo en vigor medidas contra estos incidentes y luego volver a poner estos sistemas en su estado original antes del incidente de seguridad cibernética* (NCS Afganistán, 2017)*."* "[Seguridad cibernética nacional es] *la seguridad cibernética de todos los servicios, procesos y datos, y sistemas involucrados en el aprovisionamiento de estos, proporcionados por la información y la comunicación tecnologías en el ciberespacio nacional."*
Egipto	Medio Oriente	2017	"[Ciberseguridad es la capacidad] *para enfrentar las amenazas cibernéticas y mejorar confianza y seguridad de las TIC infraestructura, y sus aplicaciones y servicios en varios sectores críticos, en para crear un lugar seguro, confiable y entorno digital confiable para el Sociedad egipcia* (NSS Egypt, 2017)*."*
Pakistán	Medio Oriente	2014	"[Ciberseguridad es] *cultivar la conciencia, la responsabilidad y ayudar a desarrollar la capacidad como individuos, organizaciones y empresas para asumir la responsabilidad de asegurar parte propia del ciberespacio; y también educar que lo digital régimen se extiende por todo el mundo y no reconoce ninguna legal o límite geográfico. Las normas de precauciones, prevenciones y los preparativos, por lo tanto, deben coincidir con lo globalmente aceptable parámetros* (NCSCA Pakistan, 2014)*."*

Fuente: Elaboración propia con base en CCDCOE (Tallin).

d. La vinculación entre los actores estatales y no estatales organizados o privados se señala, pero no se expresan niveles de coordinación, ni los medios para construir una gobernanza del ciberespacio, con enfoque que involucre a las partes interesadas.
e. Se hace alusión a conceptos como INC, o amenazas a la información. No obstante, no se diferencia la parte virtual (TIC´s), de la parte física (TO´s) del ciberespacio. Ni cómo las amenazas o vulnerabilidades de la ciberseguridad pueden afectar al Estado-Nación.
f. No se trata a profundidad la importancia económica del internet, ni su trascendencia como medio de prosperidad del Estado-Nación.

La crítica anterior refleja la distancia que existe entre estas naciones con las tendencias globales en ciberseguridad. A pesar de esta situación, en América Latina, una gran cantidad de países se encuentran implementando acciones para reducir la brecha que existe entre el marco de sus ENCS y los temas de vanguardia en el ciberespacio. De esta forma, se destaca qué países han dado importantes pasos con la meta de que sus ENCS alcancen un grado de madurez más en sintonía con las tendencias globales de ciberseguridad. En esta situación destaca Colombia, quien en estos momentos se encuentra en la implementación de su segunda versión de su ENCS. Por su parte, Brasil hizo señalamientos al ciberespacio como esfera de importancia para la seguridad nacional en su *Libro Blanco de Defensa* de, 2014, no obstante, en 2018 presentó su primera ENCS con un enfoque integral más ajustado al contexto global, situación que se hace extensiva a países como Chile y Costa Rica. Por otra parte, la región de Asia se encuentra en un contexto muy heterogéneo, en el que países como China, Japón, Singapur y Corea del Sur, dan una prevalencia de primer nivel a la ENCS y el ciberespacio. Mientras otros países se encuentran en niveles semejantes a naciones de Medio Oriente y América Latina. Por último, se señala que la región de África parece ser la menos aventajada en la construcción de una ENCS y la más alejada del entorno global de ciberseguridad. Sin embargo, se destaca que esta región del mundo es dónde la penetración del internet avanza más rápidamente, por lo que se deduce que en los próximos años los temas de ciberseguridad tomaran una relevancia vital en la región.

2.6.2 Ciberseguridad y ciber amenazas: la comprensión de los actores no estatales organizados o privados

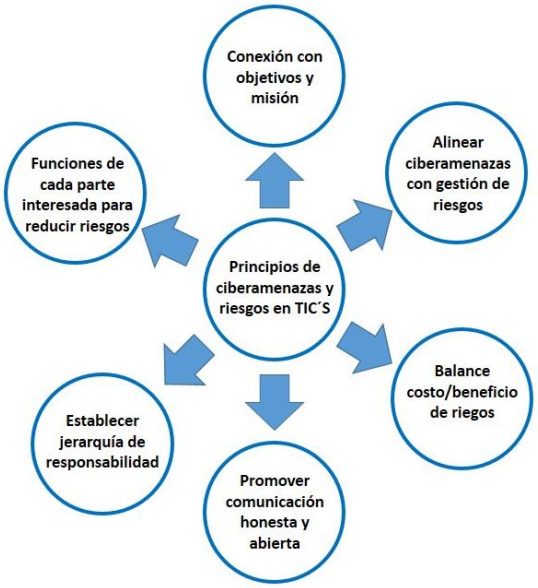
Si bien la presente investigación se centra en la comprensión de la ciberseguridad desde el Estado-Nación, un enfoque integral de seguridad exige abordar la comprensión de las ciber amenazas desde los actores no estatales organizados y privados. En ese sentido, se destaca que cuando se presentó la definición de las partes interesadas de Klimburg y Healey (2012), en el capítulo anterior, se hizo un señalamiento de que este conjunto de actores son vitales para la construcción de ciber capacidades y la gobernanza del ciberespacio, a la par de que se resaltó su capacidad de reacción más ágil frente a riesgos cibernéticos, que los Estados-Nación, como lo son las empresas de software (Microsoft, Linux, etc.), empresas de seguridad (McAffer, Norton), empresas de telecomunicaciones (At&T, Vodafone), o instituciones certificadoras en temas de ciberseguridad y seguridad informática (NIST, ISO, CBEST, etc.). En ese sentido, es importante mencionar que la ciberseguridad para los actores estatales no organizados se aborda desde la visión de cómo un ataque a una organización afecta a esta, por lo cual se construyen y utilizan metodologías de análisis y medición de riesgos e impacto (Bodeau, McCollum, & Fox, 2018). El grado de afectación a una organización causado por una ciber amenaza se puede abordar desde dos perspectivas: 1) el daño que se causa a la confidencialidad, integridad y disponibilidad de la información o sistemas informáticos, a través de divulgación no autorizada, mal uso, alteración o destrucción de sistemas de información. Y, 2) las circunstancias y eventos con el potencial de impactar negativamente en operaciones organizacionales –en aspectos como su misión, funciones, imagen o reputación-, activos e individuos de la organización, a través del acceso no autorizado, destrucción, divulgación y denegación de servicios (Wang, & Johnson, 2018).

Este conjunto de actores entiende por organización empresas, firmas, gobiernos, institutos de investigación científica, o entidades proveedoras de servicios de cualquier tipo, etc., que dispongan de tecnologías de la información o el ciberespacio para poder llevar a cabo sus operaciones organizacionales. Asimismo, metodologías como operaciones de seguridad y análisis, gestión de riesgos, manejo de responsabilidad de incidentes, son pilares en la comprensión de la ciberseguridad de múltiples agencias encargadas de diseñar certificaciones o procedimientos de prevención de ciber incidentes y seguridad informática. Del mismo modo, al ser métricas centradas en actores privados, las diferentes agencias certificadoras

utilizan variables en términos económicos para medir el impacto dentro de las organizaciones en un nivel de pérdidas monetarias que estas sufren. Un aspecto a señalar es que los actores estales no organizados son instituciones que se encuentran a la vanguardia de la utilización de TIC´s y OT´s, en diferentes aplicaciones: tales como la Inteligencia Artificial (IA), Internet de las Cosas (*Internet of Things* o IoT), *Big Data* o *blockchain,* en aplicaciones de la vida diaria de las personas, gobierno y actividades económicas.

De acuerdo a la ISACA (2009) existen seis principios para la comprensión de ciber amenazas y riesgos de las tecnologías de la información, los cuales se muestran en la figura 15. Cada uno de estos principios sirven para identificar los objetivos de la organización y calibrar el nivel de impacto que puede tener un incidente cibernético dentro de los procesos de la misma, crear protocolos de disuasión y resiliencia frente a estos, delimitar las funciones, niveles de jerarquía ante cada ciber amenaza, así como promover una comunicación honesta y abierta hacia dentro y fuera de la organización, aun cuando se esté enfrentando a una ciber amenaza.

Figura 15. Principios de ciberamenazas y riesgos en TIC´s.



Fuente: ISACA (2009)

Con base en estos principios, múltiples agencias certificadoras aplican metodologías en temas ciberseguridad, tales como NIST, CCRS, PRE-ATT&CK™, STIX™, etc. En este apartado destacamos tres de los modelos más utilizados.

I. *Operaciones de seguridad y análisis.* este enfoque utiliza un modelado de ciber amenazas centradas en las actividades de agencias o instituciones encargadas de la ciberseguridad de una organización. Se delimitan tareas y acciones como la caza de amenazas, que implican la creación de indicadores o evidencia de actividades de agresores, monitoreo continuo y evaluación de seguridad, rápido desarrollo y despliegue operativo de herramientas de defensa sobre tipos específicos de amenazas o eventos.

II. *Gestión de riesgos*: representa un modelado de ciber amenazas centradas en el análisis y la elaboración de riesgos cibernéticos. Así como su posterior evaluación, creación de respuestas alternativas –individuales o en el nivel de responsabilidad y jerarquía de las partes interesadas-, que son componentes del riesgo de la organización.

III. *Manejo de incidentes y responsabilidad de crisis*: supone el analizar los datos relacionados con un ciber incidente y decidir la respuesta adecuada a éste para minimizar el impacto, incluyendo estrategias de comunicación de información relacionada sobre el mismo con partes internas y externas como clientes, partes interesadas, organizaciones asociadas y con el público en general (NIST, 2012).

Las tres metodologías citadas anteriormente, permiten crear protocolos de atención de ciber amenazas y riesgos, ya que definen el impacto de las ciber amenazas e incidentes en una organización, las responsabilidades de las partes interesadas, las acciones a ejecutar ante una crisis y el manejo de comunicación interna y externa que es deseable utilizar en casos de ser víctima de un ciber ataque, así como el promover un enfoque de análisis que tienen la finalidad de crear capacidades de resiliencia y disuasión. En los hechos, estos enfoques han sido utilizados para abordar estudios de caso de trascendencia en que las ciberamenazas han tenido algún impacto en empresas o entidades que han visto vulnerada su seguridad informática, tales como la brecha de información o daños de operación de empresas Equifax, Cambridge Analytica, Chrysler, e incluso en casos de análisis infraestructura nacional crítica, como redes inteligentes de energía, o suministro de agua. En este sentido, se presentan en la tabla 8 algunas metodologías utilizadas por agencias certificadoras de ciberseguridad en cada una de las tres categorías citadas anteriormente.

Tabla 8. Metodologías utilizadas por agencias certificadoras de ciberseguridad.

Metodología	Técnicas	Breve descripción
Operaciones de seguridad y análisis.	**PRE-ATT&CK™** (*Adversarial Tactics, Techniques & Common Knowledge*)	Marco para categorizar y caracterizar actividades de adversarios de la organización en las primeras etapas del ciclo de vida de un ciber ataque (MITRE, 2016). Posee 17 categorías de tácticas de alto nivel definidas para cubrir ciber amenazas técnicas externas a la empresa.
	Cyber Threat Framework (ODNI ,2017)	Enfoque para caracterizar y clasificar riesgos y ciber amenazas. También respalda el análisis, toma de decisiones de alto nivel y el análisis de tendencias y brechas de información. Define cuatro etapas de acciones contra ciber amenazas: preparación, compromiso, presencia y efecto- consecuencia.
	Risk Standards Initiative (OMG, 2014).	Representa una iniciativa de *The Object Management Group* (OMG) para homologar una serie de términos relacionados con modelado de ciberamenazas, incluyendo amenazas, fuente de amenazas, actores de amenazas, eventos no deseados, tácticas, técnicas, procedimientos, explotar objetivo, objetivo y campaña. Para crear un marco estandarizado que sirva a instituciones certificadores en ciberseguridad.
	STIX™ (Structured Threat Information eXpression) (Barnum, 2014)	Es un lenguaje estructurado para capturar y compartir información sobre amenazas cibernéticas. STIX permite compartir información sobre amenazas cibernéticas y sobre cursos de acción que pueden defenderse de las actividades de estas. También, permite definir estructuras de datos para caracterizar o describir a un adversario y sus actividades, con clasificaciones como *actor de amenazas*, *malware de herramientas*, *patrón de ataque*, etc.

Metodología	Técnicas	Breve descripción
Gestión de riesgos	**NIST Framework for Improving Critical Infrastructure Cyber security** (NIST, 2012)	Define un enfoque de alto nivel para la gestión de riesgos, para complementar los programas de ciberseguridad y los procesos de gestión de riesgos de las organizaciones en sectores vitales de infraestructura crítica. El enfoque no define términos de modelado de amenazas cibernéticas, pero usa los siguientes términos: *amenazas de ciberseguridad*, *exposición a amenazas*, *entorno de amenazas*, *amenazas en evolución y sofisticadas*, e *inteligencia de amenazas cibernéticas*.
	CBEST Intelligence-Led Cyber Threat Modelling (Bank of England, 2016)	El enfoque es un subcomponente del marco para evaluaciones en inteligencia de amenazas cibernéticas, publicado por el Banco de Inglaterra. Describe un modelo analítico de actores de ciber amenazas en términos de sus objetivos, capacidades utilizadas para perseguir estos objetivos, métodos y patrones de operación. El modelo es destinado a actuar como una plantilla para realizar una evaluación de amenazas cibernéticas para definir un conjunto de escenarios realistas de prueba, basados en amenazas.
	COBIT 5 and Risk IT (Control Objectives for Information and Related Technologies) (ISACA, 2014)	Es un modelo de riesgo que se empata con un modelo de proceso; los procesos se definen para los dominios de la gobernanza de los ciber riesgos, la evaluación del riesgo y la respuesta a estos. Considera escenarios de riesgo que se describen en términos de tipo de amenaza este incluye: *datos maliciosos*, *actor*, t*ipo de impacto*, *recurso activo o afectado* y *tiempo*.
Manejo de incidentes y	**Manejo Estratégico de Crisis**	Modelo diseñado por la OCDE para los nuevos retos de las amenazas de los países miembros de este organismo, que pueden extenderse más allá de las fronteras nacionales y pueden crear

Metodología	Técnicas	Breve descripción
responsabilidad de crisis	(OCDE, 2013)	efectos económicos significativos. Considera a las ciber amenazas o ciber ataques como choques del futuro, y como detonadores de crisis en todas las esferas sociales en tiempo cercano. .

Fuente: Elaboración propia.

2.7 Disuasión, resiliencia y construcción de ciber capacidades del Estado-Nación

2.7.1 Disuasión y resiliencia un marco inicial

Nuestro análisis en torno a la ciberseguridad y sus vínculos con la seguridad nacional y la soberanía cierra con la comprensión de los términos de resiliencia y disuasión en el ciberespacio, así como en la construcción de ciber capacidades por parte de los Estados-Nación. Por resiliencia, en su noción clásica, se entiende a la capacidad de previsión, reconocimiento y anticipación de defensa, de un sistema y organización, para defenderse frente a una forma de riesgo cambiante, antes de que este tenga consecuencias o costos adversos (Haimes, 2006).

En ese sentido, se entiende que la resiliencia supone un conjunto de capacidades, acciones y protocolos que desarrolla una entidad, que se enfrenta a riesgos y amenazas constantes, que sabe que estos evolucionan y se transforman, por lo cual las capacidades de defensa deben estar en constante actualización.De igual manera, Wood (2006) la define como una respuesta adaptiva para evitar posibles pérdidas que son el resultado de identificar las amenazas constantes a una entidad, sobre las cuales se mide el grado de impacto que pueden tener cada una de ellas, así como las acciones a ejecutar para revertir el daño y recuperarse rápidamente de ellas. La definición anterior, presenta un nexo directo entre las vulnerabilidades y amenazas, dado que las primeras son los puntos endebles de una entidad o sistema, que pueden permitir la materialización del impacto de una agresión.

Por su parte, la disuasión es un concepto que surge en la política de defensa y seguridad nacional de los Estados Unidos de América, en el marco de la Guerra Fría, dado el surgimiento de un competidor cercano capaz de obstruir o alcanzar los intereses de esta nación, en este caso la Unión Soviética (Haffa Jr., 2018). El principal autor que aborda y

construye una definición de manera amplia de este concepto fue John Mearsheimer, desde la óptica del neorrealismo, en su obra *Conventional Deterrence.* En ella Mearsheimer (1985) define a la *disuasión convencional* como todas las acciones que ejecuta un Estado-Nación para persuadir a un adversario de no iniciar una acción en su contra, a razón que los costos a recibir superan los beneficios que pueden obtenerse. En ese sentido, la disuasión se define como una función clásica de la estrategia militar. Asimismo, diversos autores añaden diferentes características al concepto, entre los que destacan que es un instrumento del poder militar que se utiliza para poder influir en otros, así como un medio a través del cual pueden evitarse guerras y conflictos de altos costos.

La disuasión convencional tuvo un gran alcance como instrumento previsor de conflictos directos entre la Unión Soviética y Estados Unidos en el marco de la confrontación nuclear. Frente a esto, Quackenbush (2011) considera que la *disuasión nuclear* marcó el fin de las guerras tradicionales según la visión de Clausewitz, en que dos Estados, con capacidades semejantes de poder militar, evitaron el conflicto por los altos costos que estas podían alcanzar y marcaron una nueva forma de confrontaciones indirectas que redujeron este tipo de choques. También, se expresa que el desarrollo de metodologías innovadoras adaptadas al estudio de los conflictos como la *Teoría de Juegos*, durante la segunda mitad del siglo XX, y el desarrollo de la informática permitió que aplicaciones de disuasión convencional y nuclear se adaptaran a instrumentos como los *juegos de guerra*, que empezaron a ser de amplio uso desde los años sesenta por las fuerzas armadas de diferentes países.

Según Betts (2013) la disuasión convencional se integra de tres componentes, que son:

- *Capacidad*: consiste en la posibilidad de despliegue de fuerzas militares con los instrumentos, medios y poder de defensa suficiente en caso de sufrir una agresión o amenaza por parte de un enemigo. Lo que implica la viabilidad de ejecutar represalias en caso de una acción inaceptable en contra la seguridad nacional, soberanía e intereses de un Estado-Nación.
- *Credibilidad:* es la intención declarada y resolución creíble de proteger un interés, la cual se refuerza por la acción y capacidad de proyección de un Estado-Nación que se asume como potencia.

- *Comunicación:* implica transmitir al potencial o potenciales agresores, de manera inconfundible y concreta, la capacidad y la voluntad de que existirán represalias en caso de una amenaza que afecte la seguridad nacional e intereses del Estado.

Por su parte Haffa Jr. (2018) añade tres componentes más para que una estrategia de disuasión sea efectiva, que son:

- *Visibilidad de la fuerza militar:* consiste en el despliegue de fuerzas armadas a nivel nacional e internacional, así como la demostración de sus capacidades reales de combare y acción. Es importante mencionar que este autor señala que en el siglo XXI se requiere tener una presencia física y virtual de las capacidades de defensa del Estado-Nación.
- *Voluntad de usar la fuerza:* corresponde al grado de compromiso y convicción de utilizar la fuerza en caso de que un adversario ejecute una amenaza o acción en contra de la soberanía o seguridad nacional. En ese sentido, se destaca que fallas en la determinación del Estado-Nación de utilizar la fuerza frente a sus agresores pueden minar la capacidad de disuasión de un país frente a sus adversarios y dañar su credibilidad. Por otra parte, el ejecutar acciones con determinación que demuestren las consecuencias que puede tener una amenaza contra el Estado, y crear un historial de qué efectos puede tener una agresión, y reducir el nivel de intención de los adversarios de materializar agresiones.
- *Racionalidad del uso de la fuerza:* los Estados-Nación deben de utilizar un uso medido y moderado de la fuerza. Por lo cual, al ejecutar acciones de represalia contra un agresor, el Estado debe responder frente a las acciones que vulneraron la seguridad nacional, más no debe hacerlo en un nivel que el grado de afectación que ejecute frente a su oponente, deriven en un conflicto de escala mayor.

En referencia a lo anterior, se expresa que la resiliencia corresponde a una capacidad adaptativa para enfrentar riesgos y amenazas, que tiene como fin la mejora y constante actualización de las capacidades de defensa, en contra de amenazas constantes y evolución. La cual es una característica que se ajusta a múltiples tipos de organizaciones como empresas y gobiernos. Mientras que la disuasión es un concepto surgido en los estudios de defensa y seguridad nacional, además de ser una táctica de la estrategia militar. La cual busca que, a

través del reconocimiento de las capacidades de reacción y defensa, los adversarios eviten ejecutar acciones en contra de un Estado-Nación, derivado del nivel de represalias que pueden ser mayores a los beneficios a obtener.

2.7.2 Resiliencia y disuasión en el ciberespacio

El uso del ciberespacio en múltiples esferas de la vida cotidiana de los individuos, actores no estatales y Estados-Nación, han hecho a la ciber defensa, directamente vinculada con el desarrollo de resiliencia y la disuasión, un aspecto clave para garantizar el desarrollo de capacidades de ciberseguridad. De acuerdo con Chase & Chan (2016) la importancia de las redes informáticas, TIC´s, TO´s, así como el alcance de las dinámicas de riesgo en la sociedad derivadas de un ciber incidente, han cimentado la necesidad de los Estados, con pretensiones de consolidar su presencia en este campo, de avanzar en el desarrollo de estas dos estrategias de acción y reacción que les permitan alcanzar una superioridad en este dominio de la política internacional.

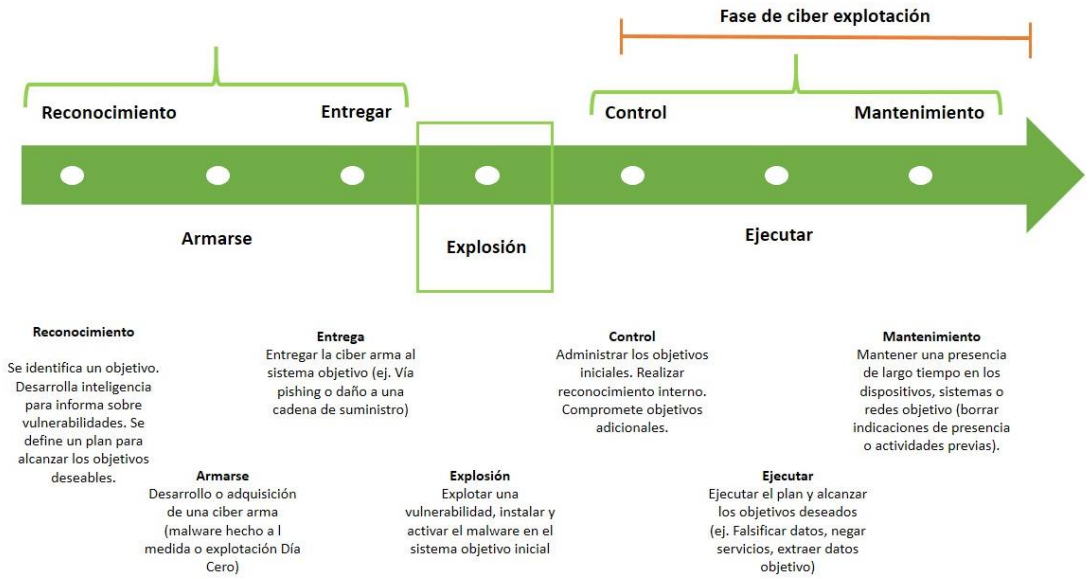
En los hechos, las estrategias de seguridad nacional o libro blanco de países de la OTAN y regiones del resto del mundo han contemplado los dos esquemas desde el inicio de la era de las amenazas no convencionales en los estudios de seguridad internacional. Por su parte, el avance de las tecnologías y la comprensión de los riesgos cambiantes, han reforzado más que nunca la identificación de vulnerabilidades y la comprensión de riesgos que pueden provenir un ciberataque.

Como se indicó en una sección pasada, los países de la OTAN han sido el conjunto de naciones que más avanzado en la evolución sus ENCS y en la utilización de metodologías y métricas que permiten consolidar las capacidades de resiliencia y disuasión. Asimismo, la evolución de una ENCS de una segunda a tercera visión de ciberseguridad, consecuentemente, muestra la capacidad de evolución y adaptabilidad del Estado-Nación, en este dominio estratégico para el poder nacional.

Para comprender las nociones de disuasión y resiliencia en el ciberespacio, autores como Bodeau, McCollum y Fox (2018) expresan que es necesario comprender el ciclo de vida de

un ciber ataque o incidente. En ese sentido, en la figura 16 se presenta las siete etapas que contemplan el desarrollo de un ataque cibernético.

Figura 16. Ciclo de vida de un ciberataque.



Fuente: Bodeau, McCollum y Fox (2018)

El ataque puede ser dividido en dos periodos, una fase previa –que contempla el reconocimiento, armarse y entrega del malware o ciber arma-, para posteriormente pasar a un punto de explosión, en dónde se determina si la agresión tiene éxito o no en vulnerar el sistema objetivo. También, se destaca que la primera fase contempla principalmente al actor agresor, que desarrolla un análisis de las vulnerabilidades de los sistemas informáticos, a la par de hacer una medición de las capacidades de disuasión de su adversario. En este punto, el ciber agresor determina las vías de entrada y niveles de consecuencias, que puedan afectarlo, por una respuesta en represalia por vulnerar los sistemas objetivo de su adversario.

Posteriormente, la fase de medición y efectividad de los niveles y capacidades de ciberseguridad de un Estado-Nación se da posteriormente en la etapa de explosión. Ya que si el Estado-Nación objetivo de la agresión tiene bien consolidadas sus capacidades de defensa y ha construido una efigie de disuasión frente a sus oponentes, éstos desistirán y no alcanzarán dicha etapa. Sin embargo, si los oponentes han detectado que existe un gran nivel de éxito de la planeación del ciber ataque y se logra vulnerar el sistema del Estado objetivo, la entrada en acción de las capacidades de resiliencia será vital para neutralizar y eliminar la

ciber amenaza. De esta forma, inicia la segunda fase del ciclo de vida de un ciber ataque, a la cual podemos denominar *fase de ciber explotación,* y se compone de los niveles de control, ejecución y mantenimiento. La etapa de control implica que el malware o ciber arma se ha introducido con éxito a los sistemas informáticos y ha empezado una etapa de reconocimiento interno basada en inteligencia, para ampliar su noción sobre las vulnerabilidades del sistema objetivo. Posteriormente, viene la fase de ejecución, que se vincula en materializar y alcanzar los objetivos por los cuales fue diseñado el ataque. Por último, se encuentra el nivel más severo que es la etapa de mantenimiento, e implica una presencia de largo tiempo en los sistemas, que se traduce en una ciber explotación, principalmente para recolectar información de las ciber vulnerabilidades, e incluso más datos de los esperados, si el actor agredido no detecta en un tiempo breve la presencia de la ciber arma.

Si el ciclo de vida de una ciber amenaza está centrado en la visión del actor agresor, la *etapa de ciber explotación* tiene una vinculación más directa con la implementación de medidas de ciber defensa y son la prueba de fuego para las capacidades de resiliencia y disuasión del Estado atacado. De manera paralela, el actor agredido inicia un proceso de ciber defensa que se presenta en la figura 17, en este sentido, se expone que el aprendizaje y medición de capacidades adaptativas de los sistemas de ciber defensa ocupan las cinco fases y cuatro niveles del proceso (Bodeau, McCollum y Fox, 2018).

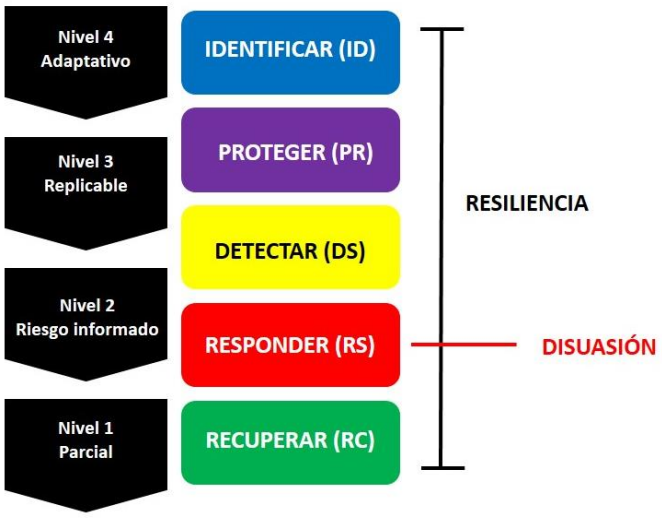
Por lo cual, la resiliencia es una capacidad que se desarrolla e implementa en cada una de sus etapas. Por otra parte, el nivel de disuasión sólo se aplica en la cuarta fase del proceso –respuesta- e implica el aplicar represalias en contra del actor agresor, para crear un precedente en el futuro de que las consecuencias fueron más altas, que los beneficios obtenidos del ciberataque. Los niveles del proceso de ciber defensa, resiliencia y disuasión representan las siguientes actividades, según Bodeau, McCollum y Fox (2018):

1. *Identificar:* el actor atacado es consciente de una irregularidad en sus sistemas, dispositivos o redes informáticas. En ese sentido, identifica dónde se encuentra la ciber arma y se inicia el proceso de defensa.
2. *Proteger:* el actor agredido protege y resguarda toda la información vulnerable o expuesta. Asimismo, hace un balance de qué tan grande fue la brecha de información

o afectaciones a los dispositivos o sistemas informáticos. A la par de que se inician tareas de recuperación en esta fase en caso de que la agresión haya sido exitosa.

3. *Detectar:* Una vez iniciados los procesos de recuperación, el actor vulnerado inicia un proceso para detectar el origen de la agresión, puede ser desde un actor estatal (gobiernos, Estados-Nación), actor no estatal organizado (empresa competidora, grupo terrorista, etc.) y no estatal no organizado (hackers o individuos solos), en este punto se tejen hipótesis sobre las motivaciones y objetivos a alcanzar por el ciber agresor y se inician los procesos de respuesta.
4. *Responder:* implica el ejecutar represalias en contra del ciber agresor para que sea consciente de que las consecuencias superaron los beneficios alcanzados derivados del ciber ataque, puede darse en un nivel entre estados, estado-actor no estatal organizado, y estado-actor no estatal no organizado.
5. *Recuperar:* Implica la recuperación total de las afectaciones de los sistemas informáticos, estos pueden darse en recuperación económica y prestigio, normalización de procesos y funciones, o reparación de los sistemas dañados. Asimismo, representa el aprendizaje sumativo del actor agredido para mejorar sus ciber capacidades y adaptación a amenazas, reducir el nivel de vulnerabilidad mediante el cual se introdujo la ciber arma a los sistemas objetivos, y la creación de precedentes de disuasión, para que en el futuro cercano los ciber agresores no alcancen la etapa de explosión, del ciclo de vida de un ciber ataque.

Figura 17. Proceso de ciber defensa, resiliencia y disuasión.



Bodeau, McCollum y Fox (2018).

2.7.3 Construcción y desarrollo de ciber capacidades

Los niveles de ciber defensa, resiliencia y disuasión de un Estado-Nación en el ciberespacio, son el reflejo del desarrollo de sus ciber capacidades. Cómo se mencionó, la ENCS forman un papel clave en el desarrollo de éstas, con base en la doctrina y estrategia de seguridad nacional, así como la importancia que ha otorgado cada nación para la construcción de ciberpoder y utilización de este dominio como un instrumento para su proyección internacional. Sin embargo, ¿cuáles son las buenas prácticas y capacidades que pueden reducir el nivel de vulnerabilidad de un país en el ciberespacio? En la actualidad existen dos métricas internacionales que evalúan la política de ciberseguridad de más de cien países a nivel global y sirven de marco para medir y evaluar el grado de compromiso de diferentes naciones del mundo con la ciberseguridad, que corresponden al *Índice Global de Ciberseguridad* (GCI por sus siglas en inglés), de la Unión Internacional de Telecomunicaciones, y el *Índice Nacional de Ciberseguridad* o (*National Cyber Security Index* o NCSI en inglés), de la la *E- Governance Academy.* Ambas métricas presentan las áreas de oportunidad y de mejora de las legislaciones nacionales de ciber crimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT), con la meta de mejorar las cibercapacidades de los múltiples países evaluados.

Respecto a la medición del *Índice Global de Ciberseguridad* se expone que dicha media es un índice compuesto, integrado por veinticinco indicadores con la finalidad de monitorear y comparar el grado de compromiso de los diferentes países del mundo con los cinco pilares de la Agenda Global de Ciberseguridad, creada por la ITU en 2007. En ese sentido, los objetivos principales de GCI son medir:

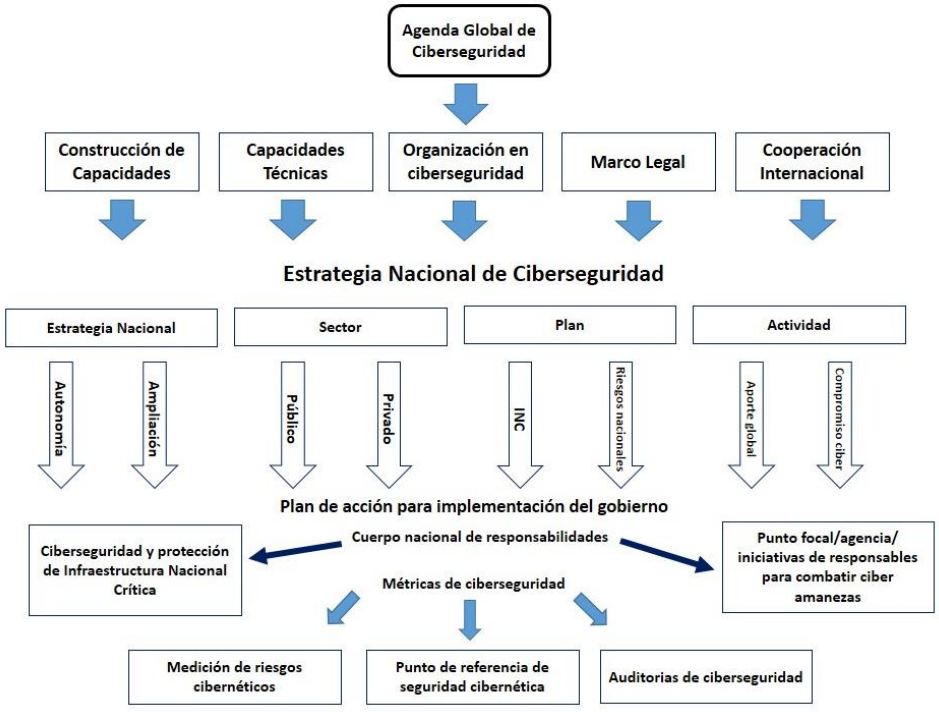
- El tipo, nivel y evolución a lo largo del tiempo del compromiso de ciberseguridad en los países miembros de la ITU.
- El progreso y seguimiento en el grado compromiso de ciberseguridad desde una perspectiva global y regional.
- La división del compromiso de seguridad cibernética o la diferencia entre países en términos de su nivel de participación en iniciativas de ciberseguridad.

La Agenda Global de Ciberseguridad de la ITU se traduce en cinco pilares que componen el GCI, a través de 25 indicadores. Asimismo, está medida tiene la finalidad de fomentar la

cooperación internacional de múltiples partes interesadas (actores estatales o actores no estatales organizados) con el objetivo construir sinergias entre las iniciativas actuales y futuras. Los cinco pilares del GCI (2019) son:

- *Marco Legal:* representa las medidas basadas en la existencia de instituciones legales y marcos jurídicos que se ocupan de la ciberseguridad y el ciber crimen.
- *Medidas Técnicas*: medidas basadas en la cantidad de instituciones técnicas encargadas de ciberseguridad y el marco de negociación entre las partes interesadas.
- *Estructura Organizacional:* medidas basadas en la existencia de instituciones y estrategias de coordinación de políticas para el desarrollo de la ciberseguridad a nivel nacional.
- *Desarrollo de capacidades:* métricas que analizan la existencia de investigación científica, educación y programas de capacitación, certificación de profesionales y agencias del sector público que fomentan el desarrollo de ciber capacidades.
- *Cooperación internacional:* representa la existencia de asociaciones, marcos cooperativos y redes de intercambio de información del gobierno con otros países.

Figura 18. Agenda Global de Ciberseguridad de la ITU (2007)



Fuente: GCI (2019)

Respecto a las buenas prácticas que se concentran en cada pilar se presentan en ela tabla 9

Tabla 9. Buenas prácticas y compromisos de la AGC.

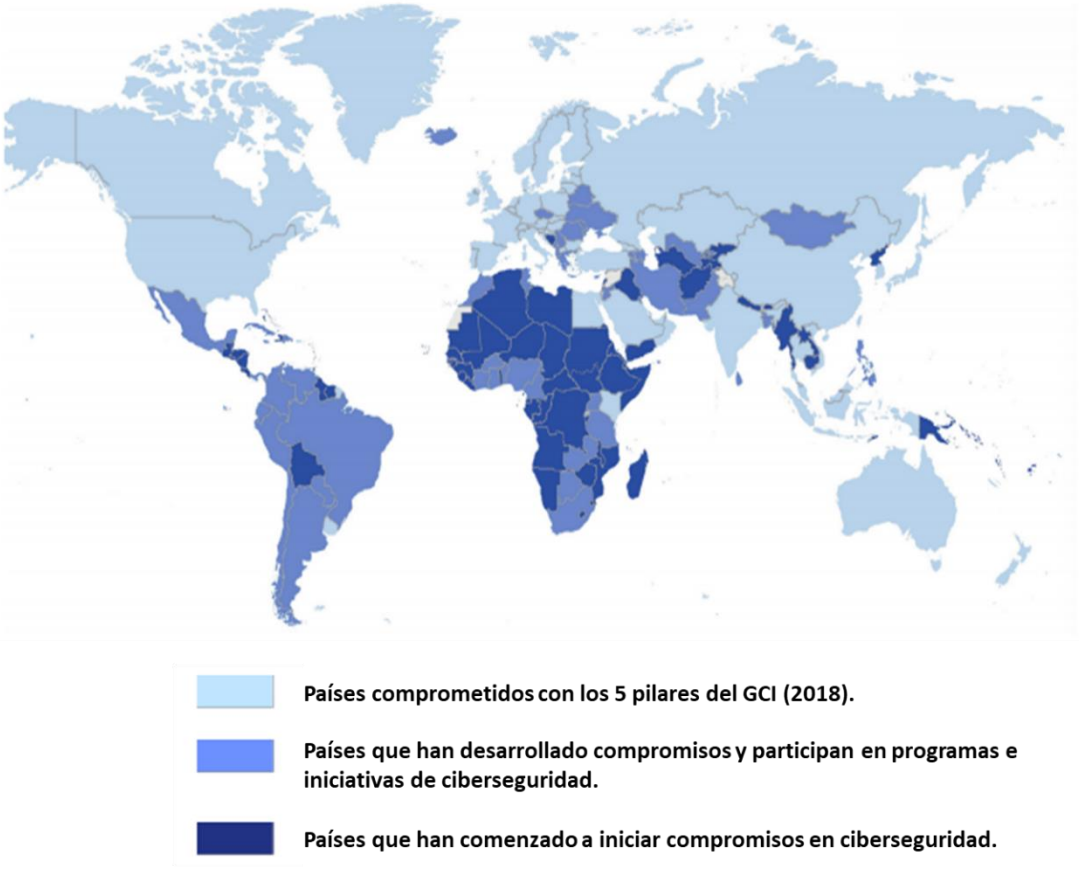
Pilar	Buenas Prácticas y compromisos
Marco Legal	i. Creación de legislación contra el ciber crimen. ii. Establecimiento de regulaciones de ciberseguridad. iii. Legislación para la contención y freno del spam.
Medidas Técnicas	i. Creación de un Equipo de Respuesta de Emergencia Informática (CERT), Equipo de Respuesta a incidentes de Seguridad Informática (CSIRT), Equipo de Respuesta a Ciber Incidente (CIRT). ii. Implementación de un marco de estandarización de procesos cibernéticos. iii. Desarrollo de mecanismos técnicos y capacidad desplegada para abordar el spam. iv. Uso de nube o servicio *cloud* con fines de ciberseguridad. v. Mecanismos de protección de niños en línea.
Estructura Organizacional	i. Creación de Estrategia Nacional de Ciberseguridad. ii. Instalación de Agencia responsable de ciberseguridad. iii. Desarrollo de métricas de ciberseguridad.
Desarrollo de capacidades	i. Campañas públicas de concientización ii. Marco de certificación y acreditación para profesionales de la ciberseguridad. iii. Cursos de entrenamiento profesional en ciberseguridad. iv. Programas de desarrollo e investigación de ciberseguridad. v. Mecanismos de incentivos.
Cooperación internacional	i. Acuerdos bilaterales y multilaterales en materia de ciber seguridad. ii. Participación en foros y asociaciones internacionales. iii. Asociación estratégica público-privada. iv. Asociación interagencial e intraagencial en ciberseguridad. v. Mejora de las prácticas a estándares globales.

Fuente: GCI (2018).

En los hechos el nivel de compromiso de los países miembros de la ITU con el GCI (2018), se mide con una puntuación que va del 0 a 1, dónde cero representa el nivel más bajo de compromiso por parte de un país, y 1 el más alto. Lo anterior se traduce en tres grupos diferentes de naciones. El primero representa a un conjunto de 54 países, que obtuvieron calificaciones que van del 0.670 al 1, por lo cual este conjunto de gobiernos muestra un alto compromiso en los cinco pilares del índice y corresponde al grupo de países El segundo corresponde a un grupo de países con puntajes medianos, que van de un valor de 0.669-0.340, y representan un total de 53 países. Este grupo de naciones se han comprometido con iniciativas internacionales de ciberseguridad y están desarrollando acciones para fortalecer

áreas vinculadas a los cinco pilares de la Agenda Global de Ciberseguridad. Sin embargo, aún necesario que alcancen un grado de madurez en sus ENCS. Por último, se encuentran los países de puntaje más bajo, que corresponden a los que obtuvieron una calificación entre los valores de 0.339-0.000, este grupo representa a un total de 87 países, y son los países menos comprometidos con la ciberseguridad a nivel internacional.

Figura 19 Grupos de países según la medición e ITU (2018).

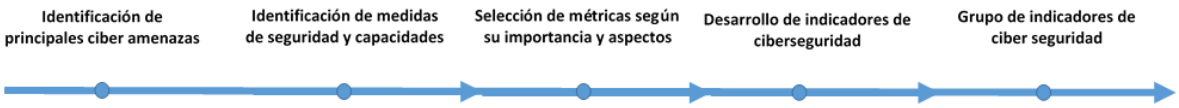


Fuente: GCI (2019).

La segunda medición a la que se hace referencia es la que corresponde al *Índice Nacional de Ciberseguridad* (NCSI, por sus en inglés), creado por la *E-Governance Academy*, esta medida, a diferencia del GCI (2018) es una métrica global que evalúa la preparación de los países para prevenir ciber amenazas y gestionar ciber incidentes. En ese sentido, se expresa que el GCI (2019) mide el grado de compromiso e importancia que los Estados-Nación han dado al tema de ciberespacio en el desarrollo de su política de seguridad y defensa nacional, así como la proyección para utilizar este dominio en el ciberespacio. Mientras que el NCSI

es un instrumento que mide sus capacidades de resiliencia, y en menor medida y de forma discreta, de disuasión, a la que se considera es una base de datos de evidencia disponibles al público y una herramienta para el desarrollo de capacidades nacionales de ciberseguridad. De esta forma, la construcción de NSCI (2018) comenzó con un diagnóstico del estado de las ciberamenazas a nivel global, así como la identificación de vulnerabilidades y las medidas de seguridad y capacidades para poder enfrentar a éstas. Posteriormente, se construyen métricas con base en la medida de las capacidades de resiliencia de los Estados que son Evaluados a través de esta métrica.

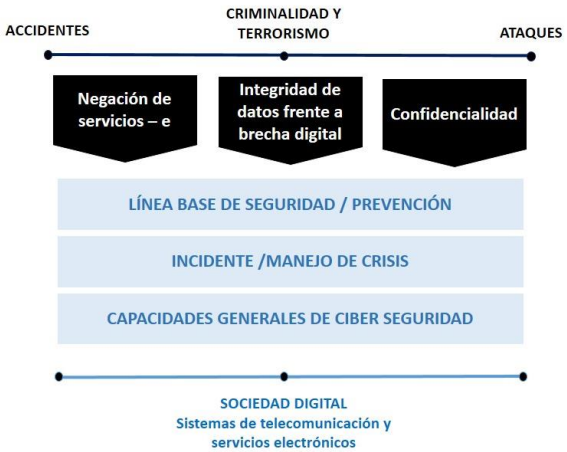
Figura 20. Proceso de desarrollo de NCSI.



Fuente: NCSI (2018).

Si bien es importante mencionar que el NCSI (2018) se empata con el GCI (2018) en aspectos como el desarrollo de marco legal, medidas técnicas, estructura internacional y cooperación internacional, posee un apartado más amplio en el desarrollo de ciber capacidades. Como se puede observar en su apartado sobre la comprensión de ciber amenazas, que posee una clasificación más amplia que en GCI (2018) y está más vinculada a analizar las capacidades de ciber defensa, resiliencia, y en consecuencia, disuasión.

Figura 21. Compresión de ciber amenazas del NCSI (2018).

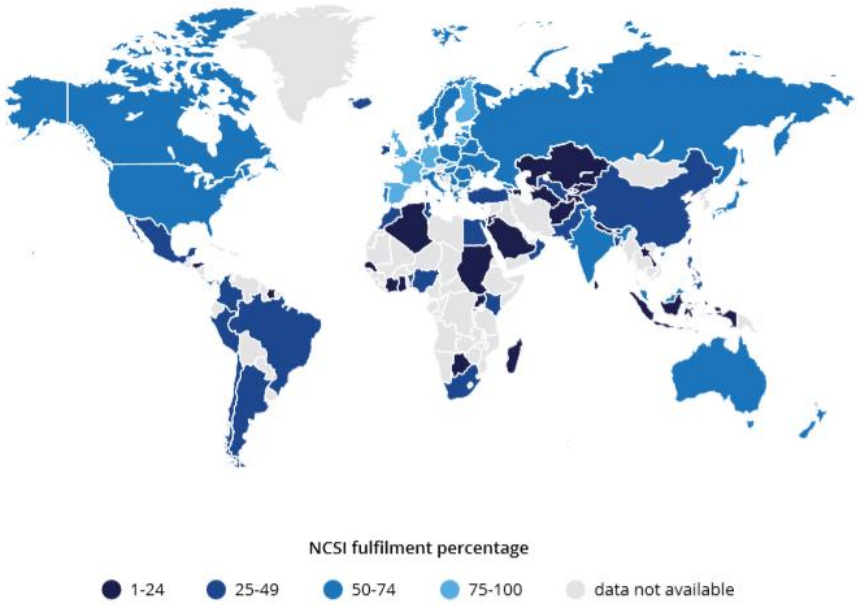


Fuente: NCSI (2018).

Por último, se destaca que la disgregación del NCSI (2018) en un total de 12 indicadores, que poseen una medición que va del 0 al 100, la cual hace más visible el nivel de capacidades de ciberdefensa de los Estados-Nación, en cada una de las variables que son:

1. *Política:* desarrollo de una ENCS y creación de legislaciones para la coordinación de temas en ciberseguridad a nivel intraagencial e interagencial.
2. *Amenazas:* análisis e información sobre ciber amanezcas y vulnerabilidades del Estado-Nación.
3. *Educación:* formación de especialistas capacitados en temas de ciber seguridad y concientización de la población sobre la importancia de la ciberseguridad.
4. *Aportación global:* avances individuales que realiza cada país para mejorar el contexto global de ciberseguridad a nivel internacional.
5. *Nivel de desarrollo digital:* grado de desarrollo y capacidades de protección de los servicios digitales.
6. *Protección de servicios esenciales:* garantía del Estado para proteger servicios esenciales como INC, redes inteligentes de energía, cadenas de suministro de bienes esenciales, etc.
7. *Identificación electrónica y confidencialidad de servicios:* grado de desarrollo y seguridad de servicios electrónicos en la vida diaria.
8. *Protección de datos personales:* seguridad de los datos de personas, empresa, etc., y garantía de su privacidad.
9. *Respuesta a ciber incidentes:* capacidades del Estado-Nación y de los equipos de emergencia informática (CSIRT, CIRT) ante u ciber incidente.
10. *Administración de ciber crisis:* capacidad de resolución de una crisis informática por parte del CERT, y las partes interesadas en la ciberseguridad del Estado-Nación.
11. *Política de lucha contra el crimen:* Grado de compromiso del Estado para luchar contra delitos realizados a través del ciberespacio.
12. *Capacidad de operaciones militares:* capacidad de las fuerzas armadas para efectuar ciber operaciones (NCSI, 2018).

Figura 22. NCSI calificación por porcentaje en el mundo.



Fuente: NCSI (2018).

Por eso se expresa que el NCSI (2018) divide en cuatro cuartiles la evaluación global del índice compuesto, que va del 0 a 100, dónde cero es el nivel mínimo de capacidades de ciber defensa y el 100 el máximo. De esa forma, dicha medida identifica sólo a nueve países con altas capacidades de ciberseguridad –con una evaluación que va del 75 al 100-, 30 países con capacidades intermedias, -con evaluación del 50 al 75-, treinta cuatro con capacidades bajas, -de evaluación del 25 al 50-, y 25 con capacidades nulas de defensa en el dominio del ciber espacio, -con evaluación del 0 al 25.

Capítulo 3. Ciberseguridad: nexos entre la soberanía y política exterior

Introducción

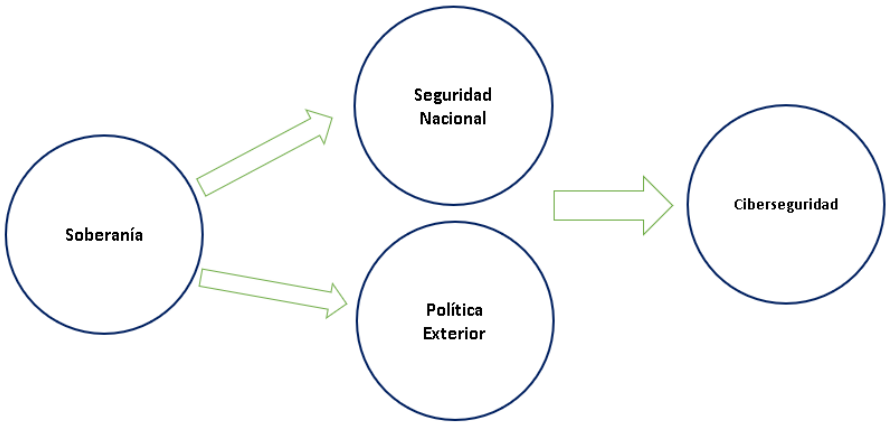
En el capítulo número dos de esa investigación se abordaron los nexos entre los conceptos de soberanía, seguridad nacional y ciberseguridad. Dicha discusión se orientó con el fin de sustentar la hipótesis principal de esta investigación, centrada en definir al ciberespacio como una nueva arena de la política internacional en la que es posible vulnerar la soberanía de los Estado-Nación, a través de la ciber explotación de sus sistemas o elementos vinculados a sistemas de Tecnologías de la información (TIC´s) o por la afectación a sus sistemas de Tecnologías de la Operación (TO´s).

No obstante, en dicha discusión sólo se abordaron los elementos del Estado-Nación que pueden ser vulnerados a través del dominio del ciberespacio, a través de una revisión del proceso de securitización que sufrió el internet en la década de los noventa, del siglo XX, para pasar por la creación de legislaciones, instituciones y Estrategias Nacionales de Ciberseguridad, en las dos primeras décadas del siglo XXI. Estos han transformado a los riesgos y amenazas provenientes del ciberespacio como una preocupación central de la política de seguridad nacional de gran cantidad de los países del mundo. Los cuales se ven reflejados en elementos como la creación de la Agenda Global de Ciberseguridad y el GCI (2018) de la Unión Internacional de Telecomunicación y métricas como la del NCSI (2018) de la *E-Governance Academy.*

No obstante, nuestro análisis del ciberespacio como nueva arena de confrontación y poder de la política internacional no está completo si no se ve la cara opuesta de este fenómeno. Es decir, comprender y abordar al ciberespacio como un campo para refrendar la soberanía de los Estados-Nación. Y entenderlo como un instrumento y medio a través del cual los países persiguen sus intereses particulares o lo que en realismo político y neorrealismo definen como el *interés nacional.* Dado que si bien se entiende a la perfección que en el contexto de

las amenazas cambiantes y la revolución digital que la inmersión del internet detonó en un contexto global complejo de riesgos y amenazas, debemos aceptar que para una gran cantidad de países, empresas privadas e instituciones, el ciberespacio supuso un campo de acción y oportunidad a través del cual podían alcanzar sus metas e intereses particulares, mejorar su posición en la configuración de la geopolítica global y mantener su grado de autonomía soberana en el concierto del poder global, a razón del nivel de desarrollo en ciber capacidades alcanzado por su gobierno y partes interesadas. En ese sentido, nos referimos a la *Figura 6. Vínculo entre la soberanía, seguridad nacional y ciberseguridad* del capítulo anterior, para completar nuestro modelo de análisis en la nueva figura 23.

. Figura 23. Vínculo entre soberanía, seguridad nacional, política exterior y ciberseguridad.



Fuente: Elaboración propia.

De esa forma, el objetivo del presente capítulo de investigación es rastrear los nexos del concepto de soberanía con la idea del interés nacional, así como de expresar como el interés nacional de los Estado-Nación posee un carácter delimitador de las acciones y estrategias de política exterior que persiguen los países de alrededor del mundo en este dominio. En lo que el ciberespacio es un nuevo campo de oportunidad y acción en el que una gran cantidad de actores de la sociedad internacional han utilizado sus características y potencial para alcanzar sus intereses particulares, mejorar su posición estratégica global, así como salvaguardar la integridad de su autonomía y capacidad de decisión soberana en la política internacional. En ese sentido, en la primera sección de este análisis se presenta una discusión en torno al

concepto de interés nacional y como este está estrechamente vinculado a las categorías de soberanía, política exterior e internacional, en las vertientes teóricas del paradigma realista, liberalista, Teoría de la Guerra y el constructivismo. En la segunda sección se analizan los métodos y estrategias para garantizar el interés nacional según el paradigma del realismo político. Posteriormente se presenta como estos elementos sirven para que los Estados-Nación delimiten una estrategia para la ejecución de su política exterior. Y en este sentido, se presentan los vínculos entre política exterior, ciberseguridad y soberanía.

Con este debate cubierto, se presentan el papel que ocupa la ciberseguridad en la política exterior de los Estados Nación, y esto como se ve reflejado a través de metodologías señaladas en el capítulo anterior como el GCI (2019) y NCSI (2018), que sirven para presentar como las naciones se agrupan al multilateralismo y cooperación para perseguir objetivos comunes. Posteriormente, y en contraposición, se presenta la metodología del *National Cyberpower Index* (NCPI) del Belfer Center de la John Kennedy School, que es una métrica más cercana a una concepción realista del ciber poder, que presenta a las naciones que son consideradas potencias del ciberespacio a través de siete diferentes dimensiones y persiguen sus intereses particulares a través de este dominio. Esta discusión sirve para presentar las capacidades de ofensa y defensa de un Estado-Nación, entre los que destacan los treinta países analizados en el NCPI, mientras, que posteriormente se presenta un análisis de los ciber comandos conocidos bajo la etiqueta de Amenaza Persistente Avanzada (*Advanced Persistent Threat,* conocidas bajo el acrónimo de APT), fuertemente analizadas por la firma de ciberseguridad FireEye, que nos presentan otra visión sobre las ciber operaciones y ciber poder de actores como China, Rusia, Irán, Corea del Norte y Vietnam.

3.1 Interés nacional y sus vínculos con la soberanía, política exterior y seguridad nacional

En el análisis de la política internacional y en el núcleo teórico de las relaciones internacionales el *interés nacional* es una categoría clave nacida en el paradigma del realismo político. Presentado por primera vez en la obra *Política Entre las Naciones* de Hans Morgenthau, el concepto es utilizado contantemente para referirse al actuar internacional y el manejo de la política exterior. Sin embargo, hasta el día de hoy esta categoría está sujeta a una gran ambigüedad y controversia, dado que el interés nacional se define como una

abstracción y un concepto dinámico y en evolución. El cual se edifica con base a la identidad, valores, ideología política y nivel de jerarquía y poder que ocupan los Estados-Nación en la sociedad internacional, con lo cual también es definido como una categoría intersubjetiva.

En su primera versión, Morgenthau (2008, p. 14) expresó que el fin del interés nacional es: [la] *supervivencia: la protección de la identidad física, política y cultural contra las usurpaciones de otros Estados-Nación*" con lo cual el máximo exponente del realismo político establece que la conducción y el actuar de la política exterior de las naciones está estrechamente vinculada a salvaguardar su existencia como país, asunto que también es un eje vital de la doctrina de seguridad nacional. Dicha definición es complementada por nociones como las establecida por Vernon Van Dyke que expresa que el interés nacional representa todo lo que los países buscan proteger o lograr en relación con sus semejantes, con lo cual se expande la noción del término a la búsqueda de objetivos o metas estratégicas que son vitales para la estructuración y conducción de la política exterior (Navari, 2018; Yanakiev, 2019). En ese sentido, podemos expresar que el interés nacional representa la delimitación de metas, estrategias y acciones, así como su puesta en marcha, que un Estado-Nación busca alcanzar y realizar en sus relaciones internacionales con otras naciones.

Morgenthau (2008) establece que el interés nacional puede subdividirse en dos diferentes clasificaciones, las cuales son: 1) componentes vitales o necesarios y 2) componentes no vitales y variables. Respecto a la primera clasificación, expresa que la finalidad de la política exterior de una nación es asegurar su supervivencia y preservar su identidad y valores a lo largo del tiempo. Por lo cual esta clasificación se subdivide en tres diferentes partes: i) la identidad física, vinculada a la integridad territorial del Estado-Nación y la protección de su población, ii) la identidad política, relacionada con los valores, principios y el modelo político (democracia, presidencialismo, parlamentarios, socialismo, etc.) que definen a cada país como actor internacional, y iii) la identidad cultural, que está estrechamente relacionada con los usos costumbres, hábitos y tradiciones de un país. Por otra parte, es importante destacar que esta noción también está relacionada a la seguridad nacional en los tiempos de guerra y paz, dado que los países deciden entrar en conflicto con otros, o incluso ir a la guerra, con la finalidad de garantizar su sobrevivencia o alcanzar una posición más estratégica en el sistema internacional.

En relación con los componentes no vitales o variables del interés nacional, se expresa que estos son determinados por el contexto histórico, regional o internacional que atraviesan las naciones. Asimismo, su estructuración y realización deben de adherirse a la necesidad de asegurar los componentes vitales. De esa forma, son de crucial importancia en este conjunto de componentes los líderes y jefes de Estado de los países, los responsables de la toma de decisiones como ministros, legisladores, los partidos políticos, la opinión pública y el debate ciudadano. Estos objetivos han sido enumerados por Vernon Van Dyke (1962) en su obra clásica *Valores e Intereses* y su lista incluye: prosperidad, paz, ideología, justicia, prestigio, engrandecimiento y poder.

Aunque cada Estado-Nación define estos objetivos de una manera que se adapta a sus intereses en circunstancias cambiantes. Por otra parte, Robinson (1995) creó una clasificación alternativa de seis tipos de intereses que los Estados-Nación buscan garantizar en su política exterior, los cuales son:

- *Intereses principales:* representan los intereses que un Estado tiene que defender a toda costa, entre ellos se incluyen la preservación de la identidad física, política y cultural contra agresiones de otros estados.
- *Intereses secundarios:* vinculados a la protección de los connacionales en el extranjero, así como garantizar las inmunidades de las misiones diplomáticas y su personal.
- *Intereses permanentes:* supone las metas y objetivos de los Estados en el largo plazo, los cuales están sujetos a cambios muy lentos, y por lo tanto, pueden requerir de largos periodos de tiempo y una continuidad de los gobiernos y líderes políticos para ser alcanzados.
- *Intereses variables:* relacionados con los intereses de un país en un determinado momento histórico y se consideran vitales para el bien nacional en determinadas circunstancias, los cuales están marcados por personalidades políticas, la opinión pública, intereses sectoriales, política partidista y costumbres políticas y morales.
- *Intereses generales:* metas y objetivos que se refieren a condiciones positivas tanto para los países, como para el contexto internacional (entre ellos se encuentran la paz internacional, la solución de conflictos, el desarme y el control de armamentos, la

estabilidad económica nacional, regional y global, las relaciones diplomáticas y la promoción del comercio como instrumento para la prosperidad), y los;

- *Intereses específicos:* que son una consecuencia de los intereses generales y se definen en términos de tiempo y espacio un Estado o conjunto de actores internacionales. Por ejemplo, promover y consolidar el paneuropeísmo, para las naciones de la Unión Europea, la lucha contra el terrorismo, a inicios del siglo XX por los países de la OTAN, o abogar por un mundo multipolar, para las naciones integrantes de los BRICS.

Por último, es importante destacar que Robinson (1995) expresa que el interés nacional de los Estados-Nación interactúa y se confronta con tres formas de intereses internacionales, los cuales son:

- *Intereses idénticos*: categoría que se refiere a aquellos que se comparten con un gran número de Estados (paz, prosperidad internacional, gobernanza global) y normalmente son promovidos por la noción histórica y contemporánea de la ética y justicia internacional, que usualmente son causas y banderas de acción de organismos internacionales y regionales como la ONU y la OEA.
- *Intereses complementarios*, categoría que representa los intereses que, aunque no son idénticos o compartidos por diferentes Estados-Nación, constituyen la base de un acuerdo multilateral o bilateral sobre cuestiones específicas (acuerdos internacionales en materia de desarme, cambio climático, política migratoria, etc.), finalmente, están los:
- *Intereses en conflicto* categoría que incluye los intereses que no son complementarios ni idénticos, es decir aquello temas en los cuales existen claras diferencias, controversias y posibilidades de conflicto entre los Estados-Nación. Por ejemplo, posturas en torno a la solución de un conflicto bélico que beneficie a determinado bando que sea aliado estratégico de un país (común cuándo se llegan a confrontar superpotencias del sistema internacional como Estados Unidos, China o Rusia), temas o visiones en torno a modelos políticos o culturales, como los que existen entre la sociedad cristiana, islámica o sínica.

No obstante, de estas tres categorías, se expresa que está clasificación no es absoluta ni completa, dado que los intereses complementarios o idénticos, puede volcarse en intereses en conflicto, a razón de una coyuntura o quiebre en el *statu quo* internacional. Así como el hecho de que el estudio del interés nacional de un Estado-Nación implica un análisis a profundidad de todas las esferas de sus intereses vitales y no vitales. Por lo cual, el esquema ofrecido por Robinson (1995) es de gran utilidad para examinar el interés nacional de gran cantidad de países del mundo. Una vez explicado las nociones básicas del concepto del interés nacional, es importante abordar los elementos teóricos que han dan identidad y características a dicha categoría, con base al paradigma teórico, entre los que abordaremos al realismo y neorrealismo, Teoría de la Guerra, liberalismo y constructivismo, aspecto que es el eje central del siguiente apartado.

3.1.1Visiones teóricas en torno a la comprensión del interés nacional

3.1.1.1 El paradigma realista

Como primera escuela teórica de las relaciones internacionales, el realismo parte de tres supuestos principales:

- El Estado-Nación es el actor principal de la política internacional.
- En la sociedad internacional no existe una autoridad central equivalente a un gobierno nacional, por lo tanto, la política internacional es caracterizada por la anarquía, y;
- La política internacional es esencialmente política de poder.

En ese sentido, uno de los principios fundamentales del realismo es el énfasis que pone entre la dicotomía de política nacional e internacional (Deng, 1995). Sobre este punto Hall (2006) expresa que el principal objetivo de la política interna de las naciones es la búsqueda de la prosperidad y el bienestar, mientras que el valor más alto de la política internacional es la supervivencia o trascendencia como potencia. Por lo cual esta arena es dónde la lucha por el poder es más ardua, dado que la política interna se rige por el marco de derecho e instituciones de cada país, mientras que en la política internacional la ley y el orden están sujetos a la lucha por el poder entre los Estados-Nación (Wight, 2002).

En ese sentido, no destaca que el paradigma realista fuera de alta efectividad para la comprensión de la política global en el periodo inicial de la Guerra Fría, durante la década de los cincuenta y sesenta, del siglo XX, en que los preceptos de este paradigma se ajustaron

a los sucesos acontecidos con la confrontación ideológica entre Estados Unidos y la Unión Soviética. En sí, episodios como la Guerra de Corea, la Guerra de Vietnam y la Crisis de los Mísiles, pusieron un énfasis preponderante sobre lo cruento y arduo que es la anarquía global y la lucha de las superpotencias por mantener posiciones de poder en la esfera global. No obstante, el paradigma empezó a entrar en conflicto durante la década de los setentas del siglo XX, a razón de que las nuevas dinámicas de cooperación, cimentadas en procesos de integración europea, así como el nuevo entorno económico global, promovido por escuelas de pensamiento como el *behaviorismo,* interdependencia compleja y el liberalismo económico, demostraron que la construcción de poder y posiciones de los actores globales, no se limitaban solamente a una lucha entre los Estados-Nación, sino también existía una fuerte injerencia de los acuerdos multilaterales, la construcción de organismos regionales o internacionales, así como la fuerte presencia de las empresas trasnacionales en la dinámicas del poder global.

Es en este contexto, que la vertiente del neorrealismo, dentro del paradigma, surge para refinar el realismo clásico. De esta forma, el principal aporte del neorrealismo se da en su concepción de abordar al sistema internacional como una estructura que configura y delimita el comportamiento de los Estados-Nación. Esto a razón de cada país está centrado en resguardar sus intereses nacionales que garanticen su sobrevivencia y existencia como actor internacional en el largo plazo. Por lo cual esta noción de subsistencia que tiene cada Estado-Nación termina por transformarse en el principio de ordenamiento del sistema internacional descentralizado y anárquico. En el que los estados están sujetos al imperativo de la supervivencia y, por lo tanto, están obligados a perseguir este objetivo según las condiciones preponderantes en el sistema internacional, frente a otros actores como las superpotencias, potencias regionales o países promedio. Por último, sobre este punto, el neorrealismo establece que los Estados-Nación solo difieren en sus respectivas capacidades según lo determinado por distribución del poder en el sistema internacional (Waltz, 2010).

Por otra parte, es importante mencionar que, si bien con los preceptos descritos anteriormente el neorrealismo no acepta completamente la noción de definir a la anarquía como la norma de la política global, por considerarla una visión con un nivel de análisis reduccionista, sí acepta el resto de los supuestos básicos del realismo. De esta forma, este paradigma propone

una teoría del interés nacional cuyo máximo postulado es articulado por Hans Morgenthau, al expresar que el principal indicador del actuar y hacer de las naciones, así como de sus líderes, en la política internacional se centra en garantizar la sobrevivencia del Estado-Nación y sus valores, así como alcanzar, construir y mantener posiciones de poder en el contexto internacional.

De esa forma, el papel de los líderes nacionales o "estadistas" se centra y operacionalizar la estrategia y plan de acción que materialice la búsqueda de los intereses nacionales objetivamente existentes por cada país. Este Estado-centrismo, vinculado a las nociones de anarquía e interés nacional hacen que este paradigma sea el más cercano a las nociones de la soberanía Wetsphaliana, aunque con el pasar del tiempo, el realismo ha aceptado que los canales de poder se miden en diferentes campos, como la cultura, política, economía, etc. (Russett, Oneal, y Cox, 2000; Sørensen, 2009) así como el hecho de que su materialización también se condiciona a los diferentes entornos y espacios geopolíticos existentes, como el mar, el aire, el espacio exterior y el ciberespacio (Craig y Valeriano, 2018).

Sobre este último punto, autores como Waver (2012) resaltan que la visión realista de la naturaleza anárquico-westfaliana de las relaciones internacionales es un medio para reforzar la fuente estructural de occidente como centro de poder en la política internacional. En el que debates recientes como los enfrentamientos entre civilizaciones, la lucha por definir un criterio universal de derechos humanos, y la hegemonía global y expansión de las nuevas tecnologías como el internet y telecomunicaciones, representan elementos de una lucha de la sociedad occidental por mantener la preponderancia de sus ideologías políticas, estilos de vida y valores como normas hegemónicas en el mundo.

3.1.2 La visión liberal

Si bien el concepto de interés nacional tiene su raíz de origen en el paradigma realista, otras escuelas teóricas o vertientes de pensamiento de las relaciones internacional también han cimentado visiones alternativas en torno a su comprensión. En contraste con el realismo, el liberalismo enfatiza el rol de los actores estatales y no estatales, a la par que considera la política internacional como un juego de suma de procesos y actores, en contraposición a la visión centrada en comprender al poder como un juego de suma cero. De esta forma, la raíz del pensamiento liberal tiene una estrecha concordancia con la escuela de la interdependencia

compleja, que centra gran parte de su análisis en las relaciones de cooperación e integración que consolidan las naciones a través de instituciones multilaterales y regímenes internacionales que, en determinados contextos, logran sobreponerse por encima de la anarquía global, aspecto clave en el paradigma realista. De esta forma, para la escuela liberalista fenómenos y procesos como el comercio internacional, la promoción de la democracia, el respeto a las normas, tratados, reglas e instituciones en las relaciones entre países son mecanismos que dejan de lado la hipótesis de la anarquía como imperativo de la sociedad internacional (Keohane y Dunn, 2002; Williams, 2005).

Del mismo modo, es importante mencionar que el liberalismo centra su atención en procesos como la globalización y el neoliberalismo económico a finales del siglo XX, que a través de la creación de zonas afines al libre comercio y el desarrollo de tecnologías como el internet redujeron la distancia entre las regiones, y cambiaron la lógica en que se desenvolvían procesos políticos de continentes enteros como América, Asía y Europa (Van de Haar, 2009). Del mismo modo Ikenberry (2011) destaca que el paradigma apoyó la noción de cimentar dinámicas que impactan en prácticamente todas las naciones del mundo como las relaciones económicas, los intercambios comerciales, el desarrollo científico y tecnológico, la cuestión de la protección del medio ambiente, el control de la población, la mitigación y alivio de desastres naturales, las prohibiciones de drogas, la prevención del crimen organizado global, la prevención de la proliferación nuclear y la atención y coordinación frente a problemáticas que no conocen fronteras como las pandemias o fenómenos migratorios (Miller, 2018). Conjunto de temáticas globales que son de naturaleza mundial e interdependiente, las cuales requieren de esquemas de cooperación y estándares globales para ser homologados entre los diferentes países que integran la comunidad internacional.

Para el caso concreto de la comprensión del ciberespacio, Petallides (2012) expresa que el liberalismo aporta una visión centrada en el hecho de que hay preocupaciones y esfuerzos globales, por gran parte de las naciones, de cimentar estándares mínimos para una regulación, securitización de esta arena de interacción de los Estados-Nación. En los hechos, esto se ve representado por el papel que juegan organismos como la Unión Internacional de Telecomunicaciones (ITU), con la creación de la Agenda Global de Ciberseguridad AGC, o lo que realizan la Agencia Europea de Seguridad de la Información (ENISA) y la

Organización de los Estados Americanos (OEA) en los ámbitos regionales de Europa o América, para liderar iniciativas centradas en la creación de ciber capacidades.

De esta forma, el liberalismo, a través de fenómenos como la globalización, hacen ver a los países del mundo que la regulación y securitización del ciberespacio, es una dimensión que deben abordar y atender si desean integrarse de manera plena a las dinámicas que acontecen en el contexto internacional, aunque estas no sean necesariamente una preocupación central de su política exterior, política de seguridad nacional, o incluso, de su interés nacional. En ese sentido, dichos postulados del paradigma realista entran en controversia con gran cantidad de los preceptos de la soberanía Wetsphaliana, dado que aceptan que existen impulsos provenientes del contexto global, que obligan a los Estado-Nación a ocuparse de temas que no necesariamente son la preocupación central de su política interna, centrada en garantizar la prosperidad y bienestar de la sociedad, e incluso de la política exterior, dado que en ocasiones los países pueden buscar conducir su relaciones diplomáticas y actuar internacional a metas que no siempre están en concordancia con las agendas de organismos multilaterales o de la opinión pública internacional (Kundnani, 2017).

Con relación a lo anterior, se expresa que, si bien el liberalismo entra en polémica con la visión de la soberanía Wetsphaliana, al poner énfasis en los impulsos externos, que delimitan las decisiones y acciones de los países en el ámbito interno, para adaptarse a las relaciones internacionales, Ikenberry (2011) expresa que el paradigma también puede entenderse como una noción táctica de los países para ganar presencia en el contexto internacional. En ese sentido, se expresa que el fenómeno de la globalización y liberalización económica iniciado en los años noventa del siglo XX, y presente en sus resultados hasta nuestros días, fue un área de oportunidad para que a través de las dinámicas y preocupaciones globales o regionales gran cantidad de Estados-Nación realizaran proselitismo a favor de determinadas causas de interés global. Y las hicieran un elemento clave de su interés nacional y política exterior para posicionarse como actores con un mayor protagonismo en determinadas esferas (Hurrell, 2006). Lo anterior, se ve con relación a países que son referentes y llevan la batuta en teman como el cuidado al medio ambiente (Canadá, Singapur, Noruega), promoción del multilateralismo global (China, Brasil, Rusia, India), e incluso creación de software y aporte global a la ciberseguridad, como es el caso de Estonia. Las cuales, si bien no son potencias

globales en esferas la militar, política, cultural o económica, son referentes globales de esas temáticas que lo hacen actores de trascendencia en dichos procesos internacionales.

En ese sentido, Yizhou (2002) destaca que el impacto de la interdependencia en la política internacional, que destacan el potencial del liberalismo para promover la posición de un Estado-Nación en el contexto internacional, se da a través de la reestructuración del interés nacional con base a un elemento de la agenda global. En la actualidad, esto es posible a razón de una serie de diez factores que potencializó a nivel interno en cada país el fenómeno de la globalización que son:

I. Incongruencia entre la nación y el estado,
II. el debilitamiento de las capacidades y responsabilidades del Estado,
III. desigualdad en recursos y calidad diplomática,
IV. cultural débil y poca identificación y legitimidad del régimen,
V. el fortalecimiento de la intervenciones extranjeras y leyes internacionales,
VI. un papel más importante para organizaciones internacionales,
VII. el creciente poder efectivo de las organizaciones no gubernamentales,
VIII. economías "sin fronteras" e interdependencia global,
IX. profundización de las crisis globales y;
X. actividades en el espacio aéreo, ultraterrestre, marítimo y ciberespacio, por actores no considerados potencias hegemónicas desde la perspectiva realista (Yizhou, 2002).

Con lo cual se expresa, que el liberalismo considera que el esquema de sistema de seguridad individual, central en el realismo, no siempre es una vía efectiva para escalar posiciones de preponderancia en la política global para los países que no tienen las características de una potencia político-militar. Por lo cual, gran cantidad de países optan por los esquemas de seguridad colectiva y la promoción de intereses multilaterales, como parte central de su interés nacional, para adquirir un papel de mayor peso en el sistema internacional.

i. La Teoría de la Guerra

La comprensión de la Teoría de la Guerra y su cercanía con la noción de interés nacional, antes que nada, requieren una revisión en torno a la comprensión de la guerra justa y la soberanía del Estado-Nación. En este sentido, se destaca que la Teoría de la Guerra Justa considera una agresión a la soberanía del Estado-Nació (en la comprensión de la integridad

de su territorio, población, gobierno e instituciones) como una afectación a su subsistencia, vida y libertades de sus habitantes, así como a la paz de la nación. En ese sentido, la Teoría de la Guerra Justa afirma que la guerra puede estar moralmente justificada bajo ciertas condiciones. En este contexto, Moseley (2011) expresa que la Teoría de la Guerra Justa se divide en tres partes:

- *Jus ad Bellum*, que implica la justicia de recurrir a la guerra por motivos de autodefensa, la defensa de otros de un ataque agresivo, la protección de personas inocentes de regímenes agresivos, o castigo correctivo por agresión, pasada una acción. Para esta declaración de guerra se cuenta con la aprobación de la ciudadanía, la competencia de una autoridad facultada para hacerlo por el Estado-Nación (como el congreso, los partidos políticos, la opinión pública, etc.). A la par que existen probabilidades de alcanzar el éxito en esta ofensiva y se cumple con el principio de proporcionalidad y recurre a la guerra como último recurso.
- *Jus in Bello*, que se refiere a la conducta justa en la guerra y tradicionalmente se refiere al trato entre oponentes en un conflicto. Esta parte de la Teoría de la Guerra Justa trata aspectos como el no utilizar armas prohibidas por el derecho internacional, hacer la distinción entre combatientes y no combatientes, que las Fuerzas Armadas utilicen y posean una fuerza proporcional, y se trate de manera humanitaria a los prisioneros de guerra. Finalmente, está él;
- *Jus Post Bellum*, o justicia al final de la guerra, que establece que al fin del conflicto deben de garantizarse los derechos cuya violación justificó la guerra, se debe realizar la declaración de paz por una autoridad apropiada que represente al Estado-Nación, debe cumplirse el principio de proporcionalidad en los acuerdos de paz (para evitar resentimiento y una mayor agresión en el futuro). Debe realizarse un proceso de justicia a combatientes, incluidos líderes políticos, y no combatientes que hayan incurrido en conductas o acciones contrarias los preceptos de la guerra justa a través de juicios públicos e internacionales de guerra para quienes merezcan un castigo

Con relación a lo anterior, se establece que las visiones de la Teoría de la Guerra Justa tienen una fuerte vinculación con múltiples elementos de la noción de soberanía del Estado-Nación, en su estado más clásico Wetsphaliano, así como con varios preceptos del derecho

internacional público y el liberalismo. No obstante, es importante destacar que esta visión refuerza la legitimidad de recurrir a la ofensiva de guerra como elemento de la seguridad nacional de un país. También, descarta que los países se involucren en acciones armadas sólo bajo el sustento de sus intereses individuales, que no estén en concordancia con las preocupaciones morales y éticas de la comunidad internacional.

Sin embargo, en contraposición a esta postura, existen una vertiente de la teoría de la guerra, fuera de la perspectiva de la guerra justa, denominada *realista* que consideran que los Estados actúan sólo en términos del interés propio. En ese sentido, se destaca que la vertiente realista se divide en dos perspectivas:

- El *realismo descriptivo*, que cree que los Estados no están motivados por la justicia, sino por el interés nacional, incluido el poder y la seguridad. Y el;
- *realismo prescriptivo*, que expresa que es prudente que los Estados-Nación actúen sin tener en cuenta moralidad en la política exterior, no sin respetar en lo más básico, las condiciones mínimas para un conflicto establecidas en la Teoría de la Guerra Justa.

En ese sentido, la perspectiva realista acepta que las guerras no son justas, sino necesarias y es precisamente esta visión la que más se acerca al origen de los preceptos del concepto de interés nacional surgidos en el paradigma realista de las relaciones internacionales. Una de las autoras que más ha marcados los puntos en común entre la vertiente de pensamiento realista de la teoría de la guerra y el realismo político ha sido Rice (2000), quien expreso que, en la época posterior a la Guerra Fría, el interés nacional las potencias internacionales como Estados Unidos tenía cinco metas, que son:

- Garantizar que sus fuerzas armadas tengan la capacidad de disuadir del conflicto, proyectar poder y luchar en defensa de sus intereses si la disuasión falla;
- promover el crecimiento económico y la apertura política a través del comercio y un sistema monetario internacional comprometido con estos principios;
- renovar relaciones sólidas e íntimas con aliados que comparten los valores occidentales o semejantes, con el fin de promover la paz, prosperidad y libertad;
- enfocar su política exterior en cimentar relaciones integrales con otras grandes potencias, que sean trascedentes para moldear el contexto del sistema político internacional;

- hacer frente de manera decisiva a la amenaza de regímenes rebeldes y poderes hostiles, que sean actores desestabilizadores del contexto internacional.

Los fundamentos anteriores, moldearon la política exterior de los Estados Unidos en la primera década del siglo XXI y crearon fuertes tensiones éticas y morales en la comunidad internacional a razón de presentar un escenario en el que los Estados-Nación, abogaban más por sus intereses nacionales, los cuales estaban en clara lejanía con las nociones del multilateralismo y la justica internacional, dejando de lado los preceptos clásicos de la teoría de la guerra justa en el actuar de la política internacional.

Relacionado a este contexto, Varacalli (2016) expresa que las visiones individualistas de los Estados-Nación parten de reconocer que en la política internacional las naciones van a la guerra o entran en conflictos por una variedad de razones, algunas más defendible que otras, pero siempre aceptando estas acciones pueden estar vinculada a derechos dudosos y controvertidos, entre los que están sus intereses nacionales. Ya que si en los hechos, los preceptos de la guerra justa operaran gran cantidad de conflictos de la historia internacional, no hubieran acontecido. En ese sentido, cuándo lo Estados-Nación deben decidir sobre promover su interés nacional o su responsabilidad moral, está claro que el interés nacional domina dicho juicio. Sobre este punto, Bahrisch y Kim (2011) señalan que autores clásicos de la Teoría de la Guerra como Alfred Tayer Mahan expresan desde el siglo XIXI que la búsqueda del interés nacional, por parte del Estado-Nación, no se diferencia de la del individuo en su búsqueda de intereses. Y, de hecho, la búsqueda de intereses se amplifica especialmente en el ámbito de las relaciones internacionales. Ya que en tiempos de paz o de guerra, las naciones actúan por un impulso determinado por el cálculo de beneficios, en el que sólo las naciones exitosas logran encontrar formas de procurar sus intereses y al mismo tiempo protegerse a ellas mismas contra sus competidores.

Por lo cual la guerra es una posible solución y una vía para asegurar por medios justos todo aquello que contribuya al progreso del Estado-Nación, que también ayuda a combatir las acciones perjudiciales tomadas por un actor agencia externa. Dado que el fin de la existencia del Estado-Nación es la auto conservación, que no sólo se limita a defender la sobrevivencia de un país, sino también implica el derecho a defender los intereses de nacionales, ya sea en respuesta directa a una provocación o no. Con lo cual se justifica que los países persigan

intereses particulares, en cualquiera de los teatros de guerra, ya sean estos el espacio terrestre, marítimo, aéreo y espacial. Asimismo, para el caso del ciberespacio, las naciones a través de sus Fuerzas Armadas, ya sea de manera individual o en colaboración con entidades privadas expertas en seguridad cibernética o desarrollo de hardware, pueden realizar operaciones ofensivas con el fin de promover los intereses de cada país, mantener o incrementar su poder e intereses particulares en la comunidad internacional, así como garantizar su subsistencia.

3.1.3 Constructivismo e interés nacional

El constructivismo como enfoque de las relaciones internacionales marca una división entre política exterior y política internacional, como un importante punto de partida. Para esta escuela teórica, la división entre ambas categorías se da a razón de que la primera corresponde a la acción de cimentar una política nacional para que un Estado-Nación se relacione con otros agentes similares. Mientras que la segunda, corresponde a una estructura global frente a la cual cada país encuentra su papel e identidad, y en la que debe atenerse a las reglas y normas que imperan en el sistema internacional (Kubalkova, 2015). Del mismo modo, la división sirve para explicar las diferencias entre lo que el constructivismo entiende como los agentes de las relaciones internacionales (Estados-Nación, Organismos Internacionales, Empresas, grupo globales, etc.), y la estructura, que se vincula a dinámica que se crea derivado de la interacción mundial de todo el conjunto de actores. De esa forma, expresa que hay una interrelación entre los agentes y la estructura, los cuales no pueden separarse.

Del mismo modo, este paradigma hace una crítica al realismo y liberalismo, escuelas que suponen que el interés nacional de los Estados representa una combinación de la búsqueda del poder del Estado-Nación, así como garantizar su seguridad y prosperidad. Sobre este punto, Finnemore (2010) expresa que dichos conceptos que son centrales en cada uno de dichos esquemas de pensamiento presentan una gran ambigüedad, dado que utilizan las tres categorías para describir el interés nacional de cada nación. Sin embargo, nunca definen ¿qué tipo de poder y con qué fin? ¿Qué tipo de seguridad? ¿Qué significa la seguridad y prosperidad para cada país? Y quizás la interrogante más trascedente: ¿cómo se obtiene o alcanza el interés nacional? Frente a estos cuestionamientos el realismo y liberalismo no tienen respuestas sistémicas y completas. Y lo anterior se debe a que las amenazas externas y las limitaciones de poder de cada Estado-Nación solo pueden abordarse e identificarse caso

por caso, por tomadores de decisión de gobierno, especialistas o analistas de política exterior de cada país.

Frente a esto, el constructivismo propone un enfoque sistémico para comprender los intereses y el comportamiento de los Estado-Nación a través de la estructura del sistema internacional, pero centrándose plenamente en el poder que posee cada uno de sus protagonistas o agentes inmersos, sino por medio de su significado y valor social (Nugroho, 2008). De esta forma, para el constructivismo no se puede entender lo que quieren los Estados, sin comprender la estructura del sistema internacional, los actores que forman parte de él. Por lo cual marca una diferencia sustancial al entender al poder y riqueza no como medios, sino como fines. Para los cuales cada nación debe decidir cómo los entiende y qué quiere hacer con ellos. Lo anterior, implica que gran cantidad de países no siempre sepan lo que quieren o cómo para utilizar sus recursos.

En este punto, se vuelven trascendentales los procesos que acontecen en la política doméstica que en múltiples casos tienen un papel determinante en la definición de objetivos e intereses nacionales. Sobre este punto Haas y Haas (2002) expresan que la definición de los intereses estatales se realiza con base al contexto de normas sostenidas internacionalmente y comprensión sobre lo que es bueno, correcto y apropiado dentro la lógica de la estructura global. Este argumento, conlleva el comprender que los Estados-Nación son entidades construidas socialmente y evolucionan continuamente. Asimismo, el constructivismo destaca, porque también aborda la construcción social de las organizaciones internacionales, tratados, estructuras legales y corporaciones multinacionales.

De esta forma, el fin del paradigma constructivista y su propuesta metodológica es el desentrañar las relaciones causales dentro y fuera de cada Estado-Nación, acción que debe realizarse de manera individual para cada país, dado que cada uno de estos actores constituyen una observación independiente (Finnemore, 2010). Esta acción es determinante para que cada nación identifique las preferencias que moldean su interés nacional, hecho que lo ayudaran a determinar la distribución del poder que posee como actor internacional y el papel que ocupa en la estructura global, es decir, si representa una potencia global, regional o un país intermedio. También, harán visibles e identificables las necesidades de su seguridad

nacional, así como las vías en que esas preferencias pueden transformarse en políticas nacionales (Nugroho, 2008).

Para los fines de esta investigación, se debe de expresar que el ciberespacio puede entender como una estructura social de la sociedad internacional, en la cual los Estados-Nación deben definir las preferencias de su interés nacional, las necesidades de su seguridad nacional, así como las acciones que ejecutaran respecto a este dominio para alcanzar sus metas y garantizar su seguridad. Por otra parte, este enfoque también nos ayuda a comprender los impulsos externos que demarcan a la ciberseguridad como un aspecto crucial que deben tomar las naciones del mundo, como lo hace la ITU a través de la AGC, así como la importancia y peso que dan los países al desarrollo de ciber capacidades, que puede medirse y analizarse a través de los doce indicadores del NCSI (2018).

Por lo que estas métricas sirven como instrumentos que guían las normas de comportamiento e instituciones internacionales, que proporcionan a los Estados-Nación dirección y metas para la acción. Así como encarnar los valores, reglas y roles que definen el comportamiento de las naciones en el ciberespacio. Por otra parte, los sucesos como los fenómenos de los ciberataques de Tallin (2007), Stuxnet (2011), o el Cablegate (2011) nos demuestran el poder potencial que poseen determinados actores en la estructura internacional, en el que vemos que existen naciones que son potencias en el ciberespacio (como Estados Unidos, Rusia, China, etc.), potencias de grado medio (Estonia, Israel, etc.) y países que avanzan en la construcción de sus ciber capacidades (por ejemplo, las naciones de América Latina). Con lo cual, dicha interacción y socialización internacional permite a los actores comprender su posición en la política global. Y diseñar un interés nacional y política exterior racional con base a los costos y ganancias derivados de romper o acatar las normas del sistema global, así como los recursos disponibles que poseen y necesitan en relación a los valores, reglas y roles de la estructura internacional.

3.2 Métodos y estrategias para garantizar el interés nacional

Una vez expresadas las principales interpretaciones teóricas en torno al interés nacional que sirven para el presente estudio, es necesario abordar los métodos que poseen los Estados-Nación para perseguir su interés nacional. En ese sentido, los debates teóricos sirven para remarcar que esta acción representa por parte de las naciones el asegurar las metas y objetivos

que posee como actores de la comunidad internacional, a la par que representa un derecho y deber primordial de toda nación, dado que los gobiernos de los países siempre están trabajando para asegurar su interés nacional. Sobre este sentido, Sklenka (2007) presenta un conjunto de cinco métodos o instrumentos populares que generalmente emplean las naciones para asegurar sus intereses nacionales en las relaciones internacionales, que son:

La diplomacia como medio del interés nacional, el más antiguo y universalmente aceptado para asegurar los intereses nacionales. Ya que a través de la diplomacia la política exterior de una nación puede ser identificada por una nación extranjera a través de las relaciones bilaterales o multilaterales. Y de esta forma, los diplomáticos establecen contactos con los tomadores de decisiones y diplomáticos de otras naciones, con el fin de llevar a cabo negociaciones para lograr las metas y objetivos deseados de los intereses nacionales de su nación. Asimismo, esta tarea representa una ardua labor por persuadir a otros países de aceptar los intereses de una determinada nación como demandas justas y legítimas. Y para lograr estas tareas pueden recurrir a medios como las amenazas y las recompensas, las cuales son especificadas con base a la capacidad de ejercer poder como actor internacional y el asegurar los objetivos del interés nacional definidos por la política exterior de su nación. Del mismo modo, es importante destacar que las negociaciones diplomáticas constituyen el medio más eficaz de resolución de conflictos y reconciliación de los intereses divergentes que existen entre los Estados-Nación. Lo cual se logra a través de concesiones mutuas, medidas de cesión y reconciliación aceptables para cada nación. Del mismo modo destaca que, a pesar del regirse bajo la noción de la anarquía internacional y la lucha del poder, el mismo Hans Morgenthau consideró a la diplomacia como el medio más primario para que un Estado promoviera los objetivos y metas de su interés nacional.

Propaganda: corresponde al segundo método importante para asegurar el interés nacional, y se vincula a convencer a otros acerca de la justicia de las metas y objetivos o fines que las naciones desean asegurar. De esta forma, consiste en el intento de inculcar a las naciones la necesidad de asegurar las metas que una nación desea alcanzar. En el contexto de la Guerra Fría, la propaganda se unió a los valores nacionales y modelos políticos de las superpotencias como la Unión Soviética y los Estados Unidos, y fue un componente central entre la lucha entre el modelo democrático y socialista (Burchill, 2005; Frankel, 1984). Del mismo modo,

es importante entender que la propaganda está dirigida directamente a la población y líderes políticos de otros Estados-Nación. Y su objetivo es siempre asegurar los intereses propios, intereses que se rigen exclusivamente por los intereses nacionales del propagandista. Del mismo modo, la propaganda encuentra puntos en común con el término del *softpower* de Nye (2010), que supone la enmarcación, atracción y persuasión de la agenda política a través de valores culturales, políticos o ideológicos de una nación. Por último, se expresa, que, en la actualidad, a través del revolucionario desarrollo de los medios de comunicación, como el internet, y el avance de las telecomunicaciones, en tiempos recientes ha aumentado el alcance de la propaganda como medio para asegurar el apoyo a objetivos del interés nacional, de los cuales no queda excluido el uso del ciberespacio.

- *Medios económicos:* están principalmente al alcance de las naciones prósperas y desarrolladas, que utilizan la ayuda económica y los préstamos con otros países como medio para asegurar sus intereses en las relaciones internacionales. Por lo cual este método y sus instrumentos se sirven de la existencia de las brechas entre naciones desarrolladas y no desarrolladas como medio de oportunidad a las naciones con riqueza para promover sus intereses frente a las naciones menos desarrolladas. Esta dependencia puede darse a través de la importación de bienes industriales, conocimientos tecnológicos, ayuda externa, armamento y para la venta de materias primas. Del mismo modo, es importante destacar que, a partir de la década de los setenta, del siglo XX, este método ha fortalecido el papel de los instrumentos económicos de los países extranjeros en la política internacional. Y que en la era de la globalización, la conducta de las relaciones económicas internacionales ha surgido como un medio clave de los intereses nacionales.
- *Alianzas y tratados*, relacionados a los convenios que dos o más estados celebran en aras de asegurar sus intereses comunes. Este método se utiliza principalmente para asegurar intereses idénticos y complementarios. Sin embargo, incluso los intereses conflictivos pueden llevar a alianzas y tratados con estados de ideas afines contra rivales u oponentes comunes. Por otra parte, es importante mencionar que en la actualidad las alianzas y tratados son vinculantes para los Estados-Nación, lo que hace que sea una obligación legal para los miembros de las alianzas o signatarios trabajar por la promoción de los intereses comunes acordados. A la par que estas

pueden concluirse cuándo se ha alcanzado el interés específico particular, para el que fueron creado, o esté se ha transformado dadas las circunstancias del contexto internacional. En consecuencia, las alianzas son de naturaleza militar o económica. Y estás han tenido una utilidad trascendente del inicio de la Guerra Fría, hasta la segunda década del siglo XXI. Por ejemplo, la necesidad de garantizar la seguridad de los estados democráticos capitalistas contra el mundo socialista, o de mantener acuerdos de cooperación militar para resguardar la seguridad de determinadas regiones del mundo derivó en la creación de alianzas militares como la OTAN, Organización del Tratado del Sureste Asiático (SEATO por sus siglas en ingles), la Organización del Tratado Central (CENTO), o la ANZUS (la acrónimo proveniente de Australia, Nueva Zelanda y Estados Unidos) en el pacífico, etc.

Asimismo, durante su existencia en el Siglo XX, la necesidad de enfrentar la amenaza al socialismo llevó a la construcción y conclusión del Pacto de Varsovia, por los países comunistas. Lo que es un ejemplo representativo de como una alianza puede darse por encontrar intereses comunes de un determinado grupo de Estados-Nación, y dejar de existir dada una transformación cualitativa en el contexto internacional. Por el lado del ámbito económico, el ejemplo más representativo se da en el marco de la necesidad de la reconstrucción económica de Europa después de la Segunda Guerra Mundial, que llevó al establecimiento de la Comunidad Económica Europea (en la actualidad la Unión Europea), así como el Tratado de Libre Comercio de América del Norte (TLCAN) y un gran conjunto de agencias y procesos de integración económica. Los cuales presentan ejemplos sobre su vigencia y transformación para determinados actores, lo cuales pueden ser abandonados cuándo ya no responden a sus intereses nacionales, como fue el caso del Reino Unido con su salida de la Unión Europea a través del Brexit, o reconfigurarse y transformarse, dado que actores determinados consideran necesitan se actualizados para seguir siendo benéficos a la prosperidad del Estado-Nación, como aconteció con la renovación del TLCAN al Tratado Comercial México, Estados Unidos y Canadá (TMEC). Con lo que se evidencia que las alianzas y los tratados son medios populares para asegurar los intereses nacionales.

- *Medios coercitivos*, los cuales están más cerca de las nociones del poder bélico o *hardpower* en las relaciones internacionales. En sí, los medios coercitivos corresponden a una ley no escrita de la política internacional que las potencias hacen latente a otros Estados-Nación, para externarles a estos, ya sean adversarios o aliados, que no deben realizar determinadas acciones que afecte o vulneren sus intereses nacionales. Porque de caso contrario, las potencias harán tangible su fuerza para asegurar dichas metas. Sobre este punto, es importante mencionar que el derecho internacional también reconoce los medios coercitivos, que no son la guerra, como los métodos que pueden utilizar los estados para cumplir sus metas y objetivos deseados, entre los que se incluyen la intervención, los embargos, los boicots, las represalias, la réplica y la ruptura de relaciones diplomáticas, que son medios coercitivos populares que puede utilizar una nación para obligar a otros a aceptar una condición, acatar una conducta o abstenerse de seguirla.

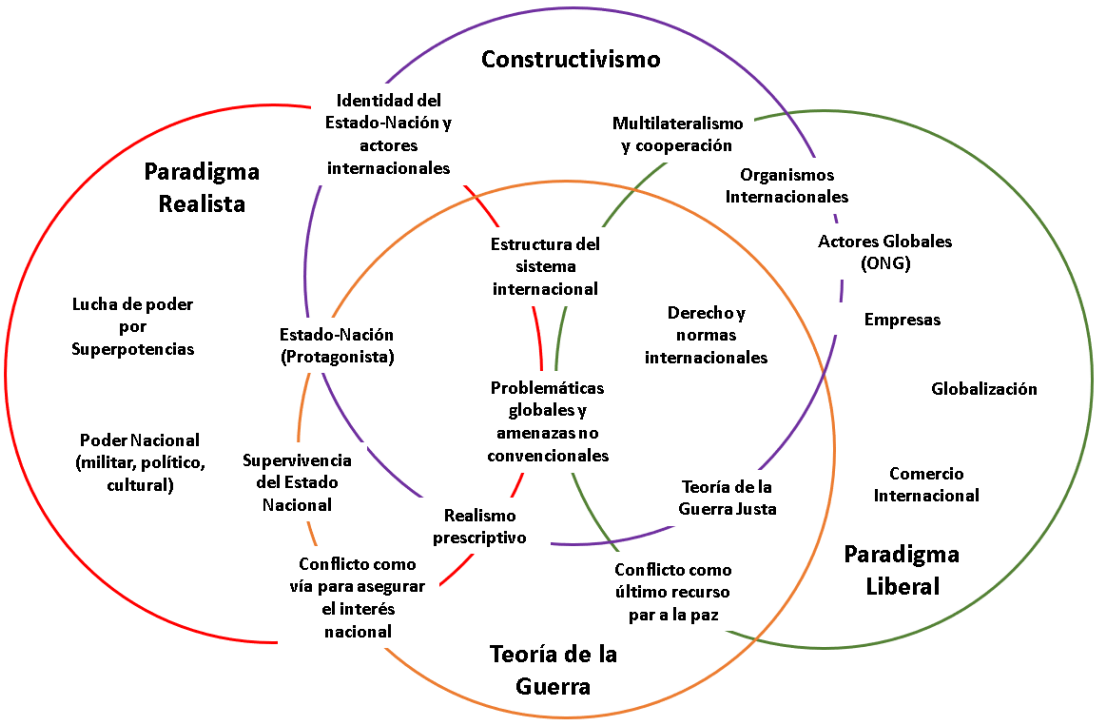
  Del mismo modo, a pesar de que la guerra y la agresión son declarados medios ilegales o mecanismos con los cuales se procede cuándo se han agotado todas las instancias pacíficas o viables a través del derecho internacional, continúan siendo utilizados por los Estados en el curso real de las relaciones internacionales. Y a pesar de que en la actualidad la mayoría de los países dan cuenta de la importancia de los medios pacíficos de resolución de conflictos, como las negociaciones diplomáticas, como métodos ideales para promover sus intereses nacionales. Al mismo tiempo, siguen manteniendo vigencia los medios coercitivos, siempre que se les considere oportuno o necesarios para salvaguardar el interés nacional. Con lo cual el poder militar todavía es una parte importante del poder nacional y, a menudo, los Estados-Nación lo utilizan para asegurar sus metas y objetivos deseados. Dado que, dentro de los paradigmas teóricos, y la operación y ejecución de la política exterior, gran cantidad de pensadores y operadores políticos consideran que las naciones tienen el derecho y el deber de asegurar sus intereses nacionales y tienen la libertad de elegir los medios necesarios a tal efecto, ya sean al utilizar medios pacíficos o coercitivos cuando lo deseen o lo consideren esencial.

3.3 La construcción de una estrategia y política exterior de los Estados-Nación

La construcción de la política exterior de un Estado-Nación deriva del proceso histórico de la conformación del Estado, la creación de su identidad, así como del desarrollo de sus capacidades intersubjetivas que le otorgan un papel dentro del sistema internacional. En ese sentido, los referentes teóricos señalados en la sección anterior sirven para establecer un análisis de cómo los Estado-Nación configuran su política exterior con base a estas variables. Asimismo, es importante mencionar que el abordaje de los paradigmas realista, liberal, constructivista y de la Teoría de la Guerra corresponde a un enfoque ecléctico que no se ajusta rígidamente a un paradigma de análisis o un conjunto de supuestos, sino que se basa en múltiples teorías, estilos e ideas para obtener información complementaria en torno a las unidades de análisis.

Con relación a lo anterior, en la Figura 24 se presenta un modelo de análisis y abordaje teórico metodológico para entender la construcción de la política exterior de los Estados-Nación, con base al fenómeno internacional que desee abordarse y el cuál será utilizado dentro de nuestro análisis.

Figura 24. Propuesta de modelo teórico-metodológico de análisis de la política exterior.



Fuente: Elaboración propia.

Del mismo modo, se describe brevemente su aplicación con base a cada paradigma de pensamiento y se sugieren algunas dinámicas de la política internacional que pueden abordarse con los mismos:

1. Paradigma realista: el primer paradigma de análisis aborda elementos del realismo clásico y del neorrealismo. De esta forma, dos esferas individuales que son clave y exclusivas de este esquema de pensamiento corresponden a abordar la lucha por el poder de las superpotencias en el sistema internacional y aceptar la existencia de una anarquía global. Asimismo, el realismo se centra y tiene un eje central en calibrar el poder nacional que detentan los diferentes países del mundo. De esta forma, es objeto de análisis del realismo clásico el poder nacional de los Estados con base a su poderío militar. Mientras que el neorrealismo, abre el abordaje del paradigma a elementos como los factores políticos y culturales. Por último, se destaca que el paradigma realista tendrá puentes complementarios para el análisis ecléctico con el constructivismo, en aspectos como delimitar la identidad de los actores internacionales. También, se empalmará y complementará con la Teoría de la Guerra, en contener como a uno de sus ejes centrales la supervivencia del Estado-Nación ante el esquema anárquico que impera en la sociedad internacional.

Asimismo, ambos esquemas expresan que los conflictos suponen vías tangibles y aceptables para que las naciones alcancen su interés nacional. A la par de aceptar que la detonación de estos puede estar justificada en una causa a fin a los intereses del Estado-Nación, o con base a una norma moral y ética internacional que exige una acción de disuasión. Ante lo cual, cada país es libre de proceder con base a sus intereses y capacidades que detenta. En última instancia, se expresa que el único paradigma con el cuál el realismo parece tener una clara divergencia es el liberalismo. No obstante, si bien no hay esferas de articulación tan estrechos como los que existen con el constructivismo y la Teoría de la Guerra, estos se dan al aceptar la existencia de una estructura del sistema internacional delimitado por la interacción de los actores que desemboca en el establecimiento de problemáticas y amenazas globales y regionales.

2. Constructivismo: en el plano del modelo de análisis para el abordaje de la política exterior que maneja la presente investigación destaca que tanto este paradigma, como la Teoría de la Guerra son capaces de tejer puentes con las otras tres propuestas teóricas seleccionadas.

También, es importante destacar que el constructivismo representa el marco analítico más flexible a razón de que su propuesta intersubjetiva para abordar los femémonos y sucesos internacionales, permite identificar el proceso histórico contextual de manera más amplia que permite entender desde la identidad de un Estado-Nación, a la vocación de un organismo internacional o de un proceso de integración, hasta los fines y objetivos de un tratado internacional o las causas y determinantes socio históricas y culturales que explican un conflicto prolongado en el sistema internacional. Lo que lo acopla a paradigmas como el realista, liberal y a Teoría de la Guerra, a la par de servir de instrumento reforzador de sus supuestos.

3. Paradigma liberal: como se mencionó anteriormente, el liberalismo es un enfoque que presenta claras divergencias y antagonismos con el realismo, en la comprensión y análisis de la política internacional. Esto se da a razón de que su visión cimentada en el multilateralismo y la cooperación, en la lógica de la diplomacia, se ha trasformado en una perspectiva vinculada a la construcción de instituciones internacionales que buscan regular el actuar de los Estados-Nación, con base a normas y tratados cimentados en el derecho internacional. Visión que es claramente contraria a la búsqueda de los intereses particulares y la anarquía global clave dentro de la comprensión realista. Por otra parte, es importante destacar que este paradigma juega un papel de trascendencia al abrir espacios para empresas trasnacionales, organismos internacionales y Organizaciones No Gubernamentales. Del mismo modo, en el liberalismo caben las protestas y acciones de pequeños grupos e individuos, que en muchas ocasiones no alcanzan el grado de institucionalidad de los Estados-Nación o grupos señalados. Por último, destaca que dentro de este paradigma fenómenos como la globalización y sus consecuencias en ámbitos como la economía y la cultura son unidades clave en el análisis de la política internacional.

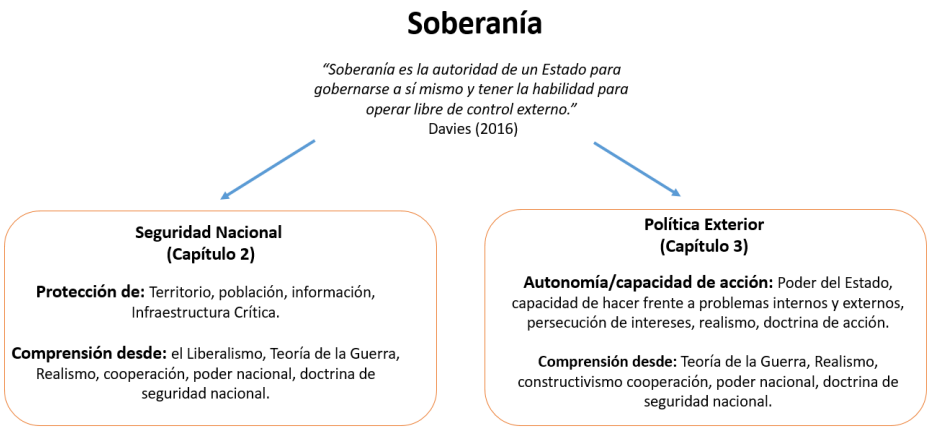
4. Teoría de la Guerra: La Teoría de la Guerra tiene una interpenetración, al igual que el constructivismo, con los otros tres paradigmas señalados. En este sentido, podemos expresar que, dentro del núcleo más duro de este esquema de análisis, vinculado al realismo prescriptivo, los vínculos son cercanos con el paradigma realista al empalmarse aspectos con garantizar la supervivencia del Estado-Nación como fin último y central, así como utilizar el conflicto como una vía para asegurar el interés nacional de los Estados-Nación. En este cruce,

se tejen puentes con el constructivismo, a razón de que es necesario identificar cómo se entiende y ve a sí mismo cada país a través de la construcción de su identidad y capacidades en la política internacional. Por otra parte, el núcleo suave de la Teoría de la Guerra se inter penetra con la Teoría de la Guerra Justa, dado que está visión institucionalista en torno del conflicto se ajusta a los preceptos que están en el marco de las leyes y acuerdos internacionales. Del mismo modo, al considerar que los conflictos entre los Estados-Nación, sólo acontecen cuándo se han agotado todos los medios y los países sólo entran en ellos cuándo se quiere alcanzar un bien que beneficie a toda la comunidad internacional y esté ajustados a la moral y ética imperante en el contexto global.

3.4 Puntos de encuentro entre la soberanía y política exterior

En el capítulo anterior, en la sección *2.4 Puntos de encuentro en la soberanía y seguridad nacional* presentamos la figura 8 que tejía los nexos entre soberanía, seguridad nacional y política exterior. Del mismo modo, en ese mismo diagrama, se adelantó la estructura del análisis que se vincularía en el capítulo dos al abordar la tríada de soberanía, seguridad nacional y ciberseguridad. Mientras que el capítulo tres, que ahora nos ocupa, centra su análisis en la soberanía, política exterior y ciberseguridad. De esta forma, al observar de nuevo la figura 8, se expresa que en este punto podemos completar el modelo de análisis al tejer los vínculos entre las tres categorías. Dado que el abordaje teórico del capítulo dos y el realizado hasta el momento en el presente nos permiten marcar de forma clara los vínculos entre los tres conceptos.

Figura 8. Nexos entre soberanía, seguridad nacional y ciberseguridad.



Fuente: Elaboración propia.

Para ejemplificar esto utilizamos la figura 25 que representa el modelo de operación entre el Estado Nación, su soberanía, la política exterior y la seguridad nacional en el marco del contexto internacional. En dicho diagrama se presenta al Estado-Nación como una unidad (marcada en una esfera roja). En ese sentido, se expresa que, a nivel interno, el Estado-Nación tienen una meta principal, que representa su supervivencia como país. Vinculado a esta dimensión, se encuentra la seguridad nacional (marcado en una esfera azul) que se interrelaciona con los tres principales componentes que emanan de la soberanía: la integridad territorial, la responsabilidad de proteger y la protección de las instituciones y los valores político-culturales del Estado-Nación.

Figura 25. Modelo de análisis de puntos de entre la soberanía, política exterior y ciberseguridad

Fuente: Elaboración propia.

Con relación a lo anterior, se expresa que los elementos citados son detonadores que sirven para garantizar el fin último de la seguridad nacional: la sobrevivencia del Estado-Nación. Sin embargo, cuándo esta meta está por demás cubierta, es que los países utilizan los mismos impulsos y elementos para la construcción del interés nacional. El interés nacional, se materializará en los hechos con las acciones de política exterior que realicen los diferentes países y como se interrelacionan con otros actores. Estos pueden corresponder al caso de organismos internacionales, otros Estados-Nación, empresas trasnacionales, amenazas a

regiones o de carácter internacional, Organizaciones No Gubernamentales, e individuos y grupos organizados de menor jerarquía. De esta forma, las flechas azules representan las acciones de política exterior, basadas en el interés nacional de los Estados, para alcanzar sus metas en el contexto internacional. Por último, se expresa que los óvalos marcados en amarillo y verde expresan dinámicas que pueden vincularse a los esquemas teóricos presentados en secciones anteriores. Como la lucha por el poder global, tema central del paradigma neorrealista, y la globalización económica, eje importante en el análisis liberal. Con lo cual podemos por fin delimitar los tres puntos de encuentro entre los conceptos, para nuestro modelo de análisis en la dimensión de la soberanía, seguridad nacional y política exterior.

3.4.1 El papel de la ciberseguridad en la política exterior

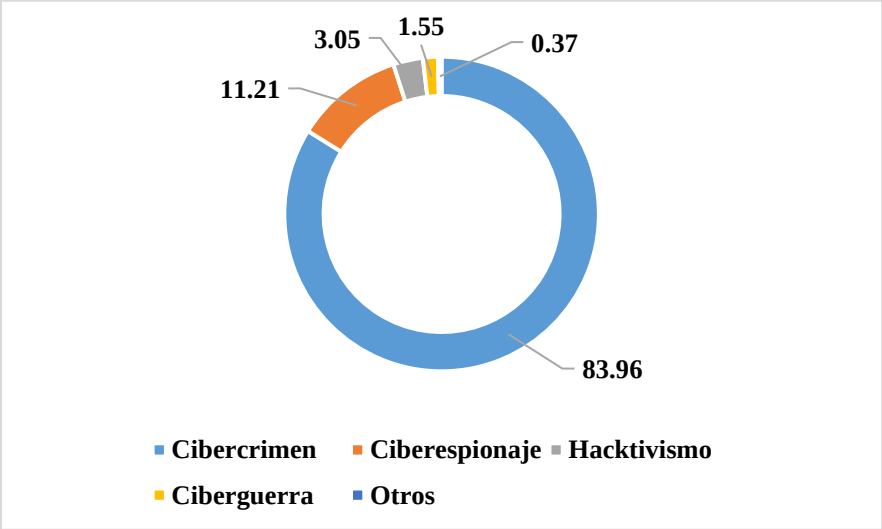
La ciberseguridad es un tema central de la política internacional y la política exterior desde finales del siglo XX, y con fuertes repercusiones en las acciones globales de los Estados Nación durante el siglo XXI. Como se abordó en capítulos anteriores, desde la popularización, democratización y normalización en la vida cotidiana del internet, a finales de la década de los noventa del siglo XX, pasando por hechos como el ciberataque de Tallin, Estonia (2007), hasta el reciente ciberataque a 18,000 agencias gubernamentales (Sahuquillo, 2020) y empresas detectado por el gobierno de los Estados Unidos, en diciembre de 2020, este campo se ha transformado en una nueva arena de influencia, confrontación y lucha de los Estados-Nación y actores de las relaciones internacionales.

En ese sentido, es un hecho lo expresado por Kello (2013) al citar que el ciberespacio se ha transformado en un dominio que, replanteó la lógica de los conflictos en el siglo XXI, dado que este nuevo campo es utilizado como un instrumento vital para la consolidación del poder nacional en el concierto de las potencias globales y el peso de las regiones en la geopolítica internacional. Asimismo, para el caso concreto de los Estados-Nación, la necesidad de crear una política nacional de ciberseguridad y una Estrategia Nacional de Ciberseguridad (ENSC) se transformó desde inicios de siglo en un aspecto clave para garantizar el poder nacional y en consecuencia el interés nacional de los países alrededor del mundo, (Klimburg, 2012).

En los hechos, esto se refleja en lo presentado por la biblioteca digital del Centro de Excelencia de la Ciberdefensa Cooperativa (CCDCOE), de la OTAN, en el que un total de 77 naciones del mundo ha creado documentos vinculados al tema de la ciberseguridad con un enfoque centrado en la política exterior del Estado-Nación, entre las que se incluyen miembros de la OTAN, aliados estratégicos de esta alianza, así como múltiples países de África, América Latina, el Caribe, Asía y Oceanía (CCDCOE Tallin, 2021).

Lo anterior, ejemplifica como gran cantidad de naciones han dado prioridad a la ciberseguridad en el ámbito de la política exterior. A nivel regional o de alianzas estratégicas, destaca lo realizado por las naciones miembros de la OTAN y la Unión Europea, que han priorizado la securitización del ciberespacio. Mientras que otras regiones como América Latina y en menor medida Asía han abordado el tema de ciberseguridad, con un énfasis más especializado en el ámbito privado, individual y penal. La inclusión de la ciberseguridad como una parte trascendental de la política exterior se da en un contexto adverso y cambiante de amenazas provenientes del ciberespacio. En relación con esto el sitio Hackmageddon (2020), centrado en la documentación de ciber incidentes o ataques de trascendencia para gobiernos y empresas, registró un total de 1,802 eventos en 2020, que involucraron a TIC´s, e infraestructuras nacionales críticas de múltiples países, como se muestra en la figura 26.

Figura 26. Motivaciones de ciber incidentes 2020.



Fuente Hackmageddon (2020).

En este contexto, AON (2019) expresa que los gobiernos alrededor del mundo ejercieron aproximadamente un trillón de dólares en gastos de ciber defensa en 2019, dónde los más afectados fueron los sectores industriales y las actividades económicas vinculadas al internet o servicios digitales, que enfrentaron fuertes pérdidas y riesgos, dado que los gobiernos nacionales no priorizaron la ciberseguridad vinculada a estándares internacionales en la materia. Sobre este dato la *Encuesta de Percepción de Riesgo Cibernético Global*, de la empresa Microsoft, expresó que sólo 28% de las empresas mundiales líderes en TIC´s consideran adecuadas las regulaciones o leyes gubernamentales para mejorar la ciberseguridad de cada país. A la par, que las entidades privadas y gubernamentales consideraron en 2019 que el principal riesgo percibido en el ciberespacio son las ciber amenazas (46%), con el potencial de infringir daños a una nación en esferas como la incertidumbre económica, daño industrial, actividad criminal, fraude, etc. (Kapersky, 2020), esferas de impacto en la política regional e internacional, como se muestra en la Figura 27.

Figura 27. Seguridad en TIC´s y riesgos percibidos en el ciberespacio.

Fuente: Kapersky (2020).

Dicho contexto representa un reto para gran cantidad de países, por el gasto y necesidad de creación de capacidades para enfrentar riesgos y amenazas provenientes del ciberespacio. Del mismo modo, para la construcción de su ciber poder, que le permita tener las habilidades mínimas de operación dentro del ciber dominio para perseguir sus intereses particulares. En

ese sentido, el portal Cybersecurity Ventures (2020) expresa que desde 2004, el mercado global de ciberseguridad pasó de los 3,500 a los 120,000 millones de dólares en 2017, con lo cual creció 35 veces a su tamaño original en dicho periodo y se prevé que el gasto mundial en productos y servicios de ciberseguridad por parte de los Estados-Nación supere los mil millones de dólares de forma acumulativa durante el período de 2017-2021. Con lo cual se anticipa un crecimiento del 12 al 15 por ciento años tras año hasta el 2025. Lo que implica una gran cantidad de gasto por parte de gobiernos nacionales y la creación de alianzas con empresas líderes en software y creación de esquemas de ciberseguridad.

Por otra parte, en los hechos organismos internacionales y regionales también han creado esfuerzos para la colaboración internacional, de los cuales destacan tres importantes que son:

1) el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, creado en 2001 por el Consejo de Europa, con la activa participación de múltiples Estados involucrados. Su principal objetivo se centra en combatir la comisión de delitos informáticos y al día de hoy es el único tratado internacional vinculante en la materia, que constituye una guía y modelo para que los países del mundo implementen dentro de su ordenamiento jurídico nacional la legislación pertinente para investigar y perseguir penalmente delitos cometidos en contra de sistemas o medios informáticos o mediante del internet, a la par de promover la cooperación internacional en contra ciber delitos. Es importante mencionar que este acuerdo ha dado un liderazgo a la Unión Europea en la materia y en política internacional, dado que el convenio está abierto para su ratificación por Estados-Nación que no sean parte del Consejo de Europa. En los hechos, y derivado del incremento de los delitos informáticos en las dos últimas décadas, se ha incrementado considerablemente la ciberdelincuencia en la esfera nacional e internacional. Por lo cual, también ha aumentado la presión global para que gran cantidad de los países del mundo se adhieran al tratado.

2) En segunda instancia, es importante señalar el trabajo de la Unión Internacional de Telecomunicaciones (ITU), que, en 2007, lanzó la Agenda sobre Ciberseguridad Global con el fin de promover la cooperación internacional para mejorar la seguridad y la confianza en la sociedad de la información. Este documento representa un importante esfuerzo global para consolidar un marco de cooperación internacional destinado a

aumentar la confianza y la seguridad en la sociedad de la información con un enfoque integral que agrupará a los gobiernos, iniciativa privada, y sociedad civil. La GCA está diseñada para promover la cooperación y la eficiencia, fomentando la colaboración entre todos los países para garantizar la seguridad en el dominio del ciberespacio, y también representa un conjunto de estándares y buenas prácticas internacionales en materia de ciberseguridad, divididos en cinco pilares estratégicos: medidas legales, medidas técnicas y de procedimiento, estructuras organizacionales, creación de capacidad y cooperación internacional, y que fueron presentados con mayor detalle en la sección anterior.

3) Por último, se encuentra el *National Cybersecurity Index* (NCSI), de la *E- Governance Academy*, que a través de una metodología de doce indicadores[22] integra un marco de análisis de buenas prácticas y estándares internacionales que detentan los países en materia de ciberseguridad. Por lo cual también enmarcan esfuerzos globales de ciberseguridad en la materia en el ámbito de la política exterior. En ese sentido se expresa que, del total de los doce indicadores del NCSI (2018), se considera que un total de ocho están estrechamente vinculados a temas de ciber poder, como parte del desarrollo de capacidades en el ciberespacio, así como con la seguridad nacional y política exterior del Estado-Nación. Mientras otros se refieren a otras esferas políticas como educación digital, seguridad pública, y servicios digitales de gobierno, como se muestra en la tabla 10.

Tabla 10. Indicadores y esferas de influencia del NCSI (2019).

No.	Indicador	Esfera de influencia
1	**Desarrollo de Política**	Seguridad Nacional y Política Exterior
2	**Delimitación de amenazas**	Seguridad Nacional
3	**Desarrollo de Educación**	Educación Digital
4	**Contribución Global**	Política Exterior
5	**Protección Servicios Digitales**	Seguridad Pública
6	**Protección Servicios Esenciales**	Seguridad Nacional

[22] Los indicadores son: 1) desarrollo de política de seguridad cibernética, 2) delimitación de amenazas en el ciberespacio, 3) educación y formación de especialistas capacitados en ciberseguridad y concientización de la población, 4) aportación de cada país para mejorar el contexto global de ciberseguridad, 5) nivel de desarrollo digital del país, 6) protección de servicios esenciales por el Estado Infraestructura Nacional Crítica, 7) servicios digitales y confidencialidad en la vida diaria. 8) Protección de datos y garantía de privacidad, 9) respuesta a ciber incidentes por parte de equipos de emergencia informática (CSIRT o CERT) ante ciber incidentes, 10) capacidad para administrar una crisis cibernética del Estado-Nación, 11) grado de compromiso del Estado para luchar contra el ciber crimen, 12) capacidad de operaciones militares de las fuerzas armadas en el ciberespacio. Y fueron descritos a detalle en el capítulo 2.

No.	Indicador	Esfera de influencia
7	**Identificación electrónica y confianza digital**	Servicios Digitales de Gobierno
8	**Protección Personal de Datos**	Servicios Digitales de Gobierno
9	**Desarrollo de CIRC**	Seguridad Nacional y Política Exterior
10	**Administración de Crisis**	Seguridad Nacional y Política Exterior
11	**Política contra Ciber crimen**	Seguridad Nacional y Política Exterior
12	**Operaciones Militares en el ciberespacio**	Seguridad Nacional y Política Exterior

Fuente: Aguilar (2021).

En ese sentido, se destaca que dichos indicadores son susceptibles de ser utilizados para realizar un diagnóstico a detalle de los entornos regionales de ciberseguridad de las alianzas y regiones del mundo. Aspecto que será crucial para entender su ciber poder con relación a sus capacidades de acción para alcanzar sus objetivos en el ciberespacio, asunto que se aborda en la siguiente sección.

3.5 Capacidades de acción, estrategia y búsqueda del interés nacional en el ciberespacio

Como se mencionó anteriormente, la AGC de la ITU, a través del *Índice Global de Ciberseguridad* (GCI), y el *Índice Nacional de Ciberseguridad* o (NCSI), representan un conjunto de métricas a través de los cuales se puede analizas las capacidades en materia de ciberseguridad de los diferentes países y regiones del mundo. Esto se da a razón de que cada medición presenta las áreas de oportunidad y de mejora de las legislaciones nacionales contra ciber crimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT), con el fin de mejorar las ciber capacidades de los países evaluados para garantizar su seguridad nacional y perseguir los intereses de su política exterior. En sí, tanto el GCI (2019) y el NCSI (2018) sirven para brindar un diagnóstico en torno al ciberpoder que detentan los países del mundo en materia de ciberseguridad. Asimismo, sirven para mostrar las asimetrías y la brecha en el desarrollo de ciber capacidades entre regiones como América Latina, África y Medio Oriente, y países que han priorizado el desarrollo de la ciberseguridad como las naciones de la OTAN.

Para conocer el panorama regional y global en torno al desarrollo de ciber capacidades por parte de los países del mundo, se recurrió al análisis regional tanto del GCI (2021) como del

NCSI (2018) para obtener un panorama de las capacidades de cada región alrededor del mundo. Para fines de nuestro análisis, y observar la posición que ocupan en el contexto internacional, se agruparon el total de naciones incluidas en el GCI en ocho diferentes subconjuntos, que son: 1) Países miembros de la OTAN, 2) Aliados estratégicos de la OTAN[23], 3) Resto de Europa, 4) Asía, 5) Medio Oriente, 6) América Latina, 7) África, 8) Oceanía. En este punto es importante destacar que cada métrica corresponde a un total diferente de países, por lo cual se presenta el análisis por separado del GCI (2019) y del NSCI (2021).

3.5.1 Índice Global de Ciberseguridad (GCI) 2018

Para el caso del GCI (2019) es importante destacar que este índice abarca un total de 194 países, los cuales separados en los conjuntos representan:

1) *Países miembros de la OTAN*: Estados Unidos, Canadá, Turquía, Francia, Alemania, Estonia, Eslovaquia, Lituania, España, Reino Unido, Suiza, República Checa, Letonia, Portugal, Bélgica, Polonia, Países Bajos, Italia, Noruega, Hungría, Luxemburgo, Grecia, Dinamarca, Islandia, Eslovenia, Croacia, Albania, Bulgaria, Montenegro y República de Macedonia del Norte.

2) *Aliados estratégicos de la OTAN:* Australia, Egipto, Israel, Japón, Jordán, Nueva Zelanda, Argentina, Filipinas, Marruecos, Pakistán, Afganistán, Corea del Sur, Bahréin y Tailandia.

3) *Resto de Europa*: Finlandia, Serbia, Georgia, Federación Rusa, Suecia, Ucrania, Bielorrusia, Rumania, Moldavia, República de Malta, Irlanda, Chipre, Mónaco, Noruega, Austria, Liechtenstein, Bosnia y Herzegovina, Vaticano, Andorra y San Marino

4) *Asía:* Turkmenistán, Singapur, Malasia, China, Kazajistán, Indonesia, India, Vietnam, Uzbekistán, Azerbaiyán, Brunei, Bangladesh, Armenia, Sri Lanka, Mongolia, Tayikistán, Nepal, Kirguistán, Laos, Myanmar, Camboya, Timor Leste, República Popular Democrática de Corea.

[23] Por aliados estratégicos se entiende a los 17 países considerados *Major non-NATO ally* o Aliado Importante no-OTAN, delimitación establecida por el Departamento de Estado de EUA y representa un conjunto de naciones que mantienen un trabajo conjunto con las Fuerzas Armadas de los Estados Unidos, pero no son miembros de la organización (US Deparment State, 2020).

5) *Medio Oriente:* Qatar, Omán, Túnez, Arabia Saudita, Argelia, Emiratos Árabes Unidos, Irán, Kuwait, Estado de Palestina, Irak, República Árabe Siria, Líbano, Yemen y Libia.

6) *América Latina:* Perú, Colombia, Chile, México, Argentina, Brasil, Jamaica, Panamá, Trinidad y Tobago, Surinam, Honduras, Uruguay, Paraguay, Cuba, Ecuador, Venezuela, Guatemala, Antigua y Barbuda, Costa Rica, Barbados, San Vicente y las granadinas, Bahamas, Bolivia, Guayana, Nicaragua, Belice, El Salvador, Granada, Santa Lucía, Dominica, Maldivas y República Dominicana.

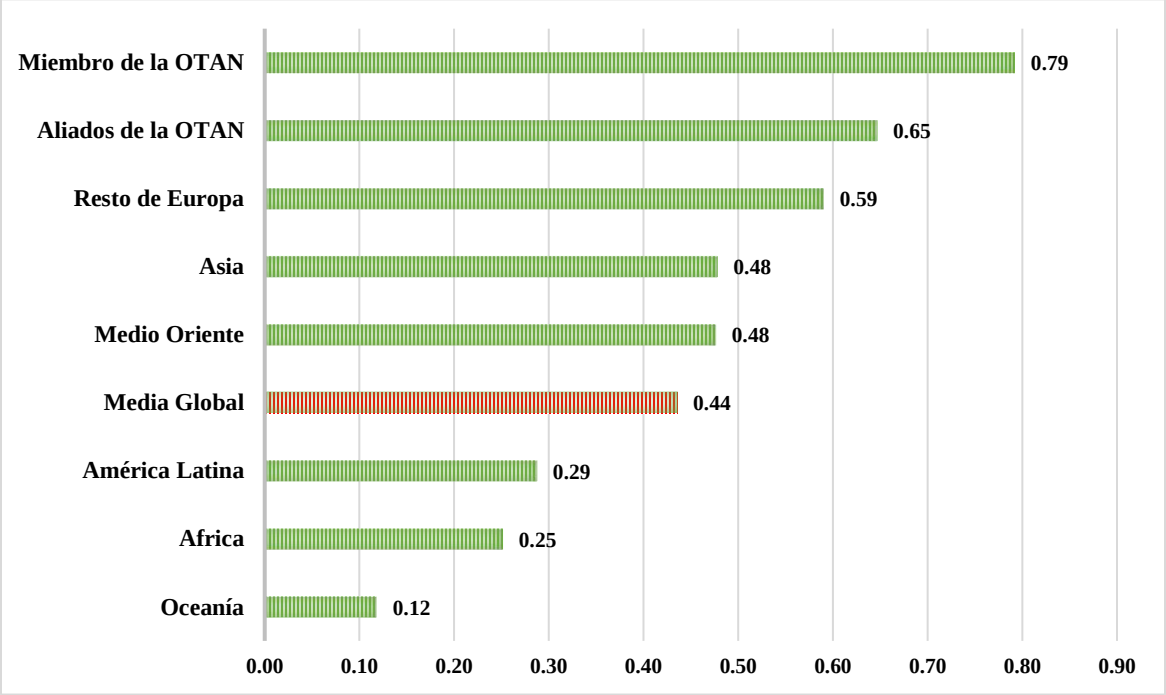
7) *África:* Mauricio, Kenia, Ruanda, Sudáfrica, Nigeria, Tanzania, Uganda, Benin, Costa de Marfil, Botswana, Ghana, Zambia, Camerún, Burkina Faso, Gabón, Senegal, Sudán, Gambia, Etiopía, Malawi, Seychelles, Tonga, Liberia, Madagascar, Guinea, Zimbabue, Bután, Congo, Mozambique, Sierra Leona, Eswatini, Namibia, Mauritania, Chad, Angola, Níger, Burundi, Togo, Mali, Somalia, Sudán del Sur, Santo Tomé y Príncipe, Djibouti, Guinea Bissau, Cabo Verde, Lesoto, República Centroafricana, Guinea Ecuatorial, Kiribati, Eritrea, Comoras y República Democrática del Congo.

8) *Oceanía:* Samoa, Fiyi, Papúa Nueva Guinea, Nauru, Vanuatu, Islas Marshall, Saint Kitts y Nevis, Islas Salomón, Tuvalu y Micronesia.

Con base en esta clasificación, se obtuvo el promedio del total de la calificación asignada a cada país respecto a la metodología del GCI (2018), que val 0 al 1. En la que el 0 representa una total ausencia de compromiso con la AGC, y el 1 un compromiso total. Al mismo tiempo, se calculó una media global, obtenida de la calificación de los 194 países del mundo, que se muestra en la Figura 28. En ella se puede observar, que el conjunto de naciones más aventajado en el desarrollo de ciber capacidades y comprometido con los cinco pilares de la AGC son los países miembros de la OTAN. Dado que los integrantes de dicha alianza ostentan una calificación en grupo de 0.79, ponderación que está por encima 0.35 de la media global del resto de las naciones del mundo. En segunda instancia, se observa que sigue el grupo conformado por sus aliados estratégicos (0.64), y en tercer puesto, el resto de los países de Europa (0.59). Respecto al caso de América Latina, destaca que la región se encuentra hasta la sexta posición, con una calificación de 0.28 (con un valor de 0.14 por debajo de la media global), para el caso de regiones como África se sitúan en la octava posición, 0.25.

Mientras que los países de Oceanía están en la última posición con una calificación de 0.11. A continuación se presenta un análisis por cada conjunto de países.

Figura 28. Media regional y grupos de países en el desarrollo de ciber capacidades según el GCI (2019).



Fuente: Elaboración propia con base en GCI (2019).

3.5.1.1 Naciones miembros de la OTAN

Un análisis centrado en las particularidades de cada conjunto de naciones nos presenta que, para el caso de las naciones miembros de la OTAN, del total de las treinta naciones incluidas en el GCI (2019) las cinco mejor posicionadas en dicha métrica son Reino Unido, Estados Unidos, Francia, Lituania y Estonia, todas con una ponderación por encima de la 0.90. Un aspecto de interés a destacar es el hecho, de que si bien como conjunto de naciones este grupo de Estados-Nación alcanzan el promedio más alto a nivel global.

Es importante mencionar que, en un escrutinio interno dentro de la organización, destaca que solo diez del total de los países se encuentran por encima del promedio de la organización. Mostrando que existen fuerte asimetrías dentro de la OTAN, dado que el rango de calificación entre el país con la nota más alta, Reino Unido (0.931), y el de la más baja, Islandia (0.449) es de 0.482. Lo que demuestra que hay prácticamente una diferencia de más

de 100% entre ambas naciones. Con los cuál se puede expresar de existir un marco de homologación y armonización entre el desarrollo de ciber capacidades, siguen existiendo fuertes asimetrías al interior de este conjunto de países, como se observa en el cuadro 11.

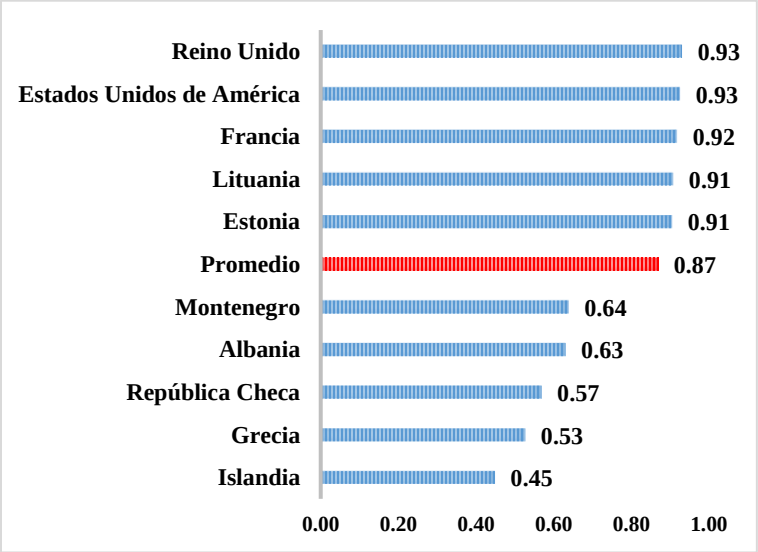
Tabla 11. Ponderaciones de países miembros de la OTAN según el GCI (2019).

No.	País	Calificación
1	Reino Unido	0.931
2	Estados Unidos	0.926
3	France	0.918
4	Lituania	0.908
5	Estonia	0.905
6	España	0.896
7	Canadá	0.892
8	Noruega	0.892
9	Luxemburgo	0.886
10	Países Bajos	0.885
Promedio		**0.869**
11	Turquía	0.853
12	Dinamarca	0.852
13	Alemania	0.849
14	Croacia	0.840
15	Italia	0.837
16	Polonia	0.815
17	Bélgica	0.814
18	Hungría	0.812
19	República de Macedonia del Norte	0.800
20	Suiza	0.788
21	Portugal	0.758
22	Letonia	0.748
23	Eslovaquia	0.729
24	Bulgaria	0.721
25	Eslovenia	0.701
26	Montenegro	0.639
27	Albania	0.631
28	República Checa	0.569
29	Grecia	0.527
30	Islandia	0.449

Fuente: Elaboración propia con base al GCI (2019).

Del mismo modo, es importante mencionar que estas asimetrías son más visibles cuándo se comparan los cinco países con las calificaciones más altas dentro de esta métrica, contra los cinco peor evaluados. Mostrando la divergencia y alta variabilidad en el desarrollo de ciber capacidades de los países integrantes de la OTAN. Cómo se observa en la figura 29.

Figura 29. Cinco países mejor y peor evaluados de naciones miembros de la OTAN según GCI (2019).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.2 Aliados estratégicos de la OTAN

El segundo grupo mejor evaluado se centra en las naciones consideradas aliados estratégicos de la OTAN, el primer aspecto a considerar sobre este conjunto de naciones, como se mencionó en una nota de página anterior, corresponde al hecho de que está clasificación se basa en la denominación *Major non-NATO ally* o Aliado Importante no-OTAN, establecida por el US Deparment State (2020). En este punto se destaca que, del total de 17 naciones citadas en dicho documento, el GCI (2019) sólo presenta información de un total de 14, las cuales son consideradas en esta clasificación.

En segunda instancia, se resalta que este conjunto de naciones, detentan un promedio 0.14 menor al de las naciones miembros de la OTAN. Sin embargo, se destaca que países como Australia, Japón y Corea del Sur detentan calificaciones que podrían equipararse a las diez naciones de la OTAN por encima de la media en el desarrollo de sus ciber capacidades según el GCI (2019). Del mismo modo, el rango entre el valor con la calificación más alta y baja

de este conjunto de naciones presenta una diferencia de 0.713, mostrando claras diferencias y debilidades entre los países por encima de la media y los que son considerados aliados estratégicos en la región del Medio Oriente y el Magreb.

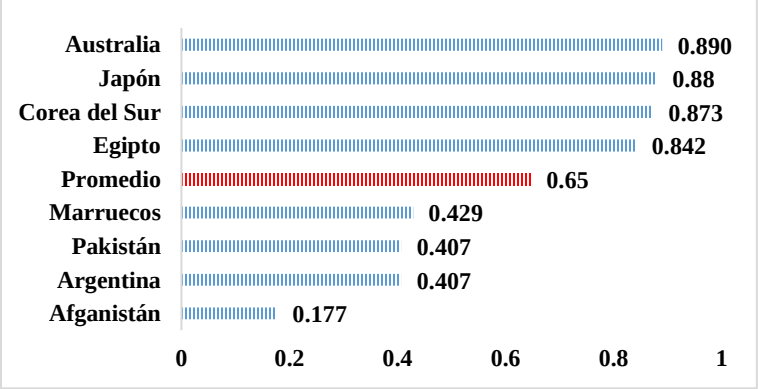
Tabla 12. Ponderaciones de países aliados de la OTAN según el GCI (2019).

No.	País	Calificación
1	Australia	0.89
2	Japón	0.88
3	Corea del Sur	0.873
4	Egipto	0.842
5	Tailandia	0.796
6	Nueva Zelanda	0.789
7	Israel	0.783
8	Filipinas	0.643
Promedio		**0.65**
9	Bahreín	0.585
10	Jordania	0.556
11	Marruecos	0.429
12	Argentina	0.407
13	Pakistán	0.407
14	Afganistán	0.177

Fuente: Elaboración propia con base al GCI (2019).

Por último, del mismo modo que en la sección anterior, la información en un gráfico de barras, visible en la figura 30, en la que se demuestran que, a ambos grupos a pesar de estar posicionados con un fuerte compromiso con la establecido por la AGC de la ITU, muestran fuertes heterogeneidades a su interior.

Figura 28. Cuatro países mejor y peor evaluados de naciones aliadas de la OTAN según GCI (2019).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.3 Resto de Europa

En el caso de los países del centro de Europa destacan el conjunto de naciones que tienen una membresía dentro de la Unión Europea, pero no son parte de la OTAN, tales como Austria, Suecia o Irlanda. En el marco de la comprensión de la AGC destaca el caso de la Federación Rusa, que detenta una calificación (0.836) debajo del promedio de las naciones de la OTAN (0.869).

Es importante señalar a este Estado-Nación, a razón de que a pesar de que su gobierno ha adquirido compromisos con la AGC, también es constantemente señalado como un actor que realiza ciber operaciones en naciones de Europa del Este como Estonia (Connell y Vogler 2017)., Georgia (Iasiello, 2017a), o Ucrania (Limnéll, 2015), e incluso en países de Europa y los Estados Unidos (Buchanan y Sulmeyer, 2016).

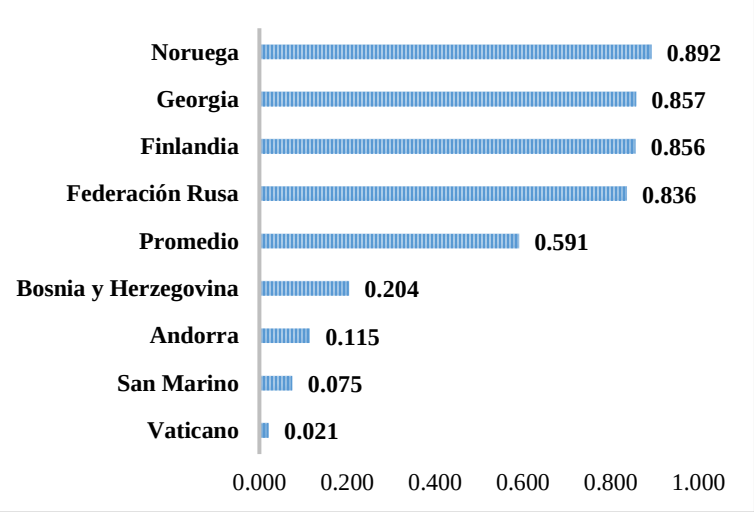
Tabla 13. Ponderaciones de resto de Europa según el GCI (2018).

No.	País	Calificación
1	Noruega	0.892
2	Georgia	0.857
3	Finlandia	0.856
4	Federación Rusa	0.836
5	Austria	0.826
6	Suecia	0.810
7	Irlanda	0.784
8	Mónaco	0.751
9	Moldavia	0.662
10	Ucrania	0.661
11	Chipre	0.652
12	Serbia	0.643
Promedio		**0.591**
13	Belorusia	0.578
14	Rumania	0.568
15	Liechtenstein	0.543
16	Malta	0.479
17	Bosnia y Herzegovina	0.204
18	Andorra	0.115
19	San Marino	0.075
20	Vaticano	0.021

Fuente: Elaboración propia con base al GCI (2019).

Con lo cual se demuestra que, por encima de iniciativas vinculadas a la cooperación internacional, utiliza más al ciberespacio como arena estratégica para alcanzar sus intereses nacionales a través de ciber poder. Por último, destaca en la figura 30 el nivel nulo de desarrollo de capacidades de microestados de Europa como Andorra (0.115), San Marino (0.075) y Vaticano (0.021).

Figura 30. Cuatro países mejor y peor evaluados de resto de Europa según GCI (2018).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.4 Asia

El continente asiático, al igual que las naciones del resto de Europa, presentan una clara variabilidad entre los países con un fuerte compromiso con la AGC y los estados con la menor ponderación dentro de la métrica, en la tabla 14 se puede observar esto.

Tabla 14. Ponderaciones de resto de Asia según el GCI (2018).

No.	País	Calificación
1	Singapur	0.898
2	Malaysia	0.893
3	China	0.828
4	Kazakstán	0.778
5	Indonesia	0.776
6	India	0.719
7	Vietnam	0.693
8	Uzbekistán	0.666
9	Azerbaiyán	0.653

No.	País	Calificación
10	Brunei	0.624
11	Bangladesh	0.525
12	Armenia	0.495
Promedio		**0.48**
13	Sri Lanka	0.466
14	Mongolia	0.465
15	Tayikistán	0.263
16	Nepal	0.26
17	Kirguizistán	0.254
18	Laos	0.195
19	Myanmar	0.172
20	Camboya	0.161
21	Turkmenistán	0.115
22	Timor Leste	0.082
23	República Democrática Corea del Norte	0.02

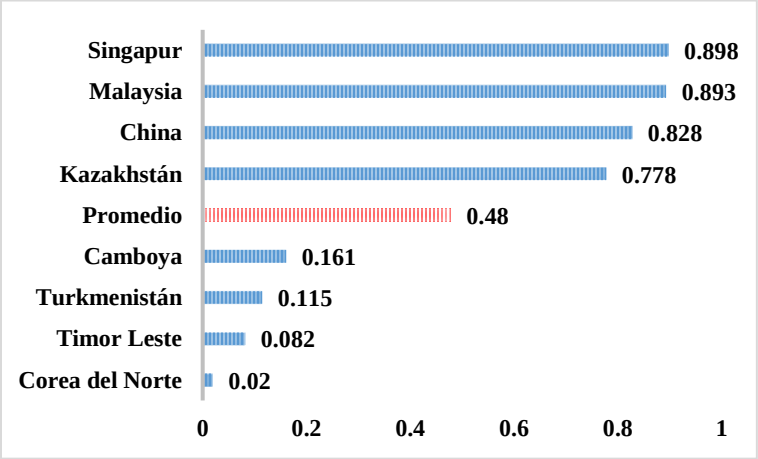
Fuente: Elaboración propia con base al GCI (2019).

En los primeros lugares destacan naciones como Singapur (0.898) y Malasia (0.893). A la par de países de importancia geopolítica en el sudeste asiático y Asía Central. Esta lógica corresponde a que el continente asiático se encuentra situado en una zona geográfica en el que se expresa existen múltiples naciones que ejercen fuertes esquemas de ciber poder y utilizan el dominio del ciberespacio para su alcanzar sus intereses nacionales.

En este continente se encuentran naciones que son reconocidas con alto potencial para operacionalizar ciber operaciones, tales como China (0.828), con una nota menor a las naciones de la OTAN y la Federación Rusa. Kazakstán (0.778), vinculada a un fuerte desarrollo de ciber capacidades por su pasado como exrepública soviética, en Asía Central, y la misma India (0.719), que al día de hoy es reconocida como una importante potencia en el desarrollo de software. En sí la condición geopolítica de estar ubicados entre dos grandes importantes actores del dominio del ciber espacio como Rusia y China, hacen a la región un espacio geográfico en el que los países deben avanzar constantemente en el desarrollo de sus defensas para la ciberseguridad. Asimismo, es de interés la ponderación de Corea del Norte, prácticamente evaluadas cero por parte de la AGC, y es considerado uno de los principales países que arman equipos de piratas y programadores informáticos para realizar ciber operaciones en contra de gobiernos y empresas de países con el fin de alcanzar objetivos

monetarios para el régimen socialista de Pyongyang. A pesar de esta condición, en la figura 31, correspondiente al comparativo de los cinco países con mejor y pero nota según e GCI, brilla el caso de países como Singapur (0.898) y Malaysia (0.893).

Figura 31. Cuatro países mejor y peor evaluados de resto de Asía a según GCI (2019).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.5 Medio Oriente

La región del Medio Oriente destaca por un fuerte posicionamiento de compromiso por parte de la AGC de parte de las naciones exportadoras de petróleo, con los casos de Arabia Saudita (0.881), Qatar (0.86) y Emiratos Árabes Unidos (0.807). En contraposición, a este grupo de países, destaca que las naciones involucradas a conflictos sociales internos, o reestructuración del régimen político, a causa primavera árabe y la Guerra Civil Siria, iniciada en 2011, prácticamente se encuentran en un claro y amplio rezago para construcción de una política nacional de ciberseguridad, o muchos menos, un grado de compromiso con la ACGS, como es visible con casos como Libia (0.206) o Siria (0.237). Condición para la cual la media de la región es un umbral efectivo en el que se ubican este conjunto de países.

Tabla 15. Ponderaciones del resto Medio Oriente según el GCI (2018).

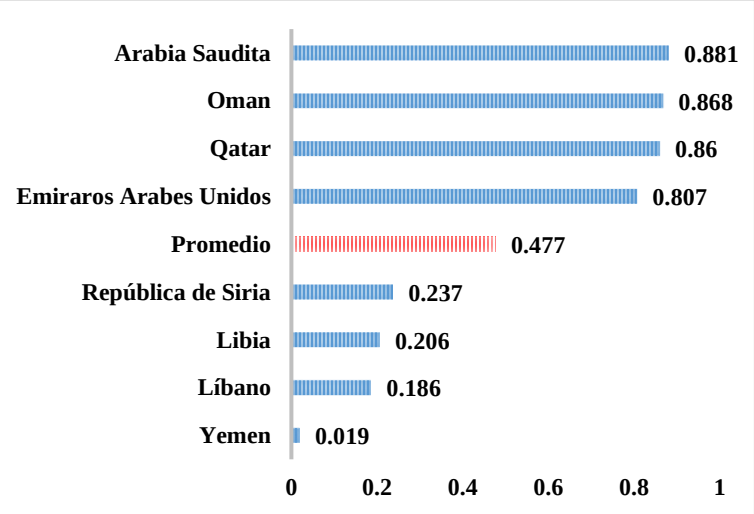
No.	País	Calificación
1	Arabia Saudita	0.881
2	Omán	0.868
3	Qatar	0.86
4	Emiratos Árabes Unidos	0.807
5	Irán	0.641
6	Kuwait	0.6

No.	País	Calificación
7	Túnez	0.536
Promedio		0.477
8	Palestina	0.307
9	Iraq	0.263
10	Argelia	0.262
11	República de Siria	0.237
12	Libia	0.206
13	Líbano	0.186
14	Yemen	0.019

Fuente: Elaboración propia con base al GCI (2019).

En ese sentido, el análisis entre los países mejor evaluados y los que están en las últimas posiciones de la región, es importante destacar, que aquellos asociados a la inestabilidad política y los conflictos regionales, con eventos que van desde la Guerra contra el Terrorismo, la Primavera Árabe y la Guerra Civil Siria, representan un conjunto de países con un severo rezago. El cual, junto a los microestados de Oceanía, están ubicados como el grupo de países con nivel mundial más bajo en el de sus ciber capacidades.

Figura 32. Cuatro países mejor y peor evaluados de resto de Medio Oriente según GCI (2018).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.6 América Latina

La región latinoamericana, representa el primer grupo de países que, de manera conjunta, posee una calificación promedio menor (0.288), a la media global del GCI (2019) situada en 0.44. Esta condición, la posiciona junto a África y los micros estados de Oceanía como los

tres grupos de países más rezagados en el contexto global con los compromisos de la AGC. A pesar de esto, destaca que la región al contrario de los casos señalados de países de la OTAN y resto de Europa, posee menos heterogeneidad como conjunto de naciones. A razón de que el país mejor posicionado en la región, en este caso Uruguay (0.681) se encuentra claramente alejado de la puntación más alta alcanzada por un conjunto de países (0.79). Lo anterior, se interrelaciona con el hecho, que, a diferencia de regiones como Medios Oriente, América Latina es una región con una mayor estabilidad política que le permite vincularse parcialmente con los compromisos de la AGC.

Esta condición, ha sido documentado a través de instrumentos como el informe *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*, que presentó que desde el 2012 los ciberataques a entidades o sitios de internet públicos y privados han crecido a cifras anuales de más del 61% lo que ha marcado un interés coordinado de los países en reforzar sus medidas de ciberseguridad ante dicho contexto internacional (OEA/Symantec 2014). A pesar de esto, es importante mencionar, que la región se ha transformado en un punto importante para realizar actividades ilícitas a través del ciberespacio, a razón de que países como Ecuador, Guatemala, Bolivia, Perú y Brasil se han encontrado dentro de los diez principales países que con más afectaciones por malware desde 2015. A la que los países más aventajados en el desarrollo de sus capacidades como el caso ya citado de Uruguay, Colombia (0.565) y Chile (0.470) presentaron cifras de infección por malware por encima de la media global situación que enmarcó a la región, junto a Asía, con las tasas más altas de virus maliciosos a nivel global (Aguilar-Antonio, 2019). También, se destaca que desde 2015 el uso del ciberespacio para realizar fraude bancario se ha transformado en un problema, dado que se estima que el 92% de las entidades financieras han presentado un ciber ataque, con una tasa de éxito del 37% (OEA, 2018).

Por su parte, Kaspersky Lab (2020) registró más de 746 mil ataques de malware diarios durante el 2020 en América Latina, lo que implica que se realizan 9 ciberataques de malware por segundo. A la par que se detectó que los tres principales países con mayor incidencia para el ciber crimen son Brasil (56.25%, del total de la región), México (22.81%) y Colombia (10.20%). Por otra parte, es importante señalar que, de un total de 62 millones de ataques detectados por esta firma durante el 2020, 66% se vinculaban a robo a entidades privadas y

comerciales, mientras 34% restante se vinculaban a actividades criminales, hacktivismo y ataques a sistemas gubernamentales.

Tabla 16. Ponderaciones de América Latina según el GCI (2018).

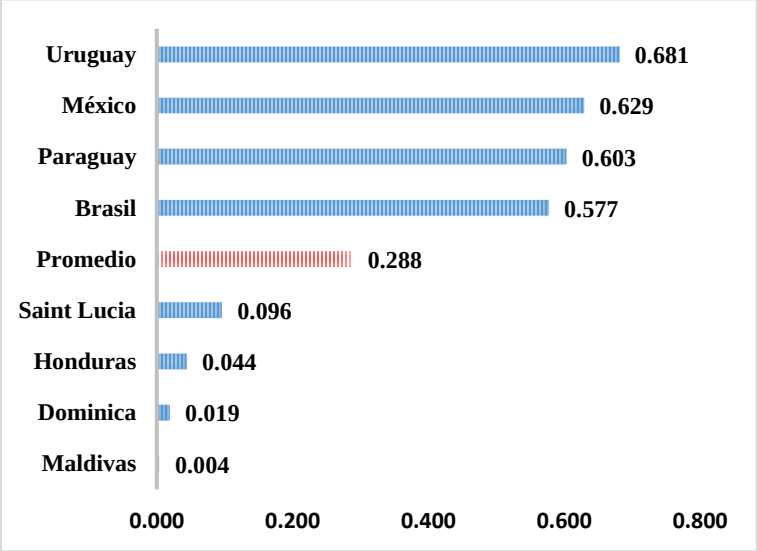
No.	País	Calificación
1	Uruguay	0.681
2	México	0.629
3	Paraguay	0.603
4	Brasil	0.577
5	Colombia	0.565
6	Cuba	0.481
7	Chile	0.470
8	República Dominicana	0.430
9	Argentina	0.407
10	Jamaica	0.407
11	Perú	0.401
12	Panamá	0.369
13	Ecuador	0.367
14	Venezuela	0.354
Promedio		**0.288**
15	Guatemala	0.251
16	Antigua and Barbuda	0.247
17	Costa Rica	0.221
18	Trinidad y Tobago	0.188
19	Barbados	0.173
20	Saint Vincent and the Grenadines	0.169
21	Bahamas	0.147
22	Granada	0.143
23	Bolivia	0.139
24	Guyana	0.132
25	Nicaragua	0.129
26	Belice	0.129
27	El Salvador	0.124
28	Surinam	0.110
29	Saint Lucia	0.096
30	Honduras	0.044
31	Dominica	0.019
32	Maldivas	0.004

Fuente: Elaboración propia con base al GCI (2019).

Al abordar, las ponderaciones de los países con las mejores notas, y los peor calificados según el GCI (2019). Se encuentra que la ausencia de desarrollo de capacidades cibernéticas puede interrelacionarse más a al tamaño de las naciones, con casos concretos como Santa Lucía, Dominica y Maldivas, que a la inestabilidad política poco presente en la región. Esta condición sólo aplicaría en es el ámbito latinoamericano a países del triángulo norte de Centroamérica.

Lo que demuestra un entorno complejo, en el que la mayoría de los países gozan de una relativa estabilidad política, a la par que su contexto regional de ciber amenazas les exige el desarrollo de capacidades para enfrentar dichos riesgos. No obstante, es claro que los países avanzan a pasos lentos que los han rezagado como grupo de países respecto a otras regiones del mundo. Del mismo modo, que ninguno de ellos, ha optado por dar un papel preponderante al desarrollo de ciber poder para posicionarse en la esfera global como una potencia regional en el dominio del ciberespacio.

Figura 33. Cuatro países mejor y peor evaluados de América Latina según GCI (2019).



Fuente: Elaboración propia con base al GCI (2019).

3.5.1.6 África

El contexto de África, región evaluada en el penúltimo lugar del GCI (2019), con una ponderación de 0.25, resalta en una particularidad contrastante, respecto a la condición de América Latina. Que es el hecho, de que al interior de este grupo de países si existen naciones con un nivel de desarrollo de capacidades semejante a las naciones integrantes de la OTAN.

Como es el caso de países como Mauricio (0.880) y Kenia (0.748). En ese sentido, es importante destacar que estos dos a países representan la dupla de países con el mayor nivel de desarrollo en temas de ciberseguridad de la región y el mayor nivel de penetración del internet respecto a su población, dado que en ambos países dicha cifra supera el 70% de la población, mientras que la media de África se encuentra situada en menos del 50% de población con acceso a internet (Johnson, 2021).

Con base a lo anterior, Kshetri (2019) expresa que se estima que para 2022, mil millones de personas en África tendrán acceso a internet, lo que representa un total promedio de 80% de su población, con lo cual este continente se transformará en la zona del planeta con reducción más vertiginosa de la brecha digital en el mundo. Esta condición, para implica fuertes riesgos para la ciberseguridad regional con base a la firma Serianu (2020) y su reporte *Africa Cybersecurity Report* que, al analizar la tendencia de los delitos cibernéticos en todos los países del continente, estima que los delitos cibernéticos han costado a las economías africanas 3.500 millones, desde 2017. En el cual, los principales afectados han sido Nigeria, con 649 millones de dólares, y Kenia, con 210 millones de dólares.

Sobre esto Symantec (2016) ha registrado 24 millones de incidentes de malware en África en el reporte *Cybercrime & cyber security trends in Africa*, a la par de que expresan que los ciber delitos estaba aumentando en África a un ritmo más rápido que en cualquier otra región del mundo. Y que gran cantidad de países se están volviendo atractivos para los ciber delincuentes, gracias al alto grado de digitalización de las actividades económicas que se está viviendo y acontecerá en los años de la presente década.

Tabla 17. Ponderaciones de África según el GCI (2019).

No.	País	Calificación
1	Mauricio	0.880
2	Kenia	0.748
3	Ruanda	0.697
4	Sudáfrica	0.652
5	Nigeria	0.650
6	Tanzania	0.642
7	Uganda	0.621
8	Benín	0.485
9	Costa de Marfil	0.456
10	Botswana	0.440

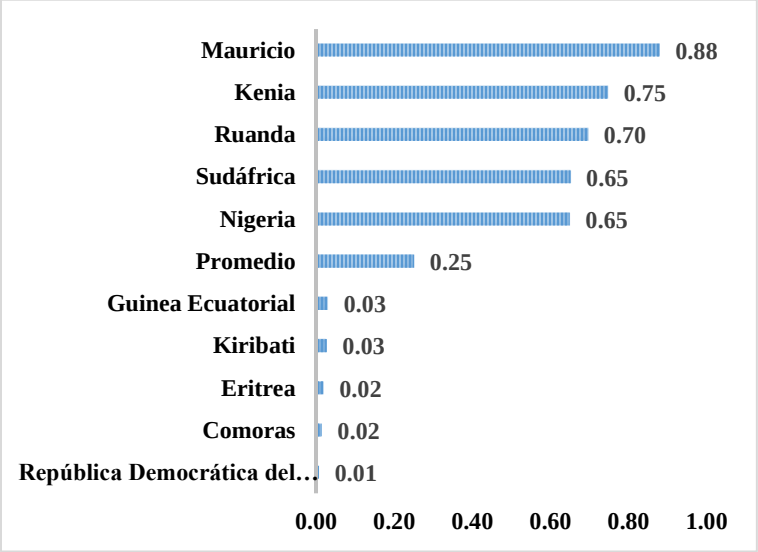
11	Ghana	0.437
12	Zambia	0.436
13	Camerún	0.432
14	Burkina Faso	0.400
15	Gabón	0.318
16	Senegal	0.305
17	Sudan	0.294
18	Gambia	0.280
19	Etiopia	0.278
20	Malawi	0.275
21	Seychelles	0.259
Promedio		**0.252**
22	Tonga	0.208
23	Liberia	0.206
24	Madagascar	0.196
25	Guinea	0.191
26	Zimbabue	0.186
27	Bután	0.181
28	Congo	0.167
29	Mozambique	0.158
30	Sierra Leone	0.138
31	Eswatini	0.133
32	Namibia	0.127
33	Mauritania	0.107
34	Chad	0.098
35	Angola	0.097
36	Níger	0.094
37	Burundi	0.087
38	Togo	0.087
39	Mali	0.085
40	Somalia	0.070
41	South Sudan	0.065
42	Sao Tome y Príncipe	0.064
43	Djibouti	0.063
44	Guinea Bissau	0.055
45	Cabo Verde	0.051
46	Lesoto	0.051
47	República Central Africana	0.036
48	Guinea Ecuatorial	0.031
49	Kiribati	0.028

50	Eritrea	0.020
51	Comoras	0.015
52	República Democrática del Congo	0.008

Fuente: Elaboración propia con base al GCI (2018).

Por último, el contraste de los países mejor evaluados y los que detentan las calificaciones más bajas con base al GCI (2019), presenta un panorama de amplia heterogeneidad que para Kshetri (2019), hacen a la región africana, la zona geográfica con los retos más adversos a concretar con base a la AGC. A razón de las adversidades económicas que enfrentan los países y el hecho que la ciberseguridad es una política no reconocida como una necesidad de la mayoría de los países africanos.

Figura 34. Cuatro países mejor y peor evaluados de África según GCI (2019).



Fuente: Elaboración propia con base al GCI (2018).

3.5.1.6 Oceanía

El conjunto de países de Oceanía está agrupado con un microestados e islas de dicho continente. Resalta que al ser países de pequeño tamaño son el conjunto de naciones más atrasado en el desarrollo de sus ciber capacidades. Del mismo, son el grupo con el menor grado de heterogeneidad con sus notas con base al GCI (2019).

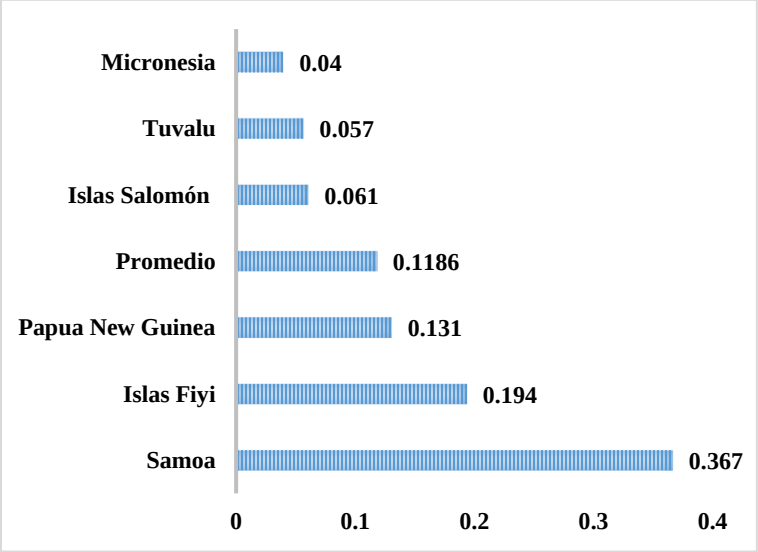
Tabla 18. Ponderaciones de Oceanía a según el GCI (2019).

No.	País	Calificación
1	Samoa	0.367
2	Islas Fiyi	0.194
3	Papua New Guinea	0.131
Promedio		**0.1186**
4	Nauru	0.101
5	Vanuatu	0.098
6	Islas Marshall	0.072
7	San Kits y Nevis	0.065
8	Islas Salomón	0.061
9	Tuvalu	0.057
10	Micronesia	0.04

Fuente: Elaboración propia con base al GCI (2018).

Al comparar las naciones más aventajadas, como Samoa (0.367) o Islas Fiyi (0.194), notamos que más que asociar aspectos como la inestabilidad política o el nivel de desarrollo, es el tamaño de los países como economías el aspecto que las hace no considerar importante el desarrollo de una política nacional de ciberseguridad.

Figura 29. Cuatro países mejor y peor evaluados de América Latina según GCI (2018).



Fuente: Elaboración propia con base al GCI (2018).

3.5.1.6 Cooperación internacional y asociaciones público-privadas según el GCI (2018)

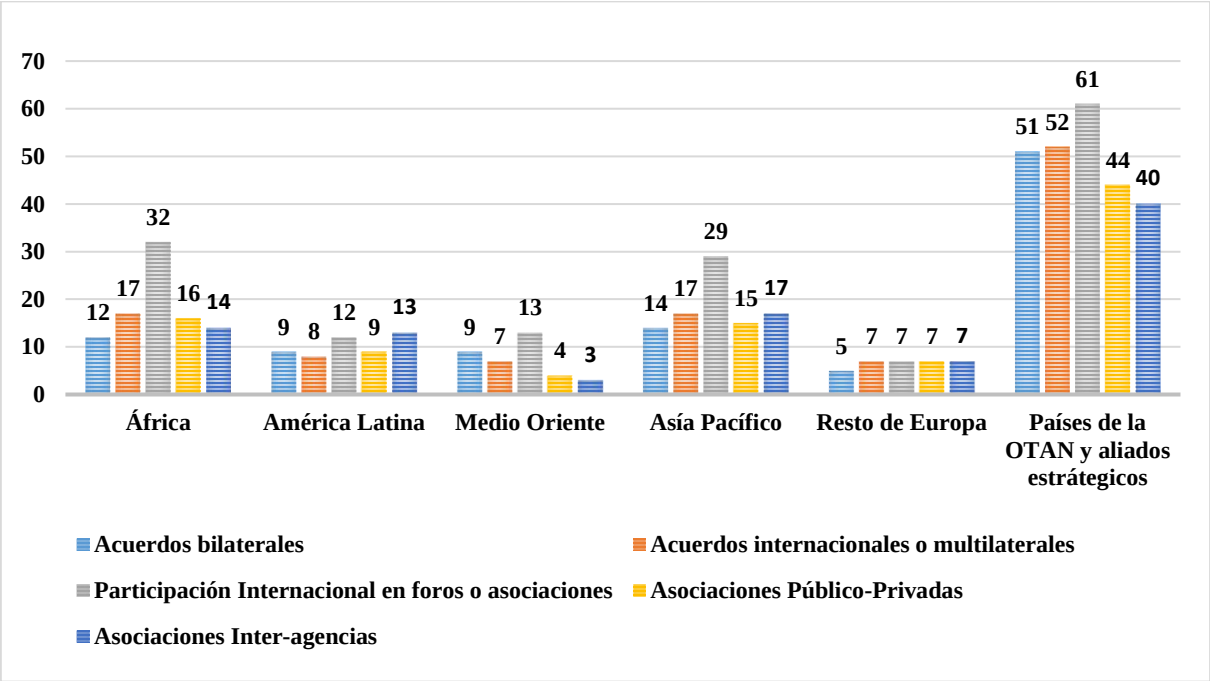
El análisis anterior, mostró el desarrollo de ciber capacidades por conjunto de naciones, agrupados al sumar el número de sus calificaciones individuales, y mostrar el promedio que detentan como grupo, con base al GCI (2018). No obstante, una variable de importancia para entender el mayor desarrollo capacidades en conjuntos regionales, o alianzas estratégicas, es el conocer el número total de asociaciones estratégicas púbico-privadas y acuerdos de cooperación internacional, de carácter bilateral y multilateral que detentan los diferentes tipos de países.

Este análisis es de interés, porque más allá de ajustarse a una visión realista, en torno a la persecución del interés y seguridad nacional por parte de los Estados-Nación. Nos acercaría a perspectivas como los paradigmas liberal y constructivista, que demuestran como las naciones, a través de los procesos de cooperación y características intersubjetivas asociados a su identidad, consolidan acuerdos en el plano regional o internacional para el desarrollo de capacidades cibernéticas y ciber poder.

En este sentido, se localizaron el total de acuerdos realizados en materia de ciberseguridad con base en la información del GCI (2019) y la biblioteca del CCD COE Tallin (2021), los cuales se presentan en la figura 35. Una vez más resalto la preponderancia de los países de la OTAN y sus aliados estratégicos con un total de 248 acuerdos o asociaciones estratégicas en materia de ciberseguridad.

No obstante, un dato de interés presentado en ese en la figura 35, es notar que, si bien África se presenta como uno de los países menos comprometidos con la AGC de la ITU, destaca su fuerte participación internacional en foros o asociaciones en materia de ciberseguridad (con un total de 61 registros) y su creciente firma de acuerdos bilaterales (12 casos) y asociaciones interagencial en la materia, con un total de (14 casos). Con lo cual aventaja a las regiones de Asía, América Latina y Medio Oriente, con lo cual demuestra que esta región, rezagada desde una su nivel de desarrollo de capacidades del GCI (2019), utiliza al multilateralismo con instrumento para la construcción de ciber poder.

Figura 35. Total de acuerdos y/o instrumentos de cooperación internacional por conjuntos de países.



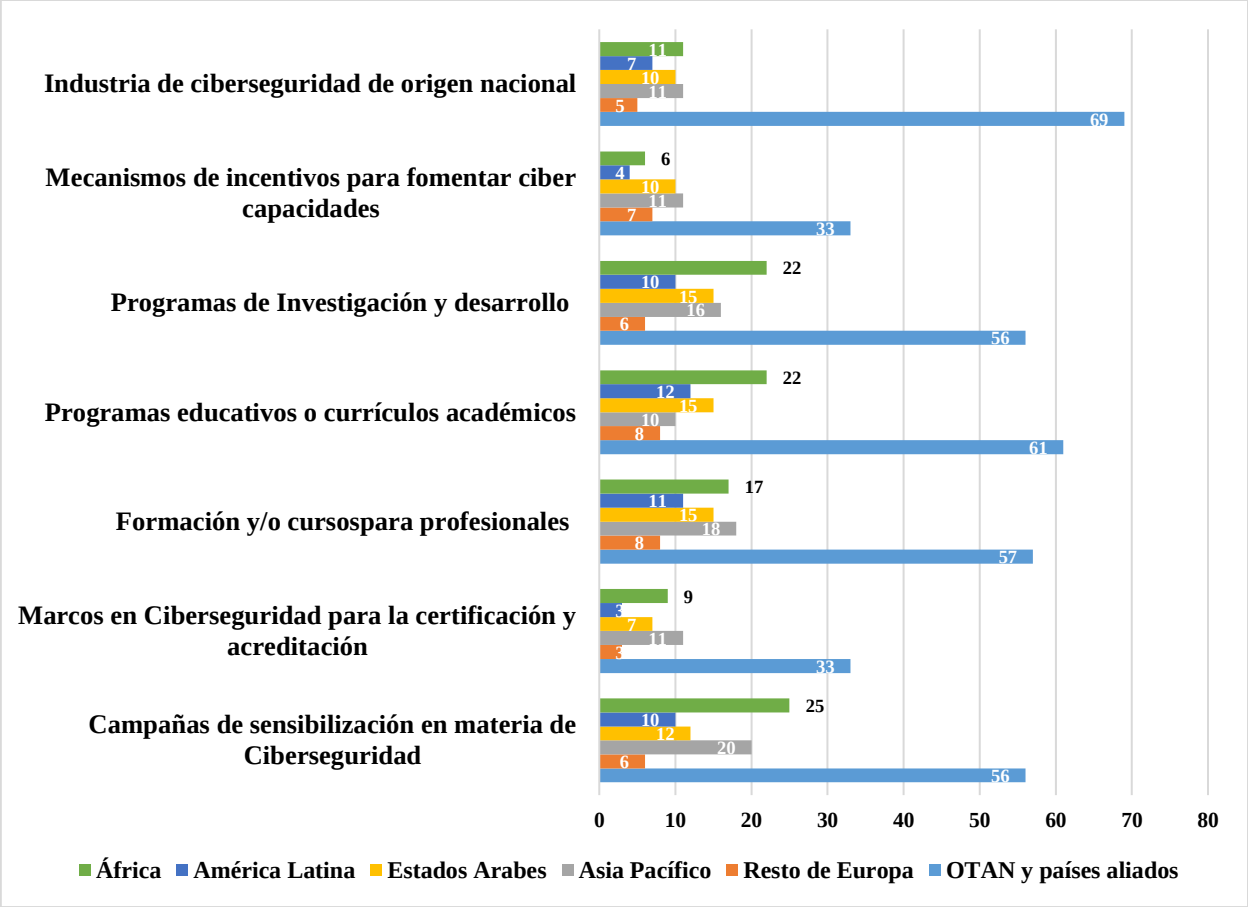
Fuente: Elaboración propia con base al GCI (2019) y CCDCOE Tallin (2021).

Por último, el GCI (2019) presenta igual un panorama estratégico con base a siete acciones clave en el desarrollo de ciber capacidades de los países para la construcción de ciber capacidades, con un enfoque integrador de partes interesadas, los cuales son: 1) campañas de sensibilización en materia de Ciberseguridad, 2) marcos en ciberseguridad para la certificación y acreditación, 3) formación y/o cursos para profesionales, 4) programas educativos o currículos académicos, 5) programas de investigación y desarrollo, 6) mecanismos de incentivos para fomentar ciber capacidades, y 7) industria de ciberseguridad de origen nacional.

Dichas acciones incluyen a actores gubernamentales, empresas y actores privados, así como a la sociedad civil y ciudadanía. En ese sentido, nuevamente se presenta una fuerte ventaja de los países integrantes de la OTAN y sus aliados. Del mismo modo, de un total de siete diferentes acciones clave considerada, destaca el tener industria nacional en materia de ciberseguridad, donde la OTAN y aliados alcanzan una cifra de 69 casos exitosos de empresas bien consolidados en el sector. Seguidos de las dimensiones de programas de educativos o académicos (con 61 casos) y programas de investigación y desarrollo (con 56 casos). De esta forma se presenta qué aspectos como tener empresas líderes en el desarrollo

informático y la creación de capital humano también son aspectos esenciales para la consolidación a nivel interno de ciberpoder por parte de los Estados-Nación.

Figura 36. Acciones clave en el desarrollo de ciber capacidades según el GCI (2019).



Fuente: Elaboración propia con base en GCI (2019).

3.5.2 National Cyber Security Index (2019)

Para el caso del NCSI (2018), de la *E-Governance Academy*, está métrica presenta información de un total de 98 países

1) *Países miembros de la OTAN*: Estados Unidos, Canadá, Turquía, Francia, Alemania, Estonia, Eslovaquia, Lituania, España, Reino Unido, Suiza, República Checa, Letonia, Portugal, Bélgica, Polonia, Países Bajos, Italia, Noruega, Hungría, Luxemburgo, Grecia, Dinamarca, Islandia, Eslovenia, Croacia y Albania.

2) *Aliados estratégicos de la OTAN:* Australia, Egipto, Israel, Japón, Jordania, Nueva Zelanda, Argentina, Filipinas, Marruecos, Pakistán y Afganistán.

3) *Resto de Europa*: Serbia, Georgia, la Federación Rusa, Suecia, Ucrania, Bielorrusia, Rumania, Bulgaria, Moldavia, Malta, Montenegro, Irlanda y Chipre.

4) *Asía:* Malaysia, Singapur, India, China, Brunei, Uzbekistán, Armenia, Sri Lanka, Azerbaiyán, Kirguizistán, Indonesia, Kazakstán, Laos, Afganistán, Tayikistán, Nepal y Bután y Turkmenistán.

5) *Medio Oriente:* Qatar, Omán, Túnez, Arabia Saudita, Algería.

6) *América Latina:* Perú, Colombia, Chile, México, Argentina, Brasil, Jamaica, Panamá, Trinidad and Tobago, Surinam y Honduras.

7) *África:* Nigeria, Benín, Kenia, Ruanda, Uganda, Costa de Marfil, Ghana, Senegal, Botswana, Sudan, Madagascar y Mauricio.

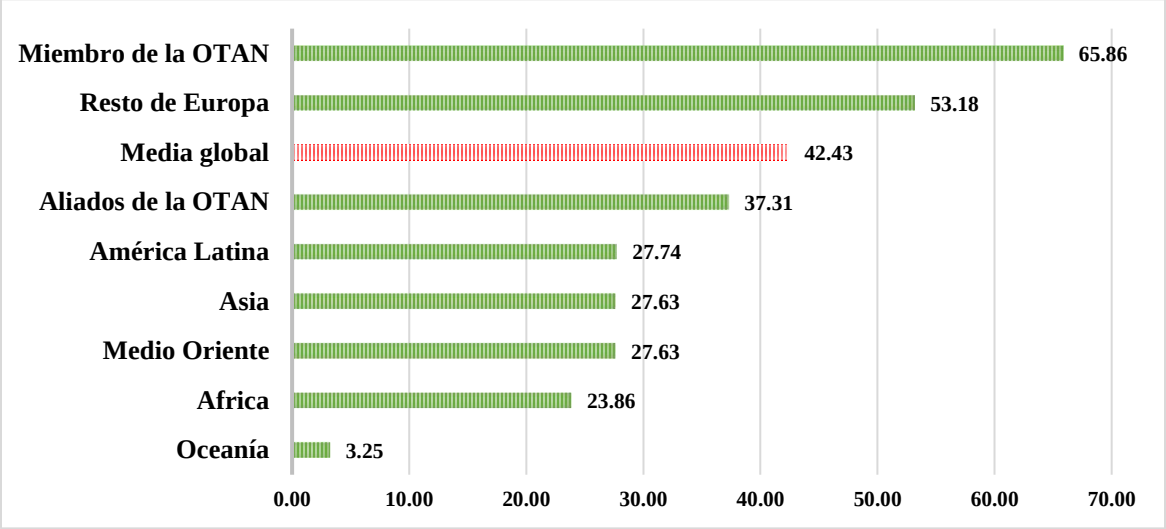
8) *Oceanía:* Samoa y Kiribati.

Se destaca que esta medida evalúa la preparación de los países para prevenir ciber amenazas y gestionar ciber incidentes. En ese sentido, se diferencia del GCI (2018) dado a qué este mide el grado de compromiso e importancia que los Estados-Nación han dado al tema de la ciberseguridad en el desarrollo de su política de seguridad nacional. Mientras que el NCSI es un instrumento que mide sus capacidades de ciber defensa y capacidad de acción ante ciber incidentes. Asimismo, es importante mencionar que el NCSI (2018) se empata con el GCI (2018) en aspectos como el desarrollo de marco legal, medidas técnicas, estructura internacional y cooperación internacional. No obstante, posee un apartado más amplio en el desarrollo de ciber capacidades, dado que trata con mayor profundidad las habilidades para atender ciber incidentes y combatir amenazas.

El NCSI (2018) se compone de un total de doce indicadores, con una ponderación que va del 0 al 100, los cuales han sido descritos en el capítulo dos esta investigación. Del mismo modo, que en la sección anterior se sumaron todas las ponderaciones de todos los países por región y se obtuvo la media global de cada conjunto descrito en la sección Anterior. En este caso, una vez más las naciones más aventajadas y líderes en el desarrollo de ciber capacidades son las naciones miembros de la OTAN, con una calificación de 65.86. Seguidos del resto de

Europa, con una calificación de 53.16. Del mismo modo, es importante destacar que la media global que detentan los países en esta medición fue de 42.43%. Por otra parte, en este caso destaca la fuerte brecha que existe entre los países aliados de la OTAN con los países miembros, la cual se extiende por una diferencia de 23.43 puntos. Un aspecto de interés que destaca en esta métrica es el hecho de que América Latina se encuentre unos puntos aventajados respecto a Asía y Medio Oriente, con un 27.74. Por último, destaca de nueva forma como África y los microestados de Oceanía están en las últimas posiciones.

Figura 37. Media regional o de grupos de países en capacidades de ciber defensa según el NSCI (2019).



Fuente: Elaboración propia con base en NSCI (2019).

A diferencia del GCI (2019), el NCSI (2018) presenta más evidencia en el desarrollo de ciber capacidades vinculadas a la seguridad del Estado-Nación y capacidades de acción frente a un ciber incidente. De esta manera, es más trascendente ver cuáles son las áreas en las que cada conjunto de naciones ha dado mayor prioridad para garantizar su seguridad e interés nacional en el contexto global. De esta forma, en la siguiente sección se presenta qué áreas han priorizado los diferentes grupos de países para consolidar su ciberpoder.

3.5.1 Países miembros y aliados de la OTAN

En el caso de los países miembros y aliados de la OTAN se encontró una clara divergencia en el desarrollo de sus capacidades en el ciberespacio a diferencia del GCI (2018) que puede ser observada en la figura 33. Por ejemplo, para el caso de las naciones integrantes de la OTAN se encontró una ponderación del 65.86 puntos, sobre un total de 100. Mientras las

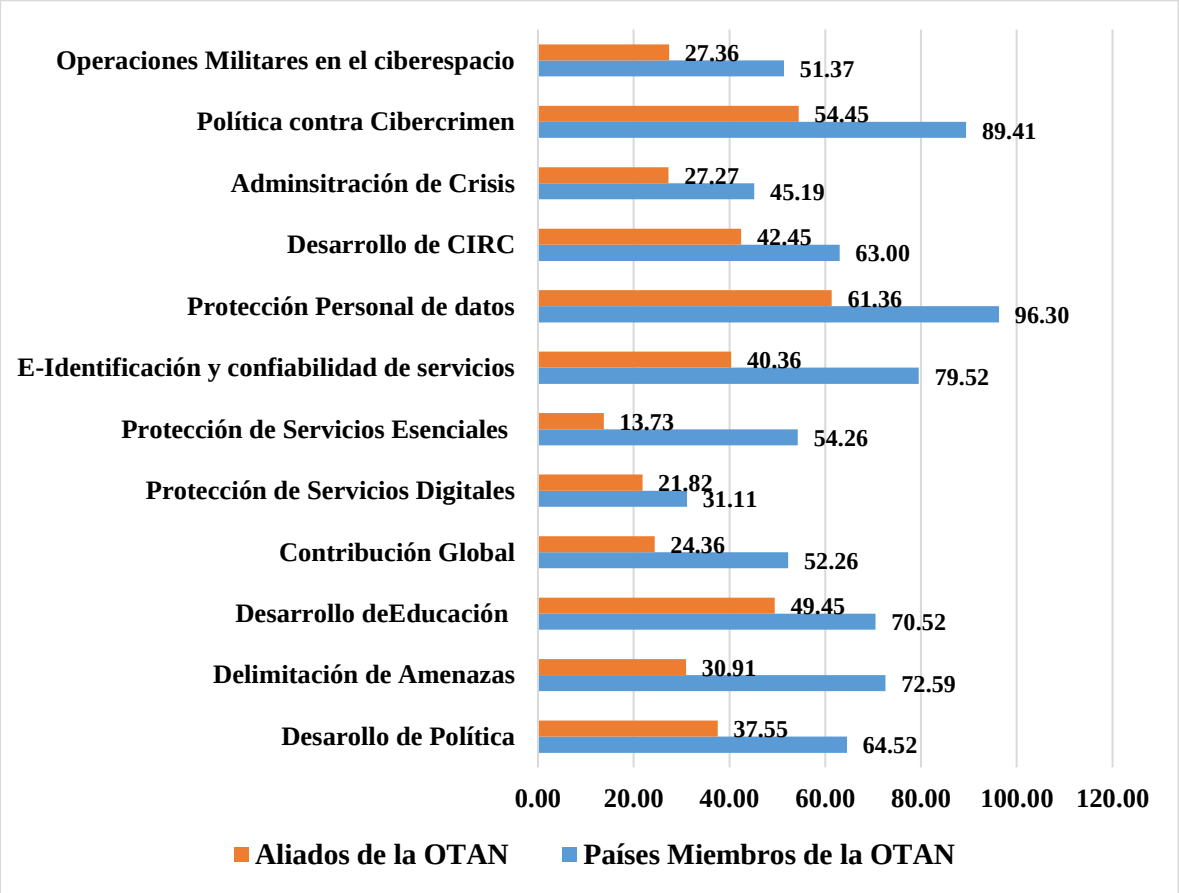
naciones aliadas de esta organización están por debajo con 28.55 puntos, con una calificación de 37.31 puntos, de un total de cien puntos.

Destaca que el avance más consolidado con el que cuentan ambos conjuntos de países es una política de protección de datos, con una alta ponderación en las naciones de la OTAN, de un total de 96.30 puntos, mientras que el grupo de países aliados alcanza la calificación de 61.36. Las otras dos mejores dimensiones aventajadas para las naciones integrantes de la OTAN son desarrollo de política de ciber crimen (89.41) e identificación electrónica y confiabilidad de servicios (79.52). Por su parte, los países aliados se encuentran bien posicionados del mismo modo en política de ciber crimen (54.45 puntos), mientras que, a diferencia de la tercera dimensión con mejor puntaje de los países de la OTAN, ellos presentan con buena ponderación en el tercer puesto la medida de desarrollo de educación en ciberseguridad (49.45), de hecho, esta es la dimensión en que menor brecha y rezago presentan los países integrantes y aliados de la OTAN.

Por otra parte, destacan las tres dimensiones en que ambos conjuntos obtienen sus ponderaciones más bajas. Por ejemplo, para el caso de integrantes de la OTAN son:1) Protección de servicios digitales (31.11), 2) administración de crisis (45.19) y operaciones militares en el ciberespacio (51.37). Sobre la primera destaca, la amplia brecha existente entre este indicador y uno fuertemente asociado, como es el caso de protección de servicios esenciales, dónde el conjunto de países de encuentra mejor posicionado con 54.26, lo que devela que a pesar de que son el conjunto de países mejor aventajados a nivel global, la ciberseguridad con enfoque integral para la sociedad aún está fuertemente expuesta.

En relación con la segunda, destaca el alto nivel de vulnerabilidad aún presente ante una crisis de para la seguridad nacional con origen en el ciberespacio. Mientras que la tercera presenta una fuerte asimetría entre los países líderes en operaciones militares en el ciberespacio como Estados Unidos (100), Francia (100) o Reino Unido (100), los de desarrollo medios, con casos como Países Bajos (67), Italia (67) y Noruega (50), y los de nulas capacidades, como Luxemburgo (0) o Islandia (0). Por último, se destaca que, respecto a los países de aliados de la OTAN, sus peores notas están presentes en los indicadores de protección de servicios esenciales (13.73), protección de servicios digitales (21.82) y contribución global (24.36).

Figura 38. Ponderación promedio de desarrollo de ciber capacidades de países integrantes y aliados de la OTAN.

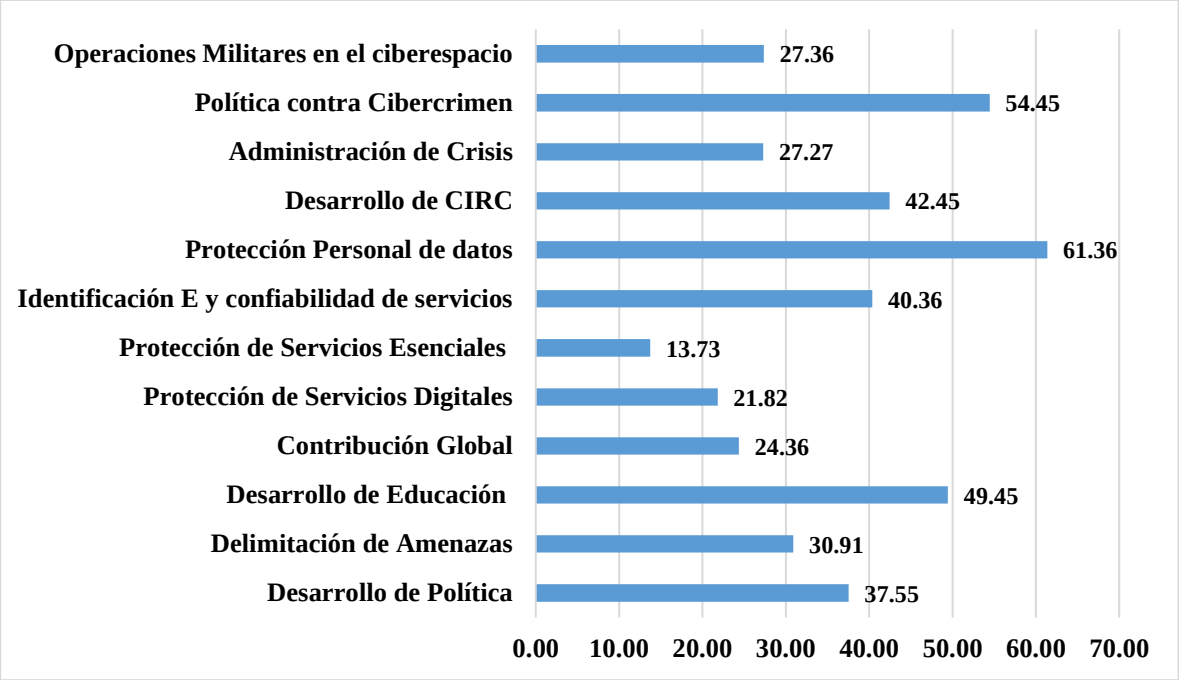


Fuente: Elaboración propia con base al NCSI (2019).

3.5.2 Resto de Europa

En el caso del conjunto de países de resto de Europa, se presenta un desarrollo significativo de ciber capacidades en las dimensiones de protección personal de datos (92.86), identificación electrónica (78.64) y desarrollo de educación (63.43). Mientras que en las dimensiones más bajas se presenta las dimensiones de protección de servicios digitales (20), administración de crisis (28.57) y contribución global (30.86). En promedio el conjunto de países alcanza un promedio de 37.31 puntos de un total de 100. Lo que da una mejor nota que las naciones aliadas de la OTAN en todos los indicadores, con especial énfasis para dimensiones como administración de crisis, protección de servicios esenciales (46.5) y desarrollo de educación (63.43).

Figura 39. Ponderación promedio de desarrollo de ciber capacidades de países del resto de Europa.



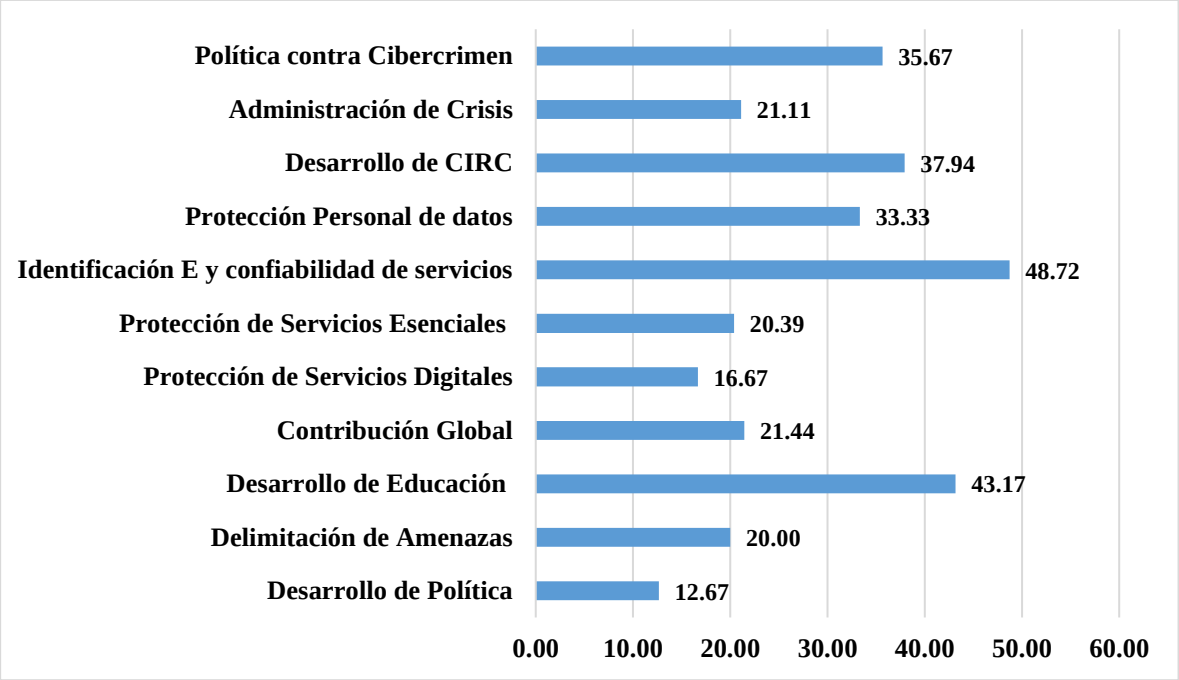
Fuente: Elaboración propia con base al NCSI (2019).

3.5.3 Asia

Para el caso del conjunto de los países de Asía se encontró la particularidad de que la dimensión en la que se encuentran más aventajados este conjunto de países fue Identificación electrónica y confiabilidad de servicios (con 48.72 puntos). Hecho resaltante frente a los países de occidente, que presentan sus mejores cifras en indicadores como política de protección de datos y desarrollo de política contra ciber crimen.

En segunda instancia, este conjunto de países presenta la dimensión de desarrollo de educación (43. 17) y en tercera posición la variable de desarrollo de política contra ciber crimen (35.67). En los ámbitos más bajos se encuentran las dimensiones de desarrollo de política (12.67), protección de servicios digitales (16.67) y delimitación de ciber amenazas (20).

Figura 40. Ponderación promedio de desarrollo de ciber capacidades de países de Asía.



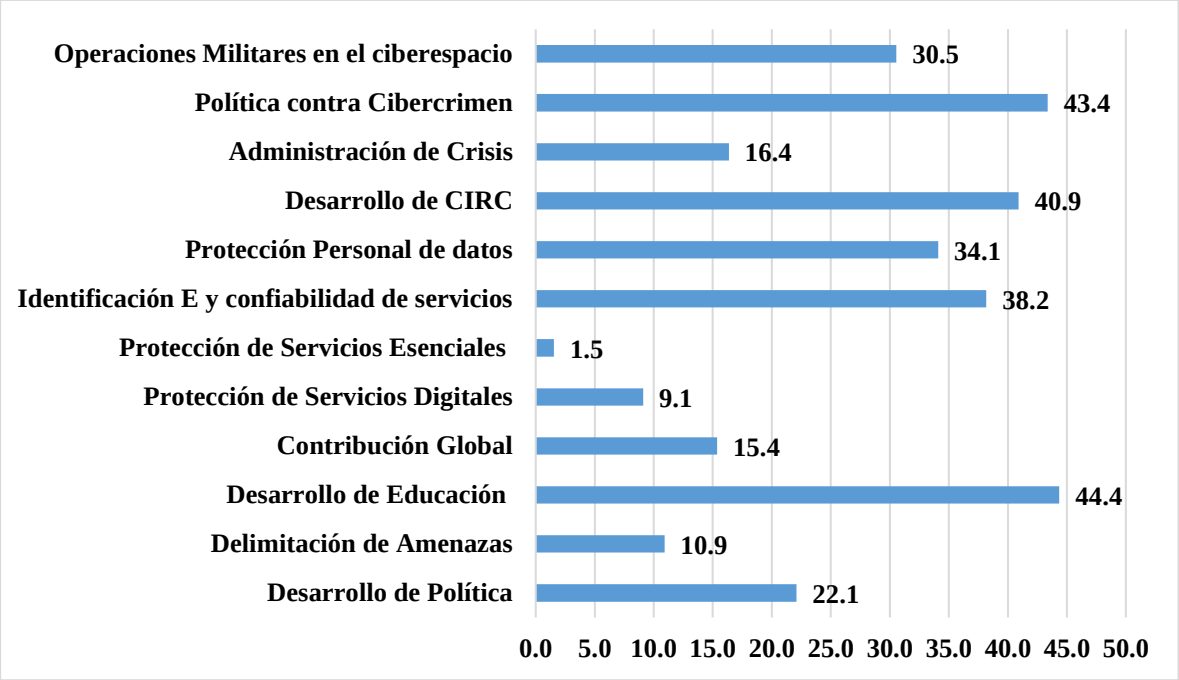
Fuente: Elaboración propia con base al NCSI (2019).

3.6.4 América Latina

Para el caso de América Latina, se destaca que las tres dimensiones entre las que mejor se encuentra posicionada la región son el desarrollo de política contra ciber crimen (43.4) y desarrollo de educación (44.4), y en tercera posición desarrollo de CIRC (40.9). Sobre este punto, es importante mencionar que la brecha existente en esta dimensión entre la región latinoamericana y los países de la OTAN no es tan amplia (representa sólo una diferencia de 22.1).

Mientras que, con los aliados de la OTAN, resto de Europa están prácticamente homologados. Por último, destaca que la región se encuentra más aventajada que el conjunto de naciones de Asía con base a esta métrica. Sin embargo, las dimensiones en las que se presenta el nivel más bajo son la protección de servicios esenciales (1.5), protección de servicios digitales (1.99 y la delimitación de ciber amenazas que pueden afectar su seguridad nacional (10.9).

Figura 41. Ponderación promedio de desarrollo de ciber capacidades de países de América Latina.



Fuente: Elaboración propia con base al NCSI (2019).

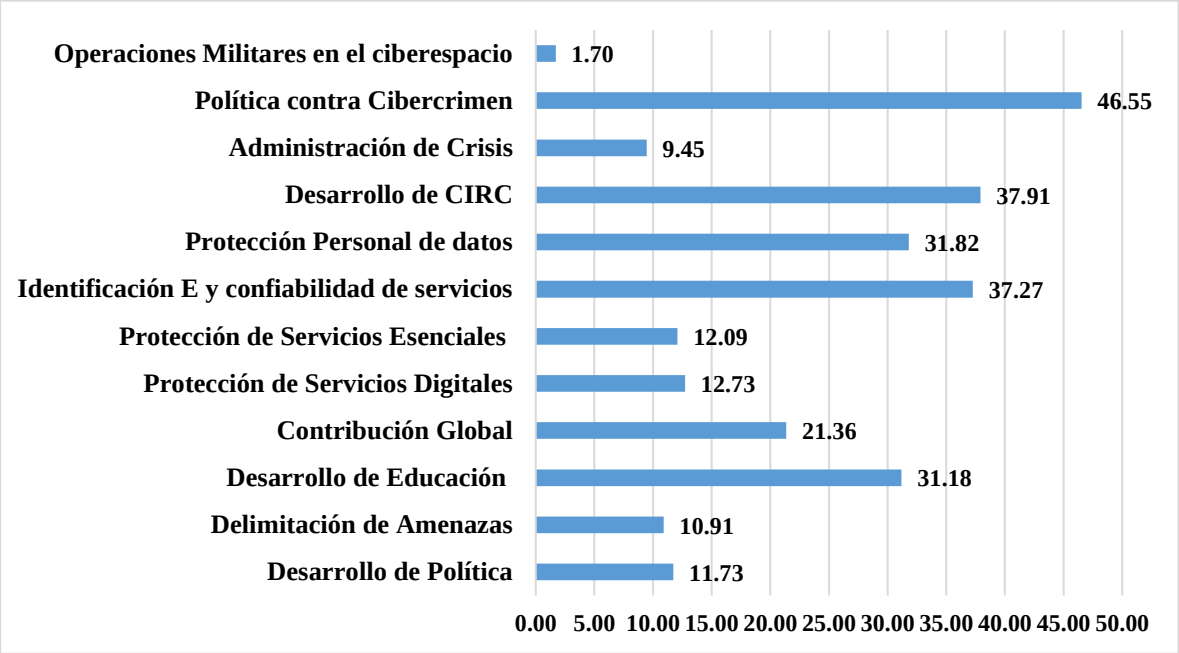
3.5.4. África

En el caso de la región africana, si bien su posición global la sitúa en el penúltimo puesto, con una ponderación global de 23.8 puntos de un total de 100. El panorama de los indicadores con mejor ponderación, del grupo de países destaca por no estar tan alejado de las medias globales. Por ejemplo, las tres dimensiones en que están más aventajados son política contra ciber crimen (46.55), desarrollo de CIRC (37.91) e identificación electrónica y confiabilidad de servicios (37.27). En el caso de este grupo de países destaca el desarrollo equilibrado de dimensiones entre indicadores de alta importancia y trascendencia en occidente, en concreto el caso de desarrollo de política contra ciber crimen, para países de la OTAN y sus aliados. Desarrollo de CIRC, con el que se encuentra en un punto equilibrado respecto a las naciones de América Latina y Asía.

Respecto a las dimensiones de menor ponderación se encuentran el caso de operaciones militares en el ciberespacio (1.7), administración de crisis (9.45) y delimitación de amenazas (10.91). Esto demuestra una baja priorización en cuestiones de ciberseguridad para actores como las fuerzas armadas y la delimitación de amenazas, que está estrechamente vinculado a la delimitación de ciber amenazas por parte de los Estado-Nación, aspecto que igualmente

influye en la dimensión de desarrollo de política de ciberseguridad, dimensión en la que la región igualmente tiene una ponderación muy baja con un valor 11.73.

Figura 42. Ponderación promedio de desarrollo de ciber capacidades de países de África.

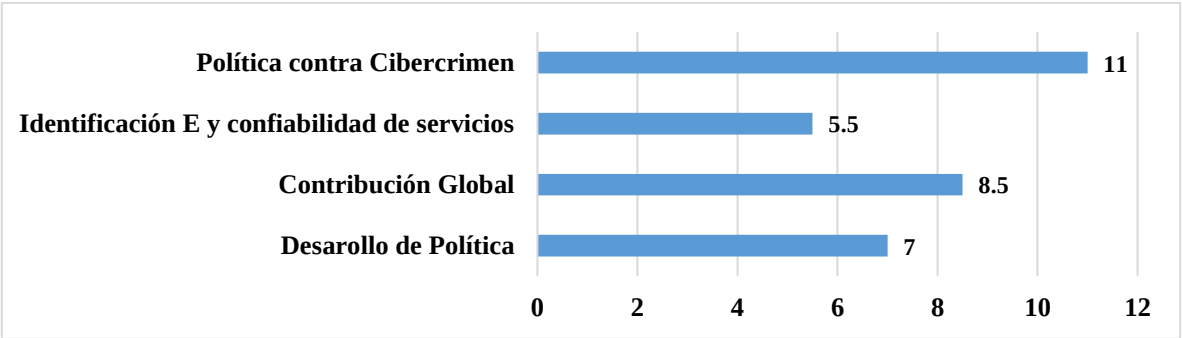


Fuente: Elaboración propia con base al NCSI (2019).

3.5.5 Oceanía

Para el caso de Oceanía se encontró que, de un total de doce dimensiones de NCSI (2019), la región presenta valores de 0 en 8 de estos. Los únicos en los cuales presentó una ponderación fueron desarrollo de política contra ciber crimen (11), contribución global (8.5), desarrollo de política (7), e identificación electrónica y confiabilidad de servicios (5.5.).

Figura 43. Ponderación promedio de desarrollo de cibercapacidades de países de Oceanía.



Fuente: Elaboración propia con base al NCSI (2019).

3.6 Niveles de acción y estrategia de los Estados Nación en el Ciberespacio

Las dos métricas anteriores, como se indicó, presentan una serie de indicadores vinculados a desarrollo de capacidades en materia de ciberseguridad. Sin embargo, ambas se asocian a esfuerzos multilaterales para fomentar la gobernabilidad del ciberespacio. Del mismo modo, como se observó, al ser lideradas por instituciones como la Unión Internacional de Telecomunicaciones (ITU) y la *E-Governance Academy* presentan un panorama incompleto respecto al nivel real de ciber capacidades que presentan países como la Federación Rusa, la República Democrática de Corea del Norte, la República Islámica de Irán, la República Popular de China, por citar solo algunos casos.

Lo anterior, se vincula al hecho de que estos países consideran al ciber poder como un componente para abonar al poder del Estado-Nación y crucial para alcanzar objetivos de su interés nacional. Del mismo modo, existen fuertes regulaciones y controles al interior de cada una de estas naciones para garantizar su seguridad nacional. Por último, cada uno se considera oponente de las potencias del mundo occidental que son transparentes en materia de ciberseguridad en métricas como el NCSI (2019) y el GCI (2018). De esta forma, no destaca que la información que se conoce respecto a cada uno de ellos se vea permeada por la falta de transparencia, el secretismo y la especulación.

En ese sentido, una medida alternativa que calibra y da luces sobre el ciber poder de los Estados Nación es el Índice Nacional de Poder Cibernético del Belfer Center de la John Kennedy School (*National Cyber Power Index* o NCPI por sus siglas en inglés), el cual mide las ciber capacidades de treinta países, con base a siete objetivos vinculados a la seguridad nacional y la política exterior. La medida se compone de un total de 32 indicadores de intención y 27 indicadores de capacidad con evidencia recopilada a través de datos públicos disponibles. A diferencia del GCI (2019) y el NCSI (2018), la finalidad del NCPI (2020) es presentar un panorama y aproximación del ciberespacio como un instrumento que abone al poder del Estado-Nacional, el cuál esté estrechamente relacionado a sus intereses y seguridad nacionales.

De esta forma, el NCPI (2020) evalúa las Estrategias Nacionales de Ciberseguridad de los países, así como sus capacidades de defensa y ofensa, la asignación de recursos de parte del gobierno a la ciberseguridad, desarrollo en el dominio del sector privado, el nivel de

profesionistas vinculados a ciberseguridad y, por último, analiza el nivel de innovación en el campo de cada país.

De esta forma el NCPI (2020) es una medida de ciber poder y potencial comprobado de los Estados-Nación[24], más que del desarrollo de sus ciber capacidades. Del mismo modo, se destaca que la puntuación final otorgada por la métrica asume que cada país evaluado puede ejercer estas capacidades de manera efectiva. Sus vínculos con el interés nacional se establecen a razón de que la medida define siete objetivos que persiguen los países a través del ciberespacio, los cuales son:

I. vigilancia y seguimiento de actores y grupos nacionales de importancia para la ciberseguridad,
II. fortalecimiento y mejora de las ciber defensa nacional por parte del Estado-Nación,
III. control y manipulación del entorno de información por parte del gobierno,
IV. recopilación de inteligencia extranjera para la seguridad nacional;
V. ganancia comercial o mejora del crecimiento de la industria nacional obtenido por los beneficios del ciberespacio,
VI. capacidad de destrucción o des habilitación de la infraestructura y las capacidades frente a un adversario del Estado-Nación y,
VII. definición de normas cibernéticas y estándares técnicos internacionales.

La visión realista y del interés nacional se refleja más en el NCPI (2020) al considera al ciber poder como la capacidad efectiva de utilizar el ciberespacio para alcanzar objetivos nacionales. Del mismo modo, presenta la capacidad real de un Estado-Nación para ejecutar una agresión en contra de un adversario o enemigo, como sería el caso de destruir o deshabilitar una infraestructura nacional crítica, a través de operaciones cibernéticas ofensivas.

[24] A pesar de que el NCPI (2020) se presente de esta forma, quedan dudas y puede que la medida sobreestime el nivel de ciberpoder y cibercapacidades de actores oponentes a los Estados Unidos. Lo anterior, se debe a que la métrica da la mejor ponderación a Estados Unidos de América, por encima de países como Irán, Rusia o China. Sin embargo, episodios como el ciberataque de SolarWinds de un hackeó de más 15 mil agencias del gobierno de ese país, con evidencia de origen del ataque en Rusia, muestran que el ciber poder y capacidad de ofensa de este actor son más amplias de lo que se considera.

Frente a esto, en NCPI (2020) presenta una evaluación general que definen mide la *exhaustividad* (*comprehensiveness* es el concepto en inglés) de un país como actor cibernético. Para dicha métrica la exhaustividad se refiere al uso que hace un Estado-Nación de la tecnología cibernética para lograr múltiples objetivos a través del ciberespacio. De esta forma, el ciber poder más completo para un nacional es el que presenta las siguientes características:

I. la intención de perseguir múltiples objetivos nacionales utilizando medios cibernéticos y;
II. las capacidades para lograr esos objetivos, ambas características vinculadas a conceptos como el interés nacional, seguridad nacional y política exterior del Estado-Nación.

De esta forma, el NCPI (2020) presenta dos diferentes caras en su medición agregada en las categorías que de *intención* y *capacidades* del Estado-Nación. La primera noción corresponde, al propósito de utilizar el ciber poder para alcanzar objetivos estratégicos afines al interés nacional de un país, en esta clasificación, la métrica especifica que naciones como China, Rusia o la citada Corea del Norte consideran al ciberespacio un dominio trascendental para el poder nacional. No obstante, el segundo concepto presenta en concreto a los países que en verdad tienen el nivel suficiente de ciber capacidades para utilizar a esta arena a su favor o infligir daños a un oponente o enemigo a través de la arena del internet.

En ese sentido, el NCPI (2020) expresa que los diez países con los poderes cibernéticos más completos, con base a los siete objetivos vinculados a la *exhaustividad*, son: EE. UU., China, Reino Unido, Rusia, Países Bajos, Francia, Alemania, Canadá, Japón, Australia. De esa forma, es importante resaltar las diferencias que existen con métricas como el NCSI (2019) y el GCI (2018). Este comparativo se presenta en la tabla 18.

Tabla 18. Comparativo de ciber capacidades de diez principales países según NCPI (2020), GCI (2019) NCSI (2018).

No.	Belfer Center National Cyber Power Index (NCPI) 2020	Ponderación	Global Cyber Security Index 2019	Ponderación	National Cyber Security Index 2018	Ponderación
1	Estados Unidos	51	Reino Unido	93.1	Francia	83.12
2	China	47	Estados Unidos	92.6	Alemania	83.12
3	Reino Unido	36	Francia	91.8	Estonia	81.82
4	Rusia	28	Lituania	90.8	Eslovaquia	80.52
5	Países Bajos	24	Estonia	90.5	Finlandia	79.22
6	Francia	23.5	Singapur	89.8	Lituania	77.92
7	Alemania	22	España	89.6	España	77.92
8	Canadá	21.5	Malasia	89.3	Reino Unido	75.32
9	Japón	21	Canadá	89.2	Suiza	75.32
10	Australia	20	Noruega	89.2	República Checa	74.03

Fuente: Elaboración propia.

Es importante mencionar que el mismo NCPI (2020) se define a sí mismo, como una combinación de los aspectos más trascendentales del GCI (2019) y NCSI (2018). De esta forma, reconoce que los objetivos en materia de ciberseguridad del Estado-Nación, no se componen de forma aislada, sino que las ciber capacidades de una nación son un conjunto de herramientas que, junto con los medios militares tradicionales del Estado, la diplomacia, las políticas públicas, las medidas punitivas y la política comercial se emplean para que un país pueda utilizar el ciberespacio para alcanzar sus objetivos nacionales.

Otro aspecto de interés del NCPI (2020), es el hecho de que utiliza bases de datos disponibles y transparentes que miden elementos específicos del ciber poder, a la par que recopila información con múltiples indicadores que se obtienen a través de la apertura de los países que comparten la evidencia con esta métrica. Una vez más, en este punto, se presenta el nivel de transparencia que se puede tener respecto a naciones como China, Rusia, Irán o Corea del Norte.

Sobre esto, es importante mencionar que el NCPI (2020) hace un importante énfasis en concreto a Corea del Norte, en el que especifica que precisamente a razón de la ausencia de mediciones confiables para integración de un nivel del ciber poder de este actor, que la medición recurrió a expertos en materia de seguridad del ámbito gubernamental, privado y académico. El último dato de trascendencia del NCPI (2020), es el indicar que califica a 30 países[25] con una ponderación que va del 1 al 5. Así como el hecho de que la selección de los países emana de una decisión de los equipos de las que la métrica considera las cinco superpotencias cibernéticas según el Belfer Center (Estados Unidos, Reino Unido, Israel, China y Rusia), un total de 6 países con grupos APT atribuidos[26], 7 y el juicio en torno a poderes cibernéticos en ascenso.

También, se incluyen a países que han manifestado, de manera abierta o encubierta, su deseo de ser considerados como una potencia cibernética. Una vez presentadas las particularidades de la métrica, podemos es importante analizar cuáles son los objetivos estratégicos que persiguen los países en el ciberespacio, para posteriormente comprender el nivel de intención y capacidades de los Estados-Nación incluidos en esta medida.

[25] Los treinta países son: Australia, Brasil, Canadá, China, República Popular Democrática de Corea, (RPDC), Egipto, Estonia, Francia, Alemania, India, Irán, Israel, Italia, Japón, Lituania, Malasia, Países Bajos, Nueva Zelanda, Corea del Sur, Rusia, Arabia Saudita, Singapur, España, Suecia, Suiza, Turquía, Ucrania, Reino Unido, Estados Unidos y Vietnam.

[26] Los países son Irán, Vietnam, Corea del Norte, Malasia, Rusia y China.

3.6.1 Objetivos estratégicos del Ciber poder según el NCPI (2020)

La trascendencia del NCPI (2020) oscila en el hecho de que categoriza un total de 7 objetivos estratégicos del ciber poder, como medio para que los Estados-Nación utilicen al ciberespacio como componente para abonar al poder nacional. A través de estos objetivos se delimitan los 32 indicadores de intención y 27 indicadores de capacidad que definen el ciber poder según está métrica. En ese sentido, la comprensión de cada objetivo es importante a la hora de abordar la noción de ciber poder que presente el instrumento. A continuación, se presenta una descripción de los objetivos comunes que los estados intentarán alcanzar a través del ciberespacio según el NCPI (2020) del Belfer Center:

1. *Vigilancia y seguimiento de grupos domésticos:* Representa el hecho de que un país ha tomado medidas para consolidar sus medidas y permisos legales para aplicar capacidades de ciber vigilancia. Con la finalidad de monitorear, detectar y recopilar inteligencia sobre amenazas y actores nacionales dentro de sus fronteras. Esta categoría puede incluye desde la vigilancia de los ciudadanos, el monitoreo de tráfico de Internet, el eludir cifrado, detectar e interrumpir servicios de inteligencia extranjeros, organizaciones criminales y grupos terroristas.

2. *Fortalecimiento y mejora de la ciberdefensa nacional:* Indica cuándo un país ha priorizado la mejora de la defensa de los activos y sistemas gubernamentales y nacionales, con el fin de desarrollar capacidades de resiliencia y disuasión en el ciberespacio. Esto incluye la defensa activa de activos del gobierno, la promoción de la ciberseguridad y su conciencia en industrias clave, la población en general, así como la sensibilización nacional sobre las ciber amenazas.

3. *Control y manipulación del entorno de información:* Representa el equilibrio que alcanza un país para priorizar el uso de medios electrónicos para controlar la información a nivel nacional e internacional, a la par de respetar y proteger la privacidad en el Internet y la libertad de expresión de sus ciudadanos. La categoría engloba aspectos negativos el cómo difundir propaganda nacional, la creación y difusión de desinformación en el extranjero, así como utilizar capacidades cibernéticas para atacar e interrumpir grupos que se encuentran fuera de la jurisdicción nacional, incluidos grupos extremistas de redes sociales o propaganda extranjera que busque afectar la estabilidad política del país.

4. *Recopilación de inteligencia en otros países para la seguridad nacional:* Supone la acción de un país para extraer secretos nacionales de un adversario u oponente a través del ciberespacio. Este objetivo se centra específicamente en la recopilación de información que no es comercialmente sensible o de fuentes abiertas, sino en la recopilación de información que informa actividades diplomáticas, militares, de planificación o seguimiento de tratados u otras situaciones en las que los países buscan mejorar su conocimiento y comprensión de un país extranjero. Esto incluye acciones para obtener la información como hackeo y violaciones de información clasificada, como planes militares, pero también incluye robo de datos personales, registros y acceso a las comunicaciones de personalidades gubernamentales de alto nivel.

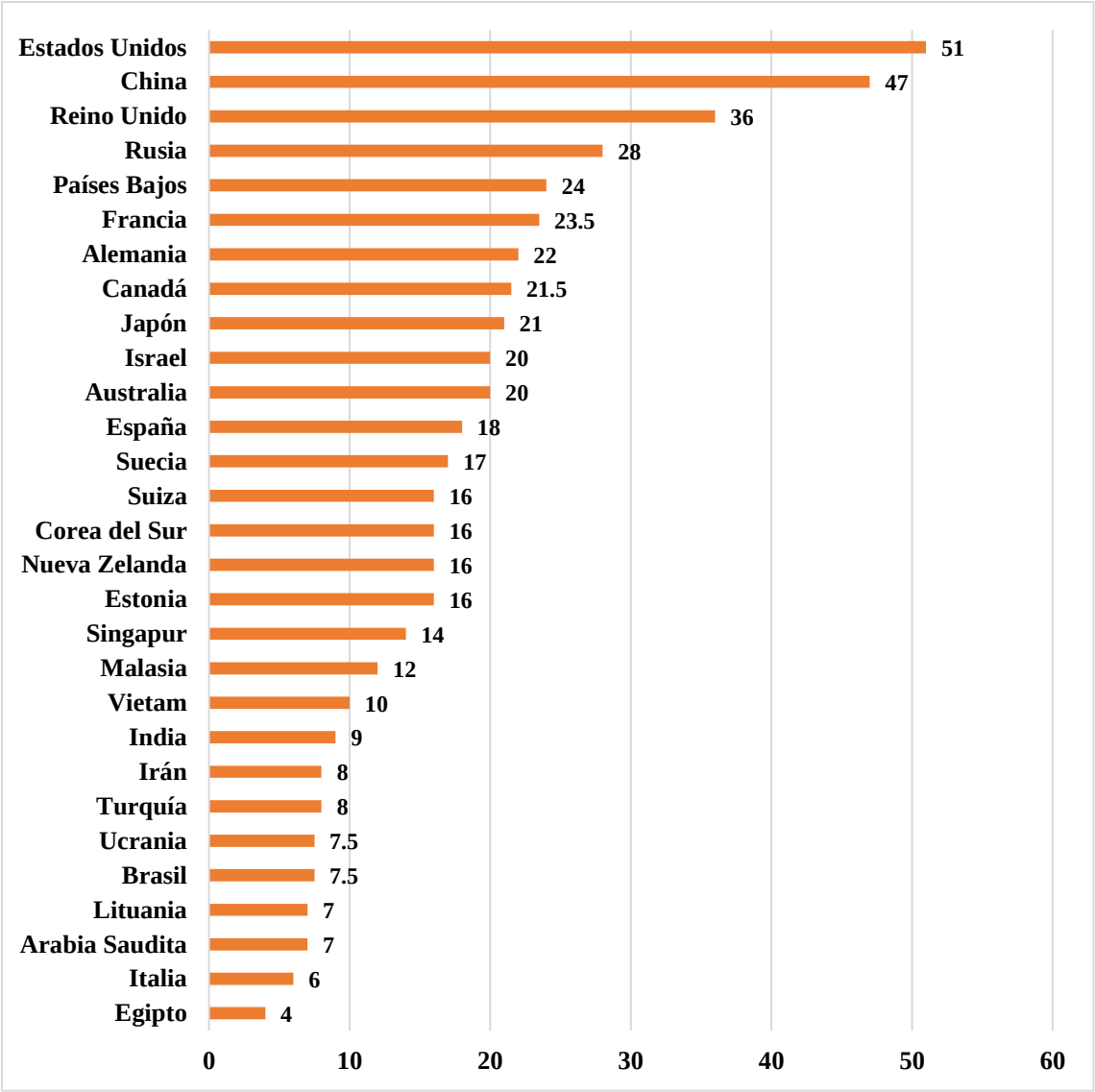
5. *Creciente competencia cibernética y tecnológica nacional:* Representa los esfuerzos del país por hacer crecer su industria de tecnología nacional o utilizar medios cibernéticos para desarrollar otras industrias a nivel nacional. Es importante destacar, que en este objetivo se engloban medios legales e ilegales. Entre los medios ilegales incluyen la realización de espionaje industrial contra empresas extranjeras y países para facilitar la transferencia de tecnología. Los medios legales incluyen la inversión en investigación y desarrollo de ciberseguridad y la priorización de desarrollo de la fuerza laboral en ciberseguridad.

6. *Destrucción o desactivación de la infraestructura y las capacidades de un adversario:* Se refiere al hecho de que un país ha utilizado técnicas, tácticas y procedimientos cibernéticos destructivos para disuadir, erosionar o degradar la capacidad de un adversario para luchar en el dominio del ciberespacio u otros campos de confrontación convencional. Incluye ataques cibernéticos a infraestructura crítica y ataques DDoS a redes de comunicaciones gubernamentales. También, a ciberataques para demostrar la intención y la capacidad de disuadir a un adversario de actuar.

7. *Definición de normas técnicas y normas cibernéticas internacionales:* Representa la participación de un Estado-Nación en debates internacionales legales, políticos y técnicos en torno a las normas de ciberseguridad global. También, engloba firmar tratados internacionales sobre la materia, participar en grupos de trabajo técnicos y unirse a asociaciones y alianzas cibernéticas para combatir el ciber delito y compartir experiencia y capacidades técnicas (NCPI, 2020).

Con base a esta medición en la figura 45 se presentan las ponderaciones que presentan los países incluidos en el NCPI (2020), en una ponderación que va del 1 al 100.

Figura 45. Medición de ciber poder del NCPI (2020).



Fuente: NCPI (2020).

Del mismo modo, destaca que en cada dimensión las posiciones de los países son diferentes. Lo anterior, se debe a que el NCPI (2020) considera que cada país prioriza con base a su interés nacional cada uno de los objetivos del Estado-Nación que representa cada uno de los siete indicadores de la métrica. Este contraste se puede observar en la tabla 19.

Tabla 19. Ponderación por objetivo nacional del NCPI (2020) de los 10 países con ciber poder más completo.

No.	País	Dimensiones[27]						
		Vigilancia	Defensa	Información y Control	Inteligencia	Comercio	Ofensiva	Normas
1	Estados Unidos	3/30	4/61	1/59	1/58	1/32	1/59	1/58
2	China	1/49	1/69	3/41	3/35	2/28	4/31	5/35
3	Reino Unido	4/29	9/54	6/15	2/50	3/15	2/55	6/32
4	Rusia	2/37	18/47	2/41.5	10/15	26/2	3/49	15/20
5	Países Bajos	9/24	3/62	14/9.5	5/10	6/12	9/18	9/23
6	Francia	18/14	2/63	10/10	12/13	16/5	10/15	2/43
7	Alemania	7/25	10/50	10/10	14/10	14/7	7/19	4/37
8	Canadá	5/26	5/61	11/10	7/18	15/6	12/9	10/22
9	Japón	21/11	6/60	10/10	18/6	4/15	16/4	3/42
10	Australia	10/24	11/49	9/11	9/16	8/10	14/7	7/25

Fuente: Elaboración propia con base al NCPI (2020).

Un aspecto trascendental de este análisis es ver las metas que priorizan los diez países con el ciber poder más completo el NCPI (2020). Por ejemplo, para el caso de las dimensiones estratégicas para la seguridad nacional podemos señalar a los indicadores de defensa, información y control, vigilancia y normas, en los que se pueden encontrar claras diferencias sobre cómo los Estados priorizan sus objetivos.

Por ejemplo, para el caso de la dimensión de defensa, vinculada a la capacidad de proteger a la nación de agresiones provenientes del ciberespacio, destacan las capacidades de naciones como China (1° posición/69 puntos), Francia (2°/63) y Países Bajos (3°/30). En el caso de información y control, las tres primeras posiciones son ocupadas por Estados Unidos (1°/59), Rusia (18°/47) y China (3°/41). Para vigilancia lideran China (1°/49), Rusia (2°/37) y Estados Unidos (3°/30). Y para normas se ubican al frente Estados Unidos (1°/58), Francia (2°/43),

[27] En el listado se presentan la posición que ocupan en el ranking, seguido de la ponderación alcanzada por cada país en esa misma medición.

Japón (3°/42). Mientras que para indicadores trascendentales para para la política exterior como capacidades ofensivas, se encuentran en primeras posiciones las naciones de Estados Unidos (1°/59), Reino Unido (2°/55) y Rusia (3°/49). O el caso de inteligencia Estados Unidos (1°/58), Reino Unido (2°/50) y China (3°/35). Por último, para el caso del comercio en primera posición están Estados Unidos (1°/32), China (2°/28) y Reino Unido (3°/15).

Del mismo modo, en este ranking de las 10 naciones con más ciber poder más completo, destaca la ausencia de potencias del ciberespacio reconocidas por el mismo Belfer Center, como es el caso de Israel. O países que comúnmente son señalados en la opinión pública internacional por ejecutar gran cantidad de ciber operaciones con la finalidad de alcanzar objetivos particulares como Corea del Norte e Irán. Sin embargo, los indicadores de intención y capacidades del NCPI (2020), muestran un mejor balance y equilibrio respecto a estos actores transcendentales para comprensión del ciber poder, que se presenta a continuación.

3.6.2 Medidas de intención y capacidades según el NCPI (2020)

Uno de los aportes más trascendentales del NCPI (2020) para conceptualizar el ciber poder, es el plantear la diferencia que existe entre las intenciones de un país para utilizar el ciberespacio para perseguir un objetivo nacional, y sus capacidades para alcanzar dicha meta. De esta forma, la métrica expresa que la *capacidad* representa la efectividad de una nación para lograr un objetivo estratégico a través del ciberespacio, frente a la cual puede decidir alcanzarlo o no. Mientras que la intención es una medida del peso que dan las naciones al ciberespacio, como un dominio para abonar elementos al poder del Estado-Nación y perseguir objetivos estratégicos a través de él. Sin embargo, los países y gobiernos pueden desear perseguir un objetivo a través del ciberespacio, pero pueden carecer de la capacidad o los recursos necesarios para hacerlo realmente.

En relación a lo anterior el NCPI (2020) divide su medición en dos diferentes instrumentos para contextualizar esta diferencia, los cuales son el *Índice de intención cibernética (CII*) y el *Índice de capacidad cibernética (CCI),* cada uno descrito a continuación.

3.6.2 Índice de intención cibernética (IIC)

La primera subdivisión planteada del NCPI (2020) está integrada por un total 32 indicadores que están agrupados en los siete objetivos de la métrica. Estos son combinados con la puntuación de los factores de intención dentro de las Estrategias Nacionales de Ciberseguridad de los países analizados, los cuales se les suma la puntuación de los ataques atribuidos a cada país en cuestión. Por último, la calificación general de cada nación es el promedio de los siete objetivos nacionales en una escala que va del 0 al 100. Los resultados de este análisis para cada dimensión en la tabla 20.

Tabla 20. Ponderación por intención del IIC del NCPI (2020).

No.	ICC	Vigilancia	Defensa	Información y Control	Inteligencia	Comercio	Ofensiva	Normas
1	China	Rusia	Reino Unido	Estados Unidos	Reino Unido	China	Reino Unido	Reino Unido
2	Estados Unidos	China	Países Bajos	China	Estados Unidos	Iran	Estados Unidos	Alemania
3	Reino Unido	Vietnam	Francia	Rusia	España	Reino Unido	Israel	Estados Unidos
4	Rusia	Arabia Saudita	Estados Unidos	Vietnam	Países Bajos	Japón	España	Japón
5	Países Bajos	Reino Unido	China	Israel	Israel	Suiza	Rusia	Francia
6	Israel	Estonia	Japón	Irán	Rusia	Países Bajos	Iran	Suiza
7	España	Países Bajos	Canadá	Reino Unido	Nueva Zelanda	Suecia	China	Países Bajos
8	Australia	Australia	Suecia	Alemania	Canadá	Australia	Países Bajos	China
9	Canadá	Estados Unidos	Estonia	Nueva Zelanda	Australia	Estados Unidos	Estonia	Canada
10	Irán	Suiza	Australia	Francia	China	Rusia	Australia	Australia

Fuente: Elaboración propia con base al NCPI (2020).

Cada uno de los países del top 10 de las CII, y sus diferentes dimensiones, han establecido acciones estratégicas para fortalecer y mejorar las sus capacidades de ciber defensa nacional. En ellos hay una acción y voluntad política importante de crear los requerimientos mínimos necesarios para protegerse contra los ciber ataques en el largo plazo a través del incremento de sus capacidades de ciber resiliencia para la seguridad del Estado-Nación, sus empresas privadas y ciudadanía. En este contexto, destaca cómo China es el país con la puntuación más alta en intención, por encima de otros países que tienen ENCS más consolidadas o participación más importante en foros internacionales, a tazón de que el país está tejiendo acciones estratégicas para su consolidación en el dominio, aunque puede tener varias áreas

de oportunidad en algunas dimensiones. Para comprender a los países líderes en cada indicador, se presenta un análisis por cada uno de estos, con base a lo presentado en el NCPI (2020):

a. *Vigilancia:* Rusia, China, Vietnam y Arabia Saudita ocuparon las primeras posiciones en el indicador. Esto se debe a que las cuatro naciones tienen fuertes controles para contenido considerado ilegal por sus gobiernos, para ser de libre acceso para la población nacional. Del mismo modo, todos cuentan con cuerpos policiales y agencias de inteligencia nacionales con ciber capacidades para su regulación con l excepción de Arabia Saudita. Asimismo, los cuatro hicieron referencia a las amenazas cibernéticas dentro de sus ENCS o planes de seguridad nacional o de terrorismo nacional.
b. *Control:* en este indicador se analiza la capacidad del Estado para eliminar material extremista y refutar la propaganda extranjera o contener el flujo de desinformación en el extranjero. En ese sentido, la dimensión la lidera Estados Unidos a razón del papel de sus agencias militares y de inteligencia en casos específicos como el de contener a grupos extremistas para difundir sus ideas o reclutar a nuevos adeptos. En segunda y tercera posición del NCPI (2020) se encuentran China y Rusia, a razón de las grandes compañas de desinformación que se les han atribuido desde 2016.
c. *Ofensivo:* las estrategias cibernéticas y militares del Reino Unido, Israel, los Estados Unidos y Rusia son reconocidas por el NCPI (2020) como las que han desarrollado las capacidades destructivas más profundas a través de la arena del ciberespacio. Además, la métrica expresa que los tres países han demostrado en forma efectiva y mediante hechos sus capacidades. Del mismo modo, se pone énfasis en que en la actualidad pocas naciones llevan a cabo un acto destructivo a través de ciber operaciones, y sólo casos como China, Corea del Norte, Países Bajos, Irán, Israel y España, además de los cuatro países citados, fueron las únicas naciones que recibieron una puntuación en esta medición. El resto de naciones de la métrica, no obtuvieron una puntuación alta o no obtuvieron ninguna puntuación en la categoría. A razón de que guardan silencio o no presentan oficial sobre el hecho de que puedan emprender operaciones cibernéticas destructivas.

d. *Inteligencia:* En este indicador, el NCPI (2020) destaca la importancia de las filtraciones de Edward Snowden, entre 2013 y 2015, dónde se indicó las altas capacidades de recolección de información clasificada por Reino Unido y los Estados Unidos. Del mismo modo, es de interés como la métrica posiciona a España de la dimensión, lo cual se sustenta en las agencias militares y de inteligencia de España que han declarado y demostrado su intención de utilizar el dominio del ciberespacio para recopilar información para inteligencia.
e. *Comercial*: en esta dimensión destaca el interés de China por encabezar el liderazgo de la competencia comercial y tecnológica a través del ciberespacio. Del mismo modo, destacan naciones como Corea del Norte o Irán, que persiguen intereses económicos, de carácter legal e ilegal, a través del dominio. En ese sentido, la presencia de estos tres países se ha observado a través de la realización de espionaje industrial, con el fin de incentivar y hacer crecer su industria y economía nacional a través de la explotación de la información extraída que impacte en investigación, desarrollo de industrias nacionales y de asociaciones público-privadas.
f. *Normas:* en este indicador, el NCPI (2020) analizó las ENCS de 29 países, en 27 de estos, se encontró que los países construyeron sus normativas y legislativas apoyándose en normas de ciber delitos internacionales y normativas técnicas, con las excepciones de Egipto e India. Reino Unido y Alemania ocuparon las primeras posiciones en esta medición, y lo anterior se vincula a su amplio apoyo a instituciones internacionales y su capacidad internacional de promoción de construcción de iniciativas contra ciber delitos.
g. *Defensa:* en este campo los cinco primeros países para el objetivo de ciberdefensa estuvieron ocupados por Reino Unido, Países Bajos, Francia, Estados Unidos y China. El puntaje para la selección de estos actores se vincula a que este conjunto de países busca de manera activa una mayor resiliencia cibernética y medidas activas de ciberdefensa. En ese sentido, 15 países demostraron su intención de mejorar sus procedimientos frente a ciber incidentes, para recopilación de información de inteligencia mediante la realización de simulacros de ciberataques a sí mismos, que se centraron en la recopilación de información de inteligencia,

para mejorar su conocimiento de sus niveles reales de ciber defensa frente a un país extranjero.

3.6.2 Índice de Capacidades Cibernética (ICC)

El Índice de Capacidad Cibernética (ICC), del mismo modo que el ICC, se pondera de una escala del 0 al 100, y se basa en una serie de 27 indicadores que se agrupan a través de los siete objetivos para el Estado-Nación. A diferencia de la medida intención del NCPI (2020), presentada en la sección anterior y vinculada a la consideración, activismo y proselitismo de cada país por construir ciberpoder, el ICC presenta las capacidades los 7 objetivos por medio de capacidades efectivas de las naciones para ejercer su ciberpoder a través de diferentes operaciones. A continuación, presentamos en la tabla 21 presentamos los resultados del análisis de cada dimensión.

Tabla 21. Ponderación por capacidades del ICC del NCPI (2020).

No.	Vigilancia	Defensa	Información y Control	Inteligencia	Comercio	Ofensiva	Normas
1	Estados Unidos	China	Estados Unidos	Estados Unidos	Estados Unidos	Rusia	Estados Unidos
2	Reino Unido	Singapur	Rusia	Reino Unido	Corea del Sur	Estados Unidos	Francia
3	Francia	Canadá	China	China	China	China	Japón
4	China	Francia	Corea del Sur	Alemania	Japón	Alemania	China
5	Japón	Suiza	Suecia	Singapur	Reino Unido	Reino Unido	Alemania
6	Suecia	Países Bajos	Singapur	Israel	Singapur	Francia	Singapur
7	Canadá	Estados Unidos	Reino Unido	Francia	Países Bajos	Países Bajos	Reino Unido
8	Alemania	Japón	Nueva Zelanda	Malasia	Alemania	España	Malasia
9	Nueva Zelanda	Alemania	Arabia Saudita	Estonia	Francia	Estonia	Corea del Sur
10	Israel	Suecia	Canadá	Países Bajos	Suiza	Canadá	India

Fuente: Elaboración propia con base al NCPI (2020).

A diferencia del análisis del IIC, para el índice de capacidades presentamos un análisis por país, centrado en presentar el análisis de las cinco superpotencias del ciber espacio, establecidas por el NCPI (2020):

- *Estados Unidos:* el país obtiene la puntuación más alta en cinco de siete objetivos. Sólo se queda detrás de Rusia en la dimensión de ofensiva, y de China en la de

defensa, en esta última es importante destacar que ocupó el séptimo lugar entre 30 los países analizados. La ponderación se atribuye al desarrollo de sus ciber capacidades, la defensa cibernética nacional es un objetivo que está bien establecido en sus ENCS, como vigilancia, información y control e inteligencia destacan ampliamente a razón del potencial que tienen instituciones como el Ciber Comando de los Estados Unidos y la Agencia Nacional de Seguridad (NSA) en el extranjero. Por último, destaca el potencial de país para obtener beneficios comerciales del ciberespacio, aun por encima de China, y el de normativas, al ser el país que empuja normativas de mayor impacto a través de organizaciones como la OTAN.

- *China:* se encuentra entre los cinco primeros en todos los objetivos. Esto se vincula que, en los últimos años, China ha invertido fuertemente en investigación y desarrollo de tecnologías que permitan al país para lograr múltiples objetivos en el ciberespacio. Estos resultados reflejan una posición cada vez más dominante de China en el ciberespacio, pero también destacan la brecha significativa en la capacidad entre China y los EE. UU. en la mayoría de los indicadores.
- *Reino Unido:* obtiene una puntuación alta en dos dominios (vigilancia e inteligencia), esto no es de extrañar a razón que el país ha ocupado tradicionalmente posiciones sólidas tanto en la recopilación de inteligencia extranjera para fines de seguridad nacional y la vigilancia y monitoreo de grupos nacionales. También, ha dedicado una cantidad sustancial de dinero público a fortalecer sus capacidades para lograr varios de los objetivos evaluados.
- *Rusia:* se posiciona a la vanguardia del objetivo ofensivo, esto es debido a que el país cuenta con un comando cibernético establecido y una doctrina militar cibernética detallada. Del mismo modo, destaca su presencia en la opinión pública internacional al ser noticia en la última década por adjudicársele una gran cantidad de ciberataques disruptivos en diferentes países. Esta es una clara demostración de su capacidad para destruir e interrumpir la infraestructura del adversario y de su alto potencial para ciber operaciones con la finalidad de alcanzar un objetivo estratégico. Su segunda fortalece se asocia a la dimensión de información y control, por el nivel de control en su territorio que tiene de información extranjera. Fuera de esas dos dimensiones el país se encuentra bastante atrás, en los otros cinco objetivos estratégicos.

- *Israel*: el país constantemente es señalado por estar en la cima del desarrollo de ciber capacidades, por gran cantidad de instituciones, centros de investigación y expertos en ciberseguridad, quienes destacan su desarrollo en torno a la recopilación de inteligencia y ofensiva en el ciberespacio. Sin embargo, el NCPI (2020), lo coloca sólo en dos indicadores entre los diez principales países de la medición, que es el caso de inteligencia, dónde ocupa la quinta posición. Y vigilancia, dónde está en el décimo lugar. El mismo Belfer Center expresa que si ponderación presenta una anomalía, sin embargo, esto puede explicar por factores como el hecho de que el NCPI (2020) sólo utiliza datos de fuentes abiertas, y gran parte del programa cibernético de Israel está coordinado y dirigido de forma encubierta y no en el sector público o empresarial. También, al hecho de que el país no tiene en concreto amplio desarrollo en ciber capacidades es de carácter industrial o la dimensión económica, así como otras medidas clave dentro del NCPI (2020).

3.7 Grupos de Amenazas Persistentes Avanzadas (APTs)

Como se mencionó en la sección anterior, el NCPI (2020) es una métrica centrada en analizar las ciber capacidades y ciber poder de Estados-Nación a través de fuentes abiertas o la información proporcionada por los treinta países que son considerados dentro de la medición. Una particularidad, que destaca es el caso de Israel, que es considerado una superpotencia dentro del ciberespacio, pero que en los hechos sus ponderaciones en los siete objetivos presentan niveles que parecen una subestimación de sus capacidades. Lo anterior, se debe que gran parte de los datos necesarios para calibrar un nivel de ciber poder no están abiertos al público y se manejan de forma encubierta, en ese sentido, la falta de transparencia se vuelve un factor que no permite analizar de forma efectiva el nivel de ciber poder de un determinado actor nacional.

Lo anterior, se vuelve una problemática con un conjunto de países que siempre están la opinión pública internacional, a razón de ser señalados como actores que constantemente utilizan el ciberespacio para perseguir objetivos particulares que los beneficien, como es el caso de países como: Corea del Norte, Israel, Vietnam, China o Rusia. Los cuales a razón de rivalidad que mantienen con occidente, su hermetismo y falta de trasparencia, no presentan las nociones claras sobre cuál es el nivel real de su ciber poder. Analizar las capacidades de

operación y defensiva de este conjunto de países en el ciberespacio es posible a través de la categoría de Amenazas Persistentes Avanzadas (*Advanced Persitent Threat* por sus siglas en inglés o APTs), el cual ha sido acuñado para definir riesgos de ciberseguridad de mayor gravedad y con efectos más dañinos, a través de equipos especiales de programadores o hackers, formados por este conjunto de naciones y resguardados por ellos (Daly, 2009; Tankard, 2011).

Los APTs son trascendentes en el análisis del ciber poder, por su capacidad de perdurar en el tiempo a través de la realización de ciber operaciones. Esto lo realizan por medio de la explotación de las vulnerabilidades desconocidas oficialmente por los equipos o sistemas informáticos de gobiernos u empresas privadas, con información de alto valor estratégico o en términos de propiedad intelectual, por lo cual son amenazas dirigidas a objetivos concretos. Su principal fin es realizar acciones de ciber espionaje a empresas, gobiernos y entidades militares. Comprometiendo la seguridad de una red para conseguir información. De esta forma, con base Chen, Desmet & Huygens (2014) los tres elementos que identifican a las APTs y describen dicho acrónimo son los siguientes:

- *Amenazas:* a razón que este tipo de actores realizan ciber operaciones que persiguen objetos concretos e importantes, viables de ser alcanzados en el corto plazo.
- *Persistente:* vinculado a la planificación, sofisticación y estructuración de los ataques que combina diferentes técnicas de explotación para afectar la confidencialidad de los datos, por medio de un conjunto de actividades y procesos de alta complejidad bajo un contexto sigiloso y continuo de planeación con la motivación de quebrantar la seguridad de un sistema informático o actor bajo métodos no convencionales.
- *Avanzada:* relacionado al hecho de los APTs y sus modos de ataque, normalmente presentan grandes innovaciones en el instrumento de ciber arma o malware, o del modo de operación del ataque, que gran cantidad de las veces fue diseñada para alcanzar un objetivo específico. De esta forma, los APTs son actores que innovadores que realizan ataques de características de *Día Zero*, con el fin de manifestarse con un programa diseñado para mantenerse oculto en el sistema atacado, aprovechar vulnerabilidades desconocidas y utilizar técnicas de ingeniería social sobre un

objetivo concreto, con lo que se alejan de las herramientas de malware tradicional (Chen, Desmet y Huygens, 2014).

Los anterior presenta que actores detrás de una APT son un grupo de especialistas en hacking y programación, que al trabajar para gobiernos u organizaciones militares; cuentan con grandes recursos. En ese sentido, Bhatt, Yano & Gustavsson, P. (2014) presentan seis fases para analizar como operan las APT:

- *Reconocimiento:* recolectar información de los objetivos mediante la observación, para esto, es usado técnicas de ingeniería social e Inteligencia de Fuentes Abiertas (*Open Source Intelligence* por sus siglas en inglés u OSINT).
- *Intrusión inicial:* los atacantes envían las herramientas (*exploits*) para infiltrarse. Existen dos mecanismos comumente utilizados: i) intrusión inicial directa (envíos de exploits usando técnicas como phishing) ii) intrusión inicial indirecta: uso de terceros que tengan relación con el objetivo para hacer llegar los *exploits* a su objetivo.
- *Inicio del comando y control:* el objetivo es establecer una puerta trasera que permite al atacante tomar el control del sistema comprometido. Para los atacantes es importante mantener el anonimato, para esto, utilizan varias herramientas para explotar el sistema informático.
- *Obtención de credenciales:* una vez que los sistemas de comunicación están comprometidos, los APT pueden moverse dentro del entorno para expandir el control en los sistemas, para esto es necesario asegurarse de obtener las credenciales de accesos privilegiados del sistema en cuestión.
- *Instalación de herramientas:* implantar todos los instrumentos necesarios para asegurar la explotación del sistema y alcanzar el objetivo de la ciber operación.
- *Extracción de datos:* supone la culminación de la operación y la extracción exitosa de la información en cuestión.

Las operaciones de los APTs y su impacto en la ciberseguridad, con secuelas a la seguridad nacional o reputación institucional son famosos a nivel global. Por ejemplo, en 2010 el malware Stuxnet fue detectado por la empresa VirusBlokAda y causó un fuerte impacto en Irán, en concreto en la central nuclear de Natanz, Irán, por su diseño exclusivo para infectar

equipos Windows y afectar a sistemas SCADA. Con base a Langner (2011), Stuxnet infectó el sistema informático de la central de Natanz mediante USB infectado que afectó severamente el programa nuclear iraní, con una afectación lo retraso hasta por dos años. La modalidad del ataque fue tan sofisticada que se encontraron muestras de *Stuxnet* en sistemas informáticos de Indonesia, Irán, China. Otros casos representativos de malwares y ataques de APTs son *The Flame*, identificado en 2012, que vulneró múltiples sistemas de países de Medio Oriente o *Medre* un malware utilizado por APTs con objetivos industriales y militares capaz extraer información de estratégica para la defensa nacional o la propiedad intelectual. De acuerdo con la agencia estadounidense de ciberseguridad Fire Eye (2022), han sido identificadas al menos de 39 APTs, resguardadas por países como Rusia, Irán, Corea del Norte, China y Vietnam. A continuación, presentamos un análisis por país y sus principales APTs.

3.7.1 China

China es el país con más APTs según los análisis de Fire Eye (2020), con un total de 30, lo que representa más del 75% de todas las organizaciones de este tipo identificadas por esta firma de ciberseguridad. De mismo modo, es uno de los países con registros de APTs más antiguos, sus orígenes se remontan al año 2002, en el cuál el Departamento de Estado presentó evidencia de las primeras ciber operaciones de la Unidad 61398 del Ejército Popular de Liberación, un comando cibernético que se dedicaba a la infiltración de sistemas informáticos de empresas líderes en varios sectores de los Estados Unidos (Bejtlich, 2013; Li, Lai & Ddl, 2011). De esta forma, es visible observar que la nación asiática utiliza los grupos APTs como un medio de sustracción de información de propiedad intelectual, con aparentes fines de mejorar las capacidades de múltiples de sus industrias nacionales. Algunos de los sectores específicos de esta acción son: industria química (con información extraída por APT 1 y APT 23), industria aeroespacial (APT 1, 3,4 y 18), firmar de tecnología (APT 1, 16 y 40). En sí, existen grandes hipótesis de expertos en ciberseguridad, que el gran avance industrial y tecnológico de compañías chinas de los últimos años, que en determinado sector han alcanzado o se han homologado con grandes firmas de Estados Unidos, se debe a la acción de las APTs (Fu *et al.*,2015). Con lo cual China usaría este tipo de organizaciones como un actor trascendental para abonar a su ciberpoder y consolidarse como la nación más

importante en determinados sectores industriales y tecnológicos. Dando ventajas a su posición internacional y poder nacional.

Del mismo modo, es importante destacar que si bien el país ha centrado la operación de sus APTs en ciber ataques y operaciones a entidades privadas. También, las utiliza para acciones de espionaje e inteligencia a actores a los que considera adversarios u oponentes en su consolidación internacional. Tal son las evidencias de Fire Eye (2022) en torno a APT 16, dedicado a buscar información política y de periodistas en Taiwán, APT 23 y 24, dedicadas a recolectar información sensible y confidencial de personal político y organizaciones en los Estados Unidos, países de Europa, Filipinas y Taiwán. O APT 30, para realizar acciones de inteligencia en sus socios de la ASEAN (Kao, 2015). Por último, destaca el papel de APT 20, que se es un instrumento de inteligencia y colaboración del gobierno chino con Rusia para la seguridad de euroasiática, y el papel de APT 12, dedicado a monitorear periodistas nacionales de China y sus vínculos con el extranjero, con lo cual está realizando una acción de vigilancia y control de la información. Una relación completa de las APTs de China se presenta en la tabla 22.

Tabla 22. APTs de China, sectores claves y esferas de impacto.

ORGANIZACIÓN	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 1	Firmas de tecnología	Capacidad de robar información a diversos grupos de manera simultánea
	Aeroespacial	Centrado en objetivos de industrias que hablan inglés
	Administración pública	
	Investigación científica	
	Industria energética	
	Transporte	
	Construcción	
	Firmas de ingeniería	
	Servicios legales	
	Industria química	
	Servicios financieros	
	Alimentación y agricultura	
	minería	
	Educación superior	

ORGANIZACIÓN	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 2	Industria de defensa	Objetivo es robo de propiedad intelectual
APT 3	Aeroespacial	Después de explotar el host destino, descargará rápidamente las credenciales y se moverá a hosts adicionales para crear puertas traseras personalizadas.
APT 4	Aeroespacial	Apunta a las bases industriales de defensa
APT 5	Telecomunicaciones	Objetivo en compañías especializadas en satélites.
APT 6	Transporte	Objetivo es robo de propiedad intelectual
APT 7	Construcción	Objetivo es robo de propiedad intelectual
APT 8	Telecomunicaciones	Objetivo es robo de propiedad intelectual
APT 9	Industria de salud	Objetivo es robo de propiedad intelectual
APT 10	Construcción	Centrado en los objetivos de seguridad nacional China.
APT 12	Periodistas	Grupos independientes que realizaban acciones de espionaje, además, tienen relación con el Ejército Popular de liberación China
APT 14	Personal gubernamental	Objetivo es robo de propiedad intelectual
APT 15	Sector comercial	Objetivos tenían múltiples ubicaciones, desde EE.UU, Europa y Sudáfrica.
APT 16	Firmas de tecnología	Grupos con sede en China que buscaban información política y periodística de Taiwán.
APT 17	Personal gubernamental	Realizar intrusiones en la red contra objetivos específicos
APT 18	Aeroespacial	Se ha publicado muy poca información sobre este grupo

ORGANIZACIÓN	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 19	Servicios legales	Grupos independientes que realizaban acciones de espionaje bajo petición del gobierno chino.
APT 20	Firmas de ingeniería	Robo de datos en apoyo a operaciones de espionaje tradicional
APT 21	Personal gubernamental	Recolectar información de temas de seguridad nacional rusa
APT 22	Entidades políticas	Recolectar información militar
APT 23	Telecomunicaciones	Recolectar información de personal gubernamental de EE.UU y Filipinas
APT 24	Sector salud	Recolectar información de organizaciones con sede en EE.UU y Taiwán
APT 25	Industria de defensa	Recolectar información comercial de usuarios
APT 26	Aeroespacial	Objetivo es robo de propiedad intelectual
APT 27	Organizaciones internacionales con sede en América del Norte, Sur, Europa y Medio Oriente	Objetivo es robo de propiedad intelectual
APT 30	Miembros de ASEAN	Actividad sostenida por largo período de tiempo
APT 31	Personal gubernamental	Espionaje chino
APT 40	Firmas de ingeniería	Monitoreo y vigilancia a países relacionados con la Nueva Ruta de la Seda
APT 41	Sector salud	Monitoreo y vigilancia a individuos específicos

Fuente elaboración propia con base a Fire Eye (2020).

3.7.2 Rusia

Para el caso de Rusia la evidencia de los análisis de Fire Eye (2022) sólo identifica dos APTs y muestra que su principal operación se encuentra en su zona de influencia geopolítica, para el caso concreto del Cáucaso y Europa Occidental (Lemay, 2018). En ese sentido, se puede argumentar que gran cantidad de las ciber operaciones del país se concentran en naciones como Georgia, Ucrania o los países de la Unión Europea. Destaca, que no exista evidencia

sobre las acciones de inteligencia rusa, o que no utilice a las APTs con intereses de posicionamiento económico, para el control de la información nacional o vigilancia de la población. Por último, Fire Eye (2022) no presenta APTs centradas en ciberoperación de inteligencia en Estado Unidos u otros países occidentales con fines políticos (Ghafir & Prenosil, 2014). La clasificación de las APTs rusas se presenta en la tabla 23

Tabla 23. APTs de Rusia, sectores claves y esferas de impacto.

ORGANIZACIÓN	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 28	Cáucaso, en particular Georgia	Intentos de recolectar información geopolítica
APT 20	Gobiernos de Europa occidental	Grupo de amenaza adaptable y disciplinado que oculta su actividad en la red de una víctima

Fuente elaboración propia con base a Fire Eye (2020).

3.7.3 Irán

El caso de Irán es el de un país hermético sobre el que se reconocen capacidades efectivas de disuasión y para llevar a cabo ciber operaciones con la finalidad de alcanzar objetivos estratégicos para su interés nacional. El amplio desarrollo de la nación de ciber poder en este campo se debe a ser víctima de importantes ciber ataques que han marcado precedentes de como el ciberespacio puede influir en la política internacional y afectar la seguridad nacional (Farwell & Rohozinski, 2011). Con el caso representativo del gusano Stuxnet (2011) y sus efectos en la central de Natanz, se han transformado en una de las vulneraciones más grande que pudo sufrir un Estado-Nación a su interés nacional materializado en su proyecto nuclear que sufría varios altibajos y atrasos por dicha operación cibernética (Barzashka, 2013).

En ese sentido, Fire Eye (2020) identifica un total de cuatro APTs reguardadas bajo la tutela del gobierno iraní. Con esto se corona como el segundo país con más número de este tipo de organizaciones lo que representa el 10% del total identificadas por la firma de ciberseguridad. En ese sentido, destaca que la nación utiliza a APT 34 y 39 para acciones de inteligencia y vigilancia de bolsas de valores e instituciones financieras alrededor del mundo y medios de comunicación, agencia y proveedores de telecomunicaciones (Cohen, 2019). APT 35 y APT 33 se centran en inteligencia de carácter militar y en la realización de acciones ofensivas a

industria aeroespacial en naciones como Estados Unidos, Arabia Saudita y Corea del Sur, con lo cual quedan en manifiesta las capacidades efectivas de acción y daño de esta nación del Medio Oriente (Baezner, 2019).

Tabla 24. APTs de Irán, sectores claves y esferas de impacto

ORGANIZACIÓN	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 33	Aeroespacial	Ataque a industrias de EE. UU, Arabia Saudita y Corea del Sur
APT 34	Servicios financieros	Monitoreo y vigilancia a largo plazo
APT 35	Personal militar	Patrocinado por el gobierno iraní para espionaje
APT 39	Telecomunicaciones	Monitoreo y vigilancia a individuos específicos

Fuente elaboración propia con base a Fire Eye (2020).

3.7.4 Corea del Norte y Vietnam

En el análisis del NCPI (2020) presenta a las naciones de Corea del Norte y Vietnam con países con una posición preponderante en el IIC. Esto demuestra que ambos países se ven a sí mismos como potencias del ciberespacio y cada vez consideran a este un dominio trascendental para abonar a su ciber poder y poder nacional. En este sentido, el Belfer Center reconoce su ascenso en el panorama internacional de la ciberseguridad y la consolidación de sus capacidades efectivas para realizar ciber operaciones o perseguir intereses nacionales a través del internet.

Sobre lo anterior, FireEye (2022) da fe de las capacidades de ambas naciones al identificar a dos APTs, bajo la tutela norcoreana, y una bajo la vietnamita. En el caso de Corea del Norte, sus ciber operaciones se centran en acciones estratégicas en la industria química y en los servicios financieros (Lee, 2018). En este caso, el caso de APT 38 es reconocido como la mayor organización de este tipo, responsable de atracos económicos a bancos centrales y sistemas financieros de países de múltiples regiones del mundo como Europa, América del Norte, Latinoamérica y Asía (Yang, Kim & Oh, 2016). Con lo cual, se identifica un *modus operandi* de extracción de divisas internacionales, para posteriormente ser depositadas a través de métodos de encriptación a cuentas del gobierno norcoreano, que se dice, son de importancia para su manutención en los últimos años.

Por último, destaca que Vietnam cuenta con la APT 32, una institución dedicada acciones de inteligencia, que se en la recopilación de información de fuentes abiertas y clasificada, de amenazas y riesgos que puedan afectar a las empresas que desean invertir en su país (Baezner, 2018). Con lo cual este país estaría utilizando el dominio del ciberespacio para su consolidación como actor de trascendencia comercial en Asía y en aras de su prosperidad económica.

Tabla 25. APTs de Corea del Norte e Irán, sectores claves y esferas de impacto

ORGANIZACIÓN	PAÍS	SECTORES, ACTORES O INDUSTRIAS CLAVE	ESFERAS DE IMPACTO.
APT 37	Corea del Norte	Industria química	Uso de Malwares de extracción de información.
APT 38	Corea del Norte	Servicios financieros	Responsables de llevar a cabo los mayores atracos cibernéticos observados.
APT 32	Irán	Construcción	Amenaza para las empresas que buscan hacer negocios en Vietnam.

Fuente elaboración propia con base a Fire Eye (2020).

Capítulo 4. Estudio de caso: *Russigate* y *Solar Winds* ¿el ciberespacio como instrumento para vulnerar la soberanía del Estado Nación?

Introducción

Terminada la conceptualización teórica en torno a los vínculos entre soberanía, seguridad nacional y política exterior con ciberseguridad, es momento de asentar el análisis en torno al ciberpoder y desarrollo de cibercapacidades para probar la hipótesis de la que parte el presente estudio, centrada en probar que el ciberespacio es una nueva arena de la política internacional a través de la cual es posible vulnerar la soberanía de un Estado-Nación. Para esto, se ha escogido el caso de *Russiangate* o la intromisión de actores rusos en la elección presidencial de los Estados Unidos de 2016.

La estrategia metodológica para el análisis se dividirá en cuatro fases:

1) Un análisis de fuentes abiertas a través de medios de prensa, mediante el cual se presentará una narrativa y contextualización de lo que fue el *Russiagate*. Desde el periodo de campaña de 2016 que confronto a Hillary Clinton y Donald Trump, pasando por la creación de la Fiscalía Especial para la investigación de la interferencia rusa en las elecciones presidenciales de 2016 y la publicación del Informe Mueller. Para terminar con el polémico fin del gobierno de Trump y el descubrimiento del ciberataque de *SolarWinds* en los primeros meses de la administración del presidente Joe Biden.

2) Un análisis del contenido del *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016,* presentado por el Fiscal Especial Robert Mueller el 18 de abril de 2019, en el cuál se presentan los resultados de su investigación especial en torno a los nexos de Donald Trump con agentes del gobierno ruso, y como pudo orquestarse una ciber operación de esta nación que inclinó la balanza de la disputa electoral a un triunfo de dicho candidato. En esta sección, se analizan los volúmenes I y II, el primero vinculado a las ciberoperaciones rusas en el marco del proceso electoral de 2016 y la transición del equipo de campaña de Trump, hasta tomar la presidencia. El segundo, vinculado a los episodios de

osbtrucción de justicia del presidente, para evitar que la investigación de la Fiscalía Especial se llevará a cabo, y culminó en diez episodios de obstrucción de justicia.

3) Un análisis de las cibercapacidades de los Estados Unidos y Rusia, a través de las métricas del NCSI (2019), GCI (2018), y el NCPI (2020) para valorar la evidencia presentada por el análisis de fuentes abiertas y el análisis al Informe Mueller, para valorar con dichas metodologías la viabilidad del éxito de una ciberoperación rusa en las elecciones presidenciales de 2016. En este apartado se analizará la capacidad de ofensa y defensa de ambas naciones, así como su nivel de cibercapacidades para realizar una operación a través del ciberespacio que vulnere la seguridad nacional y soberanía.

4) La realización de un total de diez entrevistas con especialistas en ciberseguridad de las Américas, y la realización de un análisis de teoría fundamentada de los comentarios estratégicos obtenidos en cada conversatorio, con el fin de realizar un análisis sobre la viabilidad de la intromisión de Rusia en las elecciones de Estados Unidos de 2016. Con base a determinar si está puede ser considerado una violación a la soberanía nacional y la consolidación del dominio del ciberespacio para realizar esta acción.

4.1. Análisis de Fuentes Abiertas

Para el presente análisis de fuentes abiertas se realizó una búsqueda en medios de prensa y comunicación, así como en documentos gubernamentales de interés relacionados a la investigación y polémica del *Russiangate,* en el marco de la elección presidencial de Estados Unidos de 2016 y la presidencia de Donald Trump. La búsqueda se realizó de manera anual para el periodo del 2016 al 2021, abarcando un total de seis años. En total se revisaron un total de 121 documentos que permiten la reconstrucción a través de esta metodología, la sucesión de eventos vinculados a las polémicas enmarcadas en este suceso.

Del mismo modo, para su análisis eficiente y concreto, la información se dividió en tres diferentes tramas, las cuales son: a) *Russiangate,* que engloba las sospechas y polémicas del proceso electoral en el que se enfrentaron Hillary Clinton y Donald Trump, hasta la consumación de su triunfo, y todo el desarrollo de la investigación especial del Fiscal Robert Mueller. b) *Impeachment,* con relación a los esfuerzos del marco institucional de los Estados Unidos, por destituir a Donald Trump por procesos de obstrucción de justicia, derivados del informe presentado por la Fiscalía Especial, para la investigación de la interferencia rusa en

las elecciones presidenciales de 2016. Los cuales culminaron con intentos de deponer a Trump hasta los últimos días de su gobierno. c) *SolarWinds,* la detección del ciberataque y vulneración más grande de la historia de los Estados Unidos denominado con este nombre, que afectó a más de quince mil agencias relacionadas al gobierno y sector privado de este país. En el cuál se identificó fue ejecutado como una ciberoperación por parte del gobierno ruso y ponen en tela de juicio la capacidad de Rusia por haber ejecutado una ciberoperación semejante para dañar el proceso electoral de 2016. Por último, en la tabla 26 presentamos la sistematización de estas fuentes abiertas para el presente análisis.

Tabla 26. Sistematización de fuentes abiertas para análisis de tramas Russiangate, Impeachment y SolarWinds.

No.	Año	Total de documentos	Trama
1	2016	24	Russiangate
2	2017	25	
3	2018	23	
4	2019	21	
5	2020	15	Impeachment
6	2021	13	SolarWinds
	Total	**121**	

Fuente: Elaboración propia.

4.1.1 Trama Russiangate

4.1.1.1 Año 2016

La trama del *Russiangate* comienza con el nombramiento de Donald Trump, por parte del Partido Republicano, y de Hillary Clinton, del lado del Partido Demócrata, como los protagonistas de la elección presidencial más polémica de la historia reciente de los Estados Unidos. La Convención Nacional Republicana avaló la candidatura de Donald Trump el 16 de julio de 2016, con un triunfo de 1,237 votos, en la que derrotó a otros candidatos como Ted Cruz y John Kasich. El triunfo de Trump fue visto como el primer posicionamiento de un candidato republicano no perteneciente a la elite del partido en casi treinta años (Collinson, 2016).

Para los expertos en prensa, el triunfo de Trump representó una rebelión en contra del *establishment* de esta fuerza política, que tenía como sus líderes en el congreso a John Boehner y Eric Cantor. Quienes definieron las candidaturas presidenciales de personajes como Mitt Romney, en 2012, y John McCain, en 2008, que para los simpatizantes republicanos representaban al máximo a la más alta cúpula del partido (Cassidy, 2016). Si

bien, el triunfo de la candidatura de Donald Trump estuvo acompañado de una ambigua visión antisistema entre los simpatizantes del Partido Republicano, algunos analistas también resaltan que su carisma y su dominio en redes sociales ayudaron a incrementar su grado de convocatoria entre la población.

Por otra parte, la conducta de confrontación y la fuerte presencia mediática de Trump en medios de comunicación, lo ayudó a ganar la candidatura. En sí, su perfil político fue descrito "*como una combinación de agresividad, espectáculo y descalificaciones, donde se discuten los problemas domésticos* [de Estados Unidos]" (Maiquez, 2016). No obstante, ante su elección gran parte de la elite tradicional del Partido Republicano se refirieron a él como un *outsider* o un *no autentico republicano o conservador* dados sus puntos de divergencia política en determinados temas que, podían tener fuertes impactos en cuestiones de gobernabilidad interna y el papel que juega Estados Unidos a nivel mundial (Tomasky, 2015). Ante esto, diversos líderes de opinión en medios de comunicación expresaron que Trump había *secuestrado al partido* al utilizar un discurso populista, que supo aprovechar el malestar y descontento de la gente. Sin embargo, a pesar de las diferencias entre los otros grupos y personalidades al interior del partido, y divergencias entre los distintos sectores de electores, los miembros y militantes del partido expresaron que apoyarían al candidato en las elecciones de 2016, en contra del Partido Demócrata (Eatwell y Goodwin, 2018).

Para el caso de Hillary Clinton, es importante mencionar que la demócrata anunció su campaña para la presidencia de Estados Unidos y sus pretensiones de convertirse en la candidata del Partido Demócrata, el 16 de abril de 2015. A pesar de contar con una larga trayectoria en el gobierno y haber sido la primera dama durante la presidencia de su marido William Clinton, de 1993 a 2001, la representante demócrata era vista con mucha desconfianza y rechazo por una gran parte del electorado de su partido (Luhby, 2016). Así como considerada una perfecta representante de la elite política tradicional de Washington D.C., con la que existía un fuerte descontento de parte de la población estadounidense (Fajardo, 2016).

En el ámbito de la competencia interna del Partido Demócrata por la nominación de la candidatura presidencial, Clinton compitió contra dos figuras, la primera fue Martín O'Malley, el ex gobernador de Maryland con poca representatividad y presencia política a

nivel nacional. Sin embargo, su segundo adversario, el senador por Vermont, Bernie Sanders, se perfiló con una fuerte presencia política que amenazó su candidatura en más de una ocasión, hasta que alcanzó la nominación de su partido. Lo anterior, se debió al hecho de que Sanders jugó un papel de imagen reflejó de Trump al interior del Partido Demócrata. Ya que a los ojos de los militantes y simpatizantes demócratas Sanders era visto como un *outsider* o un político que no había formado parte de la clase hegemónica del partido (BBC, 2016). Asimismo, su auto denominación como *socialista* y vinculación con causas populares como el incremento del salario mínimo, la mejora del sistema de salud, y críticas a los excesos de las grandes corporaciones estadounidenses, lo hacían ver como una figura innovadora en el ámbito de la política nacional y principalmente con el electorado menor a los 29 años (Bassets, 2016).

Esta imagen se reforzó con el inició de la campaña de Sanders, el 30 de abril de 2015, en la que lanzó la promesa de una *revolución* al interior de la política de Estados Unidos, en caso de que él se convirtiera en presidente (Gambino, y Pamkhania, 2016). Esta imagen revolucionaría de Sanders se reforzaría durante el primer debate de los candidatos demócratas llevado a cabo el 13 de octubre de ese mismo año, en Las Vegas, en el que fue visto como el mejor, muy por encima de Clinton y O´Malley (Stracqualursi, 2016). El éxito de Sanders se extendería hasta episodios clave de la elección presidencial como el *Caucus de Iowa*, el 1 de febrero de 2016, en el que casi derrota a Hillary Clinton al quedarse sólo 0.23% de las votaciones por debajo de ella (BBC, 2016). Sin embargo, con el inicio de las elecciones primarias de los Estados para la nominación demócrata, en New Hampshire, Sanders derrotó con 60.4% contra 37.68% de los votos a Clinton. Con lo que marcó que sus pretensiones por convertirse en el candidato del Partido Demócrata eran seria y desafiarían seriamente a su adversaria (Bassets, 2016).

También, las complicaciones que sufrió Clinton por la nominación demócrata se complicaron por el discurso que utilizó Donald Trump, en contra de ella. En más de una ocasión el republicano se refirió a Clinton como "*más de lo mismo del entorno elitista y corrupto de Washington"* (Luhby, 2016). Este discurso se reforzó por la fuerte vinculación que tenía Clinton con figuras políticas de la capital y gobierno, así como sus relaciones personales con importantes figuras del sector empresarial y financiero (Bassets, 2016). Por último, se destaca

que Trump reforzó la figura de Clinton como una representante de la elite política de Estados Unidos al hacer promoción de un reportaje que publicó el *New York Times,* el 2 de marzo de 2015, en el que el periódico expresó que durante su gestión al frente de la Secretaría de Estado, Clinton utilizó su cuenta de correo personal, en contraposición de su correo gubernamental como era debido al ser funcionaria del gobierno.

Dicha acción violó lo establecido en la *Ley de Registros Federales de Estados Unidos*, que estipula que la correspondencia de los funcionarios del gobierno debe hacerse a través de vías formales, dado que esta se reserva para ser estudiada y revisada en el futuro (Schmidt, 2015). Lo que obligó a Clinton a entregar al Departamento de Estado más de 55,000 páginas de correos electrónicos generados durante su gestión al frente de dicha institución, los cuales tuvieron que ser revisados y posteriormente publicados para demostrar que no se había involucrado en acciones en las que utilizara su posición gubernamental para su beneficio personal (Fazekas, 2016).

Los eventos anteriores dieron a Clinton una imagen de secretismo y un aura de considerarse a sí misma una personalidad para quien no aplicaban las leyes normales para el resto de la población estadounidense. Lo que hizo que su imagen se volcara en la de una política deshonesta, poco transparente y confiable, que se incrementaran en durante los últimos meses de la campaña presidencial, que fomentaron una enorme polarización en el ámbito social de los Estados Unidos. De hecho, una encuesta publicada por el *The Washigton Post* presentó que en lo últimos tres meses de campaña la opinión desfavorable en contra de Hillary Clinton pasó del 49% al 51%, al mismo tiempo que la popularidad de Trump se incrementaba en casi el mismo margen (Cano, 2016). A pesar de estos altibajos, el 12 de julio Sanders expresó que apoyaba y haría todo lo que estuviera en su posición como senador para ayudar Clinton en convertirse en la presidenta de los Estados Unidos de América (Chozick *et al.,* 2016). Con lo cual, hizo historia el 28 de julio al convertirse en la primera mujer en ser nombrada la candidata del Partido Demócrata por la Convención Nacional de su partido (Gambino y Pamkhania 2016; Stracqualursi, 2016).

No obstante, el acontecimiento y la controversia más grande en torno a la elección presidencial de Estados Unidos de 2016 estaban aún por materializarse. El 7 de octubre de 2016, un mes antes de la fecha fijada para la jornada electoral de Estados Unidos, el portal

Wikileaks publicó un total de 2,000 correos electrónicos vinculados a la correspondencia que había mantenido Hillary Clinton con su entonces jefe de campaña Mike Podesta. Ese día se iniciaría la publicación de una serie de tandas de *e-mails* con información suficiente para comprometer la imagen pública y política de Clinton, así como sus aspiraciones presidenciales (Ximénez, 2016). En un total de seis tandas, que culminaron el 13 de octubre, *Wikileaks* publicó un total de 9,124 correos vinculados a la Convención Nacional Demócrata realizada durante el mes de julio, las campañas presidenciales de Clinton y Bernie Sanders, y las relaciones personales de la familia Clinton con empresarios o personalidades vinculadas al sector financiero, así como opiniones de gente involucrada en su campaña (Frank, 2016). Los contenidos de las temáticas de los correos se presentan en la tabla 27.

Tabla 27. Filtraciones de Wikileaks de correspondencia Clinton-Podesta.

Fecha de filtración	Total de correos	Temáticas
7 de octubre	2,060	Discursos y relación con banca privada Guerra Civil de Siria Campaña de Bernie Sanders Estado Islámico y refugiados en Medio Oriente
10 de octubre	1,190	Relaciones extramaritales de William Clinton Temas diplomáticos con Arabia Saudita, Qatar Temas Diplomáticos con El Vaticano
11 de octubre	1,193	Relación de Barack Obama con candidatura de Clinton. Campaña de Donald Trump. Campara de Bernie Sanders Vínculos de Hillary Clinton con el Departamento de Justicia de EUA
12 de octubre	673	Campaña de Bernie Sanders. Relación de Hillary Clinton con los medios de comunicación. Relación de Hillary Clinton con la clase media.
13 de octubre	2,000	Manejo de redes sociales de Clinton. Campaña de Berni Sanders y Donald Trump. Campaña de Hillary Clinton.

Fuente: Elaboración propia con base en Katehon (2016).

La filtración causó alto revuelo político ya que se dio en el contexto de la publicación de un audio por parte del periódico *The Washington Post*, en el que se escuchaba a Donald Trump hacer comentarios peyorativos en contra de las mujeres, que buscaba tuviera impacto en el incremento reciente que mostraban las encuestas en torno a su candidatura (Pereda, 2016).

Ambos actos causaron un efecto polarizador en la recta final de la campaña que, gran cantidad de analistas políticos indican impactaron en la intención de voto, de ambos candidatos en el mes previo, al día de la elección. A tal grado que miembros del equipo de campaña de Hillary Clinton, y representantes del Partido Demócrata, hicieron múltiples declaraciones de que existía una ciberoperación, orquestada por el gobierno de Rusia, que buscaba dañar la imagen de Clinton e inclinar la balanza para un inminente triunfo de Donald Trump (BBC, 2016b). Ante esto, agencias de seguridad nacional de Estados Unidos como el FBI (Buró Federal de Investigaciones), la CIA (Agencia Central de Inteligencia) y la Agencia de Seguridad Nacional (NSA), descubrieron que "*individuos con vínculos al gobierno ruso*" publicaron miles de emails hackeados de la campaña del Partido Demócrata. Con el objetivo de influir en los electores a favor de Donald Trump y dañar la campaña presidencial de Hillary Clinton. También, se especula, hackearon los sistemas informáticos del Comité Nacional del Partido Republicano. En los días posteriores a la publicación de la correspondencia, información de diversos medios indicaron que la filtración se realizó a través de un hackeó operado la organización hacktivista *DCLeaks* y un hacker que operaba por sí mismo de origen rumano, denominado *Guccifer 2.0* (Mueller, 2019).

Según la evidencia presentada, en marzo de 2016, estos actores iniciaron el hackeó de cuentas personales de voluntarios asociados a la campaña presidencial de Hillary Clinton, que posteriormente sirvieron para obtener claves de acceso, las cuales permitieron ingresar a las cuentas privadas y red de la Convención Nacional Republicana en julio de ese mismo año. Más tarde, a los correos electrónicos de los altos mandos que coordinaban la estrategia electoral de Clinton. Para que una vez que fue extraída la información, *DC Leaks* y *Guccifer 2.0* transfirieron la información a *Wikileaks* vía mensaje directo en la red social *Twitter* a través de códigos encriptados (Mueller, 2019; Shaban, 2018).

La filtración tuvo efectos en los medios de comunicación que reavivaron la imagen deshonesta y la desconfianza en torno a la figura de Hillary Clinton, vinculados al uso de su cuenta personal para comunicaciones gubernamentales del Departamento de Estado, que le habían causado daños a su campaña electoral desde 2015 (Mars, 2018). Sin embargo, uno de los impactos más fuertes se dio cuando el 28 de octubre de 2016, el entonces director del Buró Federal de Inteligencia (FBI, por sus siglas en inglés) indicó a la prensa que se habían

encontrado un nuevo lote de correos electrónicos de la cuenta personal de Clinton, enviados durante su época de Canciller, y consideraba prudente reabrir las investigaciones en su contra por violar la *Ley de Registros Federales*. Hecho que tuvo un efecto completamente polarizador en los diez días previos a la elección y fue denominado como el "Efecto Comey", posibilidad de que las actuaciones del director hubieran afectado las elecciones (Marcin, 2018).

Las declaraciones de Hillary Clinton, miembros de su equipo de campaña y diversas personalidades asociadas al Partido Demócrata, en torno a una posible ciberoperación orquestada por el gobierno ruso, abrieron el paso a hipótesis de una trama que buscaba afectar el resultado de las elecciones presidenciales de Estados Unidos (Piore, 2019). De hecho, el mismo día que *Wikileaks* publicó la primera tanda de correos vinculados a la correspondencia entre Clinton y Podesta, la Oficina del Director Nacional de Inteligencia (INS, por su siglas en inglés), James Clapper, expresó que las 17 agencias vinculadas a la seguridad nacional de Estados Unidos habían detectado evidencia de que existía una ciberoperación, coordinada desde territorio ruso, que buscaba afectar en los resultados electorales de la elección presidencial de ese mismo año (Nakashima, 2016).

Lo anterior, reposicionó en los medios de comunicación un ciber incidente detectado por el FBI a dos bases electorales de los estados de Ilinois y Arizona, en la unión americana, realizados durante el mes de junio y detectados en el mes de julio (Bruer y Perez, 2016). Dichos ciberataques se dicen fueron realizados por hackers que residían en el extranjero -aunque el director de comunicación del Estado de Arizona, Matthew Roberts, declaró a la prensa que el ciber agresor era de origen ruso-, lo que afirmo la idea del *Russiagate*. Dichos eventos impactaron en la opinión pública en torno a una posible filtración a más bases electorales de los sistemas estatales preparados para le elección presidencial de 2016, lo que claramente afectaría el resultado de los comicios y podría dar ventaja a un candidato (Isikoff, 2016).

En ese contexto, el titular del Departamento de Seguridad Nacional, Jeh Jonhson expresó en una entrevista a la cadena de medios CNN la posibilidad de abrir un debate en torno a considerar a los sistemas electorales como parte de la Infraestructura Nacional Crítica (INC) de Estados Unidos (Bruer y Perez, 2016). Sin embargo, dicha posición fue considerada

polémica por los gobernados de los estados, dado que implicaría una mayor intromisión del gobierno federal en los procesos electorales. A pesar de esta polémica Johnson ofreció protección federal para los sistemas electorales de los Estados, aunque este no fue aceptado. Por último, la discusión se cerró en torno varios comentarios expresados por autoridades gubernamentales y miembros de empresas de software, en el Simposio Gubernamental de Symantec, celebrado en agosto de 2016. En que personalidades como James Comey, director del FBI expresaron en que se tenía la suficiente confianza en las medidas de protección electoral de los estados eran lo suficientemente avanzados para evitar una operación que creará introdujera un algoritmo que afectará el resultado de la elección (Sotomayor, 2016).

En este contexto, el Director Nacional de Inteligencia del gobierno de los Estados (*Director of National Intelligence* o DNI en acrónimo) en conjunto con la toda comunidad de Inteligencia del país (U.S Intelligence Community, USIC) confirmaron que el gobierno de Rusia dirigió los ciberataques para hackear los correos electrónicos de personas e instituciones, incluyendo organizaciones políticas estadounidenses (DNI, 2016). Y que las acciones rusas tuvieron como objetivo intervenir en las elecciones presidenciales de Estados Unidos, por medio de ciber operaciones recurrentes con origen en Rusia, desde países de Europa y Eurasia para influir en la opinión pública. Dado el impacto de los ataques, el USIC consideró que estas actividades fueron autorizadas por personalidades del gobierno ruso del más alto nivel. Frente a esta polémica, algunos estados reportaron que en sus sistemas electorales se encontraron escaneos y sondeos provenientes de servidores rusos. No obstante, el USIC no pudo atribuir dichas actividades al gobierno de Rusia (Bruer y Perez, 2016). Por lo anterior, el USIC en conjunto con departamento de *Homeland Security* concluyen que es extremadamente difícil, incluyendo para un Estado-Nación, el alterar el resultado de las elecciones mediante un ciberataque.

A pesar de este entorno, las elecciones se llevaron a cabo y Donald Trump se transformó en el 45°presidente de los Estados Unidos de América el 8 de noviembre, al alcanzar un total de 306 puntos del colegio electoral para el final de la jornada. Su triunfo causó polémica y revuelo en la prensa nacional e internacional, dado que, durante toda la campaña electoral, nueve de las diez principales encuestas señalaban como ganadora de la elección a Hillary Clinton, ya que en promedio todas presentaron que la demócrata tenía una ventaja que

oscilaba en 3.2% por encima del republicano. No obstante, de esta sorpresa, Clinton aceptó su derrota durante la noche de la jornada electoral y felicitó a su contrincante. Los resultados de la elección causaron fuertes críticas entre medios de prensa dado que el Partido Demócrata ganó la mayoría del voto popular, por más de ochocientos mil votos, aunque perdió en el sistema de distritos electorales.

A pesar de haber manejado una estrategia provocadora y de confrontación durante toda su campaña, en su discurso de triunfo, Trump mantuvo una actitud conciliadora hacía el electorado y los demócratas. Sin embargo, las dudas en torno a la legitimidad de su victoria, dado los efectos polarizadores de los eventos suscitados en la campaña, y la supuesta interferencia de Rusia para apoyarlo, dejaron una fuerte aura de desconfianza en torno a la autenticidad del resultado de la elección. Esto con relación a que eventos como la interferencia de una ciberoperación rusa, ya sea en el hackeo de las cuentas informáticas de la Convención Nacional Demócrata, la filtración de los correos de Clinton y Podesta, o en la ciber explotación de los sistemas electorales estatales, representaban una violación a la soberanía de los Estados Unidos y la imposición de un candidato afín a los intereses de una nación extranjera, por encima del pueblo estadounidense.

En este contexto el 9 de diciembre, la CIA y otras 16 agencias de inteligencia compartieron a puerta cerrada con el Senado de los Estados Unidos un reporte en que concluían que Rusia había intervenido en las elecciones presidenciales en favor de Trump, dónde expresaban que se había identificado a los individuos que entregaron los correos hackeados del Comité Nacional Demócrata, quienes tenían lazos directos con el gobierno de dicho país. Asimismo, la institución concluyó que el objetivo de Rusia era favorecer a un candidato sobre otro. Respecto al hackeo, Trump mencionó que no creía que la nación hubiera intervenido (Entous y Nakashima, 2016).

Para el 10 diciembre, la Oficina del DNI (2016b) publicó el documento *Intelligence community statement on review of foreign influence on U.S. Elections*, en que él presidente Barack Obama ordenó una investigación en torno a los ciberataques de los que se responsabilizaba a Rusia, ocurridos durante la elección presidencial. Del mismo modo, expresó que el informe estaría listo antes de que Obama dejará el cargo de presidente. En este periodo, se empezó a tejer una mala relación de Trump con las principales agencias de

seguridad del Gobierno de los Estados Unidos (Greenberg, 2016). Posteriormente, el 14 de diciembre el DNI (2016c) entregó información clasificada y desclasificada a miembros del Capitolio en relación a las elecciones. En este contexto, el presidente Obama solicitó hacer una revisión de la comprobación de posibles esfuerzos extranjeros de influenciar las elecciones. Dos días después, el DNI (2016d) recibió múltiples peticiones de miembros del Congreso y del Colegio Electoral para recibir información adicional respecto a la interferencia rusa en la elección. La cual fue entregada inmediatamente.

Por último, el 29 de diciembre el DNI (2016e), en conjunto con el Departamento de Seguridad Interna de Estados Unidos (*Departmen of Homeland Ssecurity*) y el FBI, presentan un reporte en conjunto donde se explican los detalles de las herramientas e infraestructura empleados por inteligencia rusa para comprometer y explotar la infraestructura asociada con las elecciones estadounidenses, en sectores de gobierno, político y privado. El documento indicaba que las actividades formaron parte de una campaña de operaciones cibernéticas llevada a cabo desde hace décadas en contra del gobierno y ciudadanos estadounidenses. Y que las ciber operaciones han incluido modalidades de *spear phishing* dirigido a organizaciones gubernamentales, infraestructuras críticas, *Think Tanks*, universidades, organizaciones políticas, u corporaciones.

De igual forma, se identificó que los servicios de inteligencia rusos han llevado a cabo ciber operaciones dañinas y disruptivas a infraestructuras críticas, en algunos casos haciéndose pasar por terceros para hacer que una persona errónea sea atribuida por los ataques. Con el documento, se indicaba que el gobierno de los Estados Unidos podía confirmar que el gobierno de Rusia, militares y civiles rusos habían realizado actividades maliciosas en diversas infraestructuras, con lo cual el *Russiangate* fue un hecho que afectó la legitimidad del triunfo de Trump.

4.1.1.2 Año 2017

El espectro del *Russiangate* acompañó a Trump hasta su toma de protesta como presidente de los Estados Unidos de América el 20 de enero de 2017, así como al resto de su mandato con la creación de la Fiscalía Especial para la *Investigación de la Interferencia Rusa en las Elecciones presidenciales de 2016.* Tan sólo dos meses después del inicio de su gobierno, el

20 de marzo del 2020 durante una comparecencia ante el Comité de Inteligencia de la Cámara de Representantes, James Comey, titular del FBI, indicó que la institución estaba investigando si miembros del equipo de campaña de Trump conspiraron con Rusia para influenciar las elecciones presidenciales de 2016. Esto resultó en un duro golpe a la administración Trump quien semanas antes había despedido al asesor de seguridad nacional Michael Flynn, porque éste no había informado adecuadamente al vicepresidente Mike Pence sobre sus conversaciones con el embajador de Rusia en Washington DC, durante el periodo de transición a la presidencia. Por otra parte, los supuestos vínculos con Rusia de igual forma afectaron al Fiscal General Jeff Sessions. Frente a estas polémicas declaraciones, Donald Trump anunció el despido de Comey, que la prensa indica fue una recomendación hecha por Sessions (BBC Mundo, 2017).

Por otra parte, el 6 de enero el *Intelligence Community Assessment* (ICA) publicó el documento *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. En dicho informe, se presentaba una evaluación de las actividades e intenciones de Rusia en las recientes elecciones estadounidenses. El documento incluía una evaluación analítica redactada y coordinada entre la CIA, el FBI, y la Agencia de Seguridad Nacional (*National Security Agency* o el acrónimo de NSA por sus siglas en inglés). El informe desclasificado a la opinión pública, no incluyó la información completa, así como las fuentes y métodos de inteligencia para su elaboración. Sin embargo, el documento dejó claro que por la naturaleza del ciberespacio era difícil detectar el total de operaciones cibernéticas orquestadas por Rusia durante la elección de 2016, más esto no es imposible de realizar y una fiscalía especial podía realizar dicha acción. Ya que el documento argumentaba que todo tipo de operación cibernética, malintencionada o no, deja un rastro (ICA, 2017).

Del mismo modo, el informe de ICA (2017) indica que los esfuerzos de Rusia para influir en las elecciones presidenciales estadounidenses representaban la expresión más reciente del antiguo deseo de Moscú de socavar el orden democrático liberal liderado por Estados Unidos. A la par de señalar al presidente ruso,Vladimir Putin, como el responsable y quien ordenó una campaña de influencia en 2016, dirigida a las elecciones presidenciales de Estados Unidos. En ese sentido, los objetivos de Rusia eran socavar la fe pública en el proceso

democrático de Estados Unidos, denigrar a la secretaria Clinton y dañar su elegibilidad y posible presidencia. A razón de que Putin y el gobierno ruso desarrollaron una clara preferencia por el presidente electo Trump.

De esta forma, el enfoque de Moscú evolucionó a lo largo de la campaña basándose en la comprensión de Rusia de las perspectivas electorales de los dos principales candidatos. E ICA (2017) indicó que cuándo le pareció a Moscú que, cuándo Clinton se perfilaba como la probable ganadora de las elecciones, la campaña de influencia rusa comenzó a centrarse más en socavar su figura pública. Para esto, la inteligencia militar rusa (Estado Mayor Principal de Inteligencia Ruso o GRU en siglas) utilizó *Guccifer 2.0* y *DCLeaks* para divulgar datos que afectaran su imagen pública y campaña electoral. En este punto, es importante mencionar que la Oficina del Director Nacional de Inteligencia, indicó que derivado de su análisis, encontró que los tipos de sistemas con que los actores rusos atacaron o comprometieron la elección, no estaban involucrados en el sistema de recuento de votos. O dicho del mismo modo, no tenían evidencia para confirmar esta hipótesis.

La información del reporte de ICA (2017) causó eco en la opinión pública internacional, y varias cadenas de medios de noticias sacaron en la prensa nacional viejos materiales videográficos en los que se mostraba al presidente Vladimir Putin hablar públicamente de su preferencia por el presidente electo, durante el 2015, dada su posición respecto a los temas de Siria y Ucrania, en contraste con la "*retórica agresiva*" de la secretaria Clinton. Para este punto, ya existía sospechas de una estrategia rusa para beneficiar a Trump, la cual combinó operaciones de inteligencia encubiertas, actividades cibernéticas, esfuerzos abiertos de agencias del gobierno ruso, medios de comunicación financiados por el Estado, así como intermediarios externos y usuarios de redes sociales pagados, conocidos como *trolls*.

Esta trama permeó y alcanzó un alto margen de convocatoria, a razón de acusaciones de otras naciones hacía Rusia por utilizar estrategias semejantes. Por ejemplo, durante la crisis de Ucrania en 2014, Rusia desplegó con sus Fuerzas Armadas sensores en el este de Ucrania para controlar los portales de noticias, generar desinformación y dañar la imagen del gobierno ucraniano. En ese punto, la nación eslava utilizó una campaña de influencia multifacéticos que mezcló a agentes de influencia local y nacional, organizaciones de fachada y operaciones

encubiertas. Con lo cual se pensaba que Rusia si tenía el potencial de influir en las elecciones presidenciales de EE. UU. con un esquema más sofisticado, pero parecido a este.

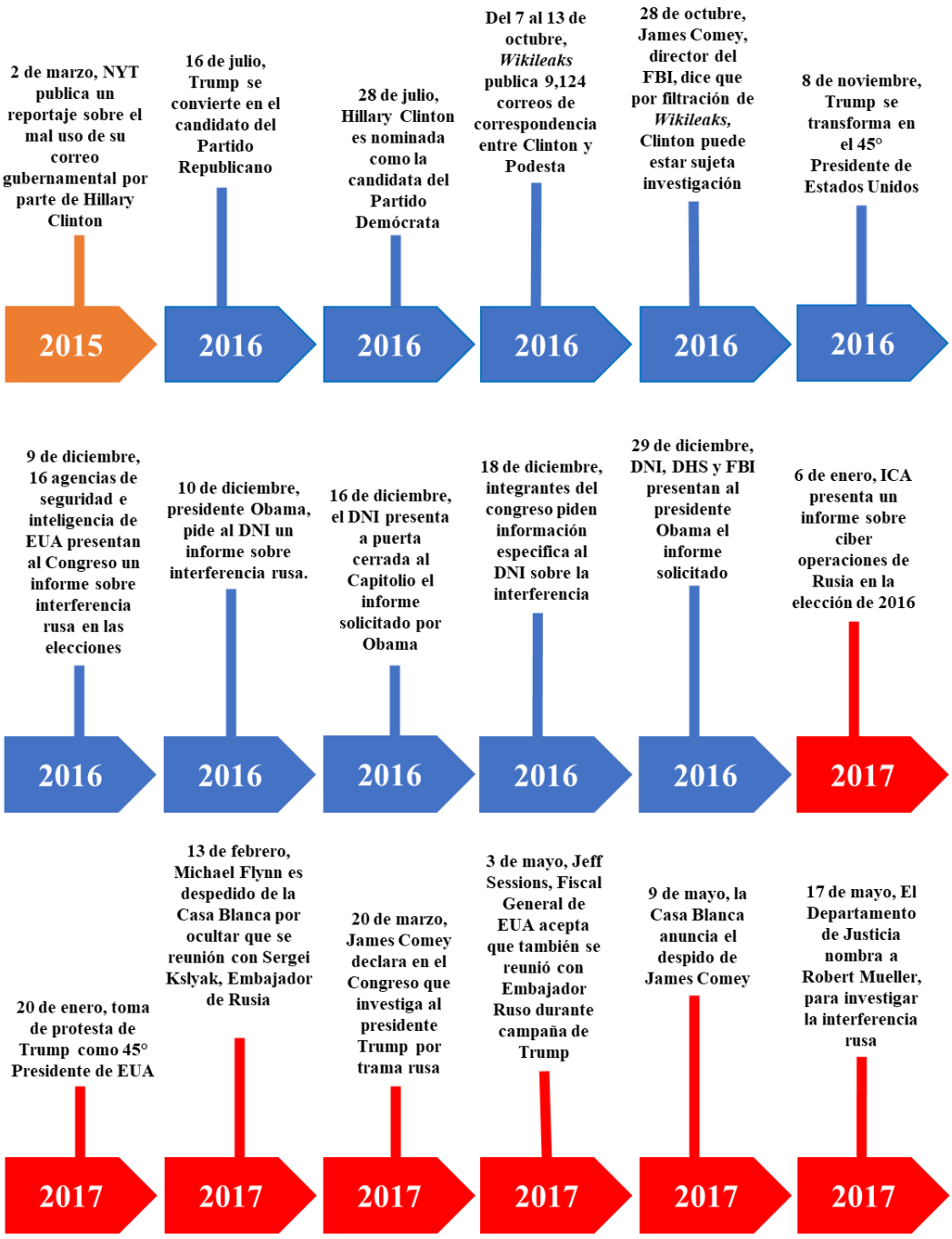
Con lo anterior, uno de los actores principalmente afectados fue la cadena televisiva del gobierno ruso de nombre Russia Today (RT). Ya que, en el contexto de la creciente sospecha sobre el Russiangate, el Congreso de los Estados Unidos, fomentado por un sector importante del Partido Demócrata, exigió al Departamento de Justicia que se realizará una solicitud a RT de registrarse como "*agente extranjero*", junto a medios de comunicación como el periódico *China Daily* o la cadena japonesa NHK (Mars, 2017). En ese sentido, el Departamento de Justicia extendió esta obligación a RT hasta noviembre, de 2017, a razón de que se consideraba que la cadena buscaba influir en la vida política interna de los Estados Unidos y alimentar el descontento en EE. UU. Del mismo modo, la cobertura mediática que dio el canal al proceso electoral estadounidense, al que definió como antidemocrático promovieron que los contenidos del país fueran vetados para finales de dicho año.

La tensión en torno a la trama del Russiangate llego a su máximo punto a inicios de mayo de 2017, cuándo Jeff Sessions, Fiscal General de los Estados Unidos y responsable del Departamento de Justicia, y quién apoyó y formó parte del equipo de campaña de Trump, en 2016, declaró que se reunió con el Embajador de Rusia, en Estados Unidos, Sergéi Kislyak, durante la campaña (Preda, 2017). Con lo cual promovió que el 17 de mayo de 2017, la Fiscalía General, a través del fiscal general Adjunto Rod Rosenstein, nombrará a Robert Mueller, quien fuera el sexto director del Buro Federal de Investigaciones (FBI) de 2001 a 2013, como asesor especial del Departamento de Justicia de los Estados Unidos (Borger, 2017). Con la designación de Mueller, Trump se transformó en el principal sujeto bajo investigación a causa de la injerencia rusa durante las elecciones del 2016. Por su parte, la designación de Mueller, según una declaración del Departamento de Justicia, correspondía a "*…garantizar una investigación completa y exhaustiva de los esfuerzos del gobierno ruso para interferir en las elecciones presidenciales de 2016."* (McCarthy, Swaine y Jacobs 2017).

Frente a esto, Trump no hizo esperar su reacción, externando que ni las campañas de Obama o Clinton habían tenido una cacería de brujas de esa magnitud. Por otra parte, es importante destacar que, tanto republicanos como demócratas estuvieron conformes con la designación de Mueller, a razón de que se le consideraba un sujeto con credibilidad y buena reputación,

por lo que los miembros del congreso estadounidense aceptaron la designación. A continuación, en la figura 46 se presenta una línea del tiempo con los principales eventos asociados a esta trama.

Figura 46. Línea del tiempo de la cronología de la trama *Russiangate.*



Fuente: Elaboración propia.

4.1.2 Trama Investigación del Fiscal Especial e *Impeachmen*t de Trump.

En la presente sección se presenta un análisis de los eventos en los años y meses que se realizó la *Investigación de la Fiscalía Especial para Investigación de la interferencia rusa en la elección presidencial de 2016,* a cargo del Fiscal Especial Robert Mueller. La cual culminó con la publicación y presentación del *Reporte de la Investigación de la interferencia rusa en la elección presidencial de 2016*, conocido por el nombre de *Reporte Mueller*. Un primer aspecto por destacar sobre el periodo que abarca esta trama se vincula a que la decisión de la creación de la Fiscalía Especial, por parte del Departamento de Justicia de los Estados Unidos de América, debe ser entendida desde distintas ópticas.

En primera instancia, y desde una comprensión de política interna, la creación de la fiscalía corresponde a una reacción del sistema político de los Estados Unidos de América para controlar el ambiente de polarización social y el actuar de Donald Trump, en su cargo de presidente. Quien desde su arribo intentó ejercer un liderazgo excesivo, que sobrepasaba los límites de sus funciones y autoridad de otras instancias (como lo eran el poder legislativo y judicial).

En ese sentido, es importante mencionar que, al momento de la creación de la fiscalía, el 17 de mayo de 2017, Trump estaba por cumplir cinco meses como presidente en los que se distinguió por un estilo de gobierno impredecible, caótico y visceral. Su exceso de aplicación de los decretos presidenciales en sus primeros meses de gobierno mostró sus intenciones de ejercer un liderazgo cercano al hiperpresidencialismo, en que la autoridad del poder ejecutivo termina por afectar el equilibrio de poderes en las democracias representativas.

Estas pretensiones de Trump por posicionarse como un líder político capaz de ejercer el control total del gobierno por sí mismo, libre de las presiones o control de la Cámara de Representantes, el Senado o la Suprema Corte de Justicia, son cercanas a los fenómenos de líderes populistas en una vasta serie de democracias representativas de la actualidad. En ese sentido, desde una óptica interna y cercana a la Ciencia Política, la creación de la Fiscalía Especial para investigar el *Russiagate* puede entenderse como un mecanismo de la maquinaria del gobierno de Estados Unidos para acatar el poder de un presidente desmesurado. De hecho, el reporte final de la investigación de Robert Mueller no encontró elementos para comprobar la intromisión del gobierno ruso en las elecciones de 2017, pero

si presentó diez episodios de obstrucción de justicia por parte del presidente Trump que enmarcan un abuso de autoridad desde su posicióno, que se presentan en la segunda sección de este capítulo.

Por otra parte, una segunda óptica desde la que puede abordarse la creación de la Fiscalía Especial corresponde a un análisis de dimensión internacional, en el que podemos partir de la hipótesis de veracidad de la consumación de la intromisión de una ciber operación rusa, que impactó y definió el triunfo de electoral de Trump, en las elecciones presidenciales de 2016. Lo anterior, implica que eventos como el hackeó a la Convención Nacional Demócrata y la filtración de la correspondencia de Clinton y Podesta, sí afectó e impactó en la desempeñó del proceso electoral, a tal grado que influyó en la opinión y voto de los ciudadanos estadounidenses.

Asimismo, se resalta el hecho de que un hackeo al sistema electoral, para afectar los logaritmos vinculados al conteo de votos, y definir el triunfo de un candidato a fin a los intereses de una potencia extranjera –en este caso Rusia- es una severa afectación a la soberanía nacional de los Estados Unidos. En ese sentido, destaca el hecho de que el sistema electoral de una democracia debe formar parte de su infraestructura nacional crítica, dado que está encargada de resguardar uno los elementos más emblemáticos de una democracia representativa: los procesos electorales. Con lo cual, una afectación, ya sea por la manipulación del electorado, vía la opinión pública o la desinformación, o la intromisión de un código malicioso, que afecte el resultado electoral, en efecto representaría una violación y daño severo a la soberanía, seguridad nacional y política exterior de un Estado-Nación. En ese sentido, a continuación, presentamos el análisis de los hechos de la Trama Investigación del Fiscal Especial e *Impeachment* de Trump.

4.1.2.1 Año 2017

Antes de cumplir cuatro meses en la Presidencia de los Estados Unidos, Donald Trump se enfrentó a la creación de la *Fiscalía Especial para Investigación de la interferencia rusa en la elección presidencial de 2016*, el 17 de mayo de 2017, las investigaciones sobre el Russiangate empezó a desarrollarse bajo la supervisión del Fiscal Especial Robert Mueller, antiguo director del FBI, como responsable de la misma. La creación de la fiscalía corrió a cargo de Rod Rosenstein, asistente del Fiscal General de los Estados Unidos, y a quien se

designó como encargado de entregar su cargo a Mueller (Preda, 2017). Ante el nombramiento, Trump se declaró "*…víctima de la mayor caza de brujas a un político en la historia de América*". También indicó que: "*…con todos los actos ilegales que tuvieron lugar en la campaña de Clinton y la Administración Obama, jamás se nombró un fiscal especial"*, a través de su cuenta de Twitter (Ahrens, 2017).

En ese sentido, el primer paso que dio la pesquisa se centró en las destituciones de personalidades al frente de instituciones clave en el aparato de inteligencia y sistema de procuración de justicia por parte del presidente Trump, en los primeros días de su gobierno. Frente a esto, los medios de comunicación indicaron que la investigación comenzaría a través de acciones del presidente que podían ser catalogados como episodio de obstrucción de la justicia. El primero de estos, se asoció al despido de James Comey, séptimo director del FBI, el 9 de mayo de 2017.

El despido de Comey causó revuelo en la opinión pública a razón de que había liderado una de varias investigaciones sobre Rusia en el marco de la elección presidencial de 2016. A la par de que testificó ante el Congreso de los Estados Unidos sobre este tema, la semana anterior, que Trump lo presionó para que abandonara una investigación que el FBI realizaba al ex asesor de seguridad nacional del Trump: Michael Flynn (BBC,2017).

Sobre esto, en su declaración, Comey expresó que el presidente Trump le pidió a través de un memorándum proveniente de la Casa Blanca, que cerrara la investigación federal sobre Flynn, en una reunión en la Oficina Oval en febrero. Con lo cual la documentación de la solicitud del presidente Trump era la evidencia más clara de que el presidente había tratado de influir directamente en el Departamento de Justicia y el FBI, en una investigación sobre los vínculos entre los socios de Trump y Rusia (Schmidth, 2017).

Como primer paso, durante la segunda semana del mes de junio de 2017, el Senado de los Estados Unidos citó a comparecer a Daniel Coats, entonces Director de Inteligencia Nacional, Mike Rogers, Jefe de la Agencia de Seguridad Nacional, y Richard Ledgett, en ese momento Director Adjunto de Rogers, con la finalidad, de si había existido alguna presión de Trump para terminar o interferir en las investigaciones vinculadas a Rusia con las que estaban relacionados.

En un panel organizado en el Senado, los tres personajes indicaron que nunca se habían sentido presionados para interferir en las mismas, o en el trabajo de Comey. A la par de externar que ninguno de ellos había participado en la campaña de Trump. Descartada la presión de Trump en alguno de estos personajes o instituciones, Mueller externó a los medios de comunicación que él continuaría con la investigación que Comey dejó inconclusa. Para esto, fueron clave las declaraciones del ex director del FBI en el Congreso, una semana antes de su despido, dónde declaró al Congreso que fue presionado por el líder del ejecutivo para concluir cualquier investigación a los asociados de su campaña y Rusia.

En este punto, el Departamento de Justicia de Estados Unidos dotó de facultades de abogado especial, con capacidad de iniciar investigaciones, citar registros y presentar cargos penales, al Fiscal Mueller. Las facultades del fiscal alcanzaron tal grado de independencia, que se declaró que estaba en su autonomía decidir si informaba al Departamento de Justicia de sus actividades durante el tiempo de la pesquisa (Preda, 2017). Sin embargo, antes de tomar acciones "*significativas"*, el abogado especial debía notificar al fiscal general. Y cuándo se cerrará la investigación, Mueller debía entregar un informe confidencial que explique la decisión de presentar cargos o retirar el asunto, con base a los resultados de esta (Hunt, 2017).

Una vez adjudicada esta autoridad, la opinión pública nacional empezó a destacar el despido de Comey como injustificado por parte de Trump. Ya que, dentro del aparato institucional y jerárquico del gobierno de los Estados Unidos, el presidente no tenía la autoridad para proceder en ese sentido. A razón de que el mandato de diez años de Comey expiraba hasta 2023. Y el protocolo para poder despedir al director del FBI estaba a cargo de Rod Rosenstein o Rachel Brand, ambos Fiscales Generales Adjuntos de los Estados Unidos, con lo cual se había procedido en un acto que podía ser catalogado como ilegal (Gambino, 2017).

Para este punto, integrante del Partido Republicano en el Senado comenzaron a señalar a la investigación de Mueller como un esfuerzo intencional de investigadores sesgados para socavar la presidencia de Trump. E indicaron que, de continuar este proceso, las críticas podrían crear una crisis política nacional. Sobre los integrantes del equipo de Mueller, los senadores republicanos los catalogaron como un "*equipo de ensueño*" para los demócratas y comentaristas liberales que esperan que eventualmente aplique un proceso de destitución (o *impeachment* en inglés) de la presidencia de Trump (Zurcher, 2017).

Descartada la presión de Trump para interferir en personajes o instituciones del sistema de inteligencia o de procuración de justicia de los Estados Unidos, el Fiscal Especial se centró para el mes de septiembre de 2017, en los ingresos y la fiscalización de los gastos de campaña de Trump. Para esto Mueller externo a la prensa su intención de recurrir a instancias del Servicio de Impuestos Internos de los Estados Unidos (*Internal Revenue Service* o IRS por sus siglas en inglés) para presionar a Donald Trump.

Está acción se justificaba, a razón de que, desde el inicio de su investigación, se tenían sospechas de vínculos entre los asesores de campaña y los movimientos financieros para poner en marcha la campaña del presidente Trump con actores rusos. Con lo cual, Mueller expresó que podría solicitar que los asesores de campaña del presidente fueran objeto de una investigación financiera. Todo con el fin descartar la hipótesis de vínculos entre estos con otros funcionarios del Gobierno Ruso o personas que operaron acciones para apoyar a Trump desde este país (Nitti, 2017).

En este contexto, personalidades de la Cámara de Representantes, del Partido Republicano, como Matt Gaetz, por el Estado de Florida, Andy Biggs, de Arizona, y Louis Gohmert, de Texas, acusaron a Mueller de tratar de crear un conflicto de intereses por un vínculo de carácter meramente comercial entre el equipo de campaña de Trump, con empresarios o personas de origen ruso, que no necesariamente justificaban la trama del *Russiangate*. Y para justificar este argumento, indicaron que el mismo Mueller, cuándo fue director del FBI durante la administración del expresidente Barack Obama, aprobó un acuerdo que permitía a una empresa rusa comprar una empresa canadiense, que poseía el 20 por ciento de Estados Unidos, adquirir suministros de uranio.

Lo cual no necesariamente implicaba un vínculo de carácter político, y de ser así, el mismo Mueller también debería ser investigado por tener ese tipo de relaciones (Reuters, 2017). Frente a estas declaraciones, integrantes del Partido Demócrata externaron que las actividades de los republicanos eran un esfuerzo partidista para distraer la atención de la investigación de Mueller y de los esfuerzos para garantizar que un gobierno extranjero, Moscú, no influya en las futuras elecciones estadounidenses.

A pesar de esta polémica, para el último trimestre del 2017, seis exasesores o asociados a la campaña de Trump fueron acusados en el marco de la investigación de la Fiscalía Especial,

por financiamiento fuera de la ley o de carácter ilícito. Sin embargo, hasta el fin de la pesquisa, ha ninguno de ellos se le logró acusar de conspirar con los autoridades o agentes rusos para interferir en la campaña de 2016. No obstante, cinco se declararon culpables de acciones fuera de ley durante la campaña, los cuales fueron: Richard Pinedo; George Papadopoulos, Michael Flynn; Rick Gates, Michael Cohen y Paul Manafort (Vitkovskaya *et al.*, 2017).

No obstante, descartada la variable de los nexos económicos con una autoridad o agente de Rusia, personajes del equipo de campaña como Paul Manafort, Richard Gates III y George Papadopoulos fueron investigados como operadores con nexos políticos o de espionaje para el gobierno ruso. Sobre Manafort, se indicó que existía evidencia de que el ex gerente de campaña de Trump había servido durante años como agente extranjero no registrado para un gobierno títere de Vladimir Putin en Europa del Este. En este contexto, Papadopoulos indicó que, durante su labor como asesor en política exterior de la campaña presidencial de Donald Trump, en 2016, entró en contacto con personas que sabía que estaban vinculadas al Gobierno Ruso. Lo anterior, con el fin de organizar una reunión entre el equipo de campaña y los funcionarios del gobierno ruso y tomar ventaja sobre Hillary Clinton a través de la divulgación de algunos correos electrónicos. Del mismo modo aceptó que mintió al FBI en esta declaración e informó al presidente Trump en dos ocasiones sobre esto (Hennessey y Wittes, 2017).

Los cargos contra Manafort, se intensificaron a razón de que estas declaraciones se vincularon a un documento en posesión del FBI titulado el *Dossier Steele*, de la autoría de un ex funcionario de inteligencia británico de nombre Christopher Steele, que había sido entregado a Comey y al FBI en 2016. Dicho documento, no verificado del todo, indicó que Trump ofreció un trató benéfico a Rusia durante su presidencia, si Wikileaks proporcionaba a su campaña cualquier información lasciva y dañina descubierta de los correos electrónicos pirateados de la campaña de Hillary Clinton. y el Comité Nacional Demócrata (Jacobus, 2017).

Dichas declaraciones impactaron en los medios de comunicación, a razón que dos de las personalidades más cercanas a la campaña de Trump indicaron que durante este periodo el presidente tuvo a personas de su equipo más cercano, que trabajaron activamente con un

gobierno extranjero antagónico a los Estados Unidos, con lo cual el despido de Comey del FBI podía considerarse un medio que buscaban obstruir la justicia estadounidense. En consecuencia, y derivado de las declaraciones de Papadopoulos, funcionarios de la Embajada de Australia en los Estados Unidos proporcionaron información al FBI y a la Fiscalía Especial de que el diplomático Alexander Downer, supuestamente había recibido de George Papadopoulos en un exclusivo bar de Londres, en mayo de 2016. Y que, en dicha reunión, el diplomático proporcionó un paquete de información, dentro de la que se encontraban miles de correos electrónicos que comprometían a la entonces candidata Hillary Clinton. Frente a esto, el FBI externo que mantuvo esta información de manera secreta para evitar que las elecciones fueran canceladas, por lo que durante ese periodo no emitió declaraciones, pero que esto era del conocimiento de Comey (Deutch Welle, 2017).

En este punto, los hallazgos crecientes de personajes del equipo de campaña de Trump alcanzaron a su familia. Para octubre, BBC Mundo (2017b) indicó que la Fiscalía Especial de Mueller ya investigaba Donald Trump Jr., sobre el cual se tenía conocimiento había mantenido una reunión con personajes del Gobierno Ruso. Frente a esta información, Trump declaró a la prensa nacional su intensión de desmantelar la Fiscalía Especial a razón de que estaban ya indagando a su familia. Sin embargo, el Senado estadounidense introdujo dos proyectos de ley bipartidistas diseñados para limitar la capacidad del gobierno de Trump para despedir a Mueller. Los cuales se aplicaron en medio de preocupaciones de que el presidente terminará de forma abrupta con la investigación.

Posteriormente, para el mes de noviembre, Mueller indicaría que también contaba con evidencia de una reunión entre Jared Kushner, yerno y asesor especial del presidente Trump, de haber participado en una reunión con el Embajador Ruso y el primer asesor de seguridad de la Casa Blanca durante su campaña. Por lo cual, Kushner fue convocado a un interrogatorio por el Departamento de Justica de los Estado Unidos. A pesar de las polémicas, Kushner asistió al interrogatorio y centró sus declaraciones en dos asuntos. El primero relacionado con la reunión que mantuvo en diciembre de 2016, entre las elecciones y la investidura presidencial, con el entonces embajador ruso en Washington, Sergey Kislyak. A la cual, también asistió Michael Flynn, ex asesor de Seguridad Nacional de la Casa Blanca.

En segunda instancia, habló del conocimiento que tenía de los contactos entre Flynn y el Gobierno Ruso. Frente a lo cual aceptó que Flynn se vio forzado a dimitir en febrero, cuando llevaba apenas 24 días en el puesto, tras revelarse que mintió al vicepresidente, Mike Pence, sobre sus conversaciones con Kislyak. Por último, Kushner negó que, en esa reunión, le ofreciera establecer un canal secreto y seguro de comunicación entre el equipo de Trump y el Gobierno de Putin (Faus, 2017). Con lo cual el año culminaría con cada vez mayores nexos entre Trump y las personalidades más cercanas su gobierno, con agentes o actores del Gobierno Ruso.

4.1.2.2 Año 2018

Los siguientes pasos estratégicos del Fiscal Mueller se dieron durante el mes de febrero de 2018. El día 16, de dicho mes, la oficina de la fiscalía especial presentó trece acusaciones formales contra ciudadanos y tres compañías de origen ruso frente al Departamento de Justicia de los Estados Unidos, a razón de su interferencia en las elecciones presidenciales de 2016. El mismo Mueller, indicó que se les acusa de "*violar las leyes criminales para interferir en los comicios de EE.UU. y los procesos políticos*" **(**BBC Mundo, 2018). Y que entre sus operaciones figuraban estrategias coordinadas y sistemáticas de comunicación, a través de medios digitales para promover información despectiva sobre Hillary Clinton, y denigrar a otros candidatos como Ted Cruz y Marco Rubio, así como apoyar al entonces candidato Donald Trump (Faus, 2018).

En sus declaraciones, Mueller empezó a indicar los patrones identificados de operación de dichos actores, sobre los que expresó se habían hecho pasar por estadounidenses y abrieron cuentas financieras en Estados Unidos para gastar miles de dólares al mes en publicidad política. Del mismo modo, indicó que compraron espacio en servidores de la unión americana con la intención de ocultar su procedencia. A la par de organizar y promover mítines políticos, a través la publicación de mensajes políticos en redes sociales haciéndose pasar por ciudadanos estadounidenses, en redes sociales como Facebook e Instagram. En este sentido se indicó que se estimaba había operado con un presupuesto mensual de hasta 1,25 millones de dólares. Un aspecto importante a mencionar es que el gobierno ruso, se pronunció respecto a estas acusaciones, a las que la portavoz del Ministerio de Asuntos Exteriores de Rusia, Maria Zakharova calificó de absurdas.

No obstante, de las negaciones del Kremlin, la investigación Mueller empezó a encaminar al *Russiangate* como una serie de estrategias coordinadas, con el fin de promover una "*guerra de información"* realizada entre múltiples actores rusos y el entonces equipo de campaña de Donald Trump (Mangan y Calia, 2018). En este punto, destaca que por primera vez se presentó a la organización rusa *Internet Research Agency* (IRA) como el actor central involucrado en esta estrategia de guerra de información. En ese sentido, el siguiente pasó de la investigación consistió en encontrar los últimos nexos entre los actores rusos y los implicados del equipo de campaña de Trump como Manafort, Papadoupolus, y Flyn.

Respecto Manafort, es importante decir que él se convirtió en el primer personaje del equipo de campaña en Trump enser sometido a un juicio en el marco de la investigación del fiscal especial Robert Mueller el 15 de julio de 2018, en Alexandria, Virginia (Pecorin, 2018). En este contexto, el periodista Andrew Kramer del New York Times, pronto destacó la presencia de Konstantin Kilimnik, un ex intérprete militar ruso, quien empezó a aparecer constantemente en las reuniones judiciales del fiscal especial.

A razón de que Kilimnik, había trabajado aproximadamente por diez años como gerente de oficina en Kiev para una consultoría política de Paul Manafort. Pronto, Kilimnik declaró que, en julio de 2016, mientras Manafort era presidente de la campaña de Trump, le envió un correo electrónico a él pidiéndole que ofreciera a Oleg Deripaska, presidente de la Compañía Unificada RUSAL, la empresa de aluminio más grande del mundo, sesiones informativas privadas sobre la campaña de Trump a cambio de resolver una disputa financiera multimillonaria relacionada con RUSAL en los Estados Unidos (Kramer, 2018).

Con esta acusación de Manafort, Mueller atrapó a uno de los principales asesores de la campaña de Trump y expuso una red de tratos comerciales supuestamente ilícitos entre el ex presidente de campaña y funcionarios ucranianos. La pena contra Manafort, culminó cuándo Rick Gates, uno de sus socios desde hace décadas, aceptó cooperar con Mueller testificó contra Manafort, dónde o acusó de tener un plan financiero para operar con empresarios rusos en caso de un triunfo de Trump (Polantz, 2018).

Posteriormente, el Fiscal Especial de Estados Unidos citó a Roger Stone, quien fungió como consultor político y cabildero, por sospechas la intromisión rusa en las elecciones. La señalización de Stone, derivó del interrogatorio realizado por la fiscalía especial a Jason Sullivan, un experto en redes sociales y Twitter, que trabajó con Stone durante la elección. En consecuencia, el equipo de Mueller indicó que existía evidencia de que Stone había fungido como intermediario entre WikiLeaks y el equipo de campaña de Trump, para la filtración de la correspondencia de la entonces candidata Hillary Clinton, su director de campaña John Podesta (Hosenball y Layne, 2018). Frente a esto, Stone aceptó haber mentido al Congreso a razón de que, si realizó esfuerzos por comunicarse con WikiLeaks, por lo cual fue arrestado por cargos presentados por Mueller. La nueva acusación formal contra Manafort y Gates incluyó 32 cargos de fraude fiscal y bancario.

Las declaraciones de Stone derivaron en nuevas declaraciones de personajes como Papadoupolus, quién admitió que discutió con sus contactos en Rusia durante la campaña, para promover una posible reunión entre el candidato Trump y el presidente ruso Vladimir Putin (Rodriguez y Jin, 2018). Derivado de esta declaración, Papadopoulos, quien fungió como ex asesor de política exterior de la campaña de Trump, fue condenado a catorce días de cárcel por mentir al FBI sobre la presunta injerencia rusa. Ante esto, el ex asesor de Trump alcanzó un acuerdo en el que se declaró culpable y aceptó cooperar con la fiscalía especial (France 24, 2018).

Consolidadas acusaciones contra Flyn, Papadopoulos y Manafort, Trump declaró el 27 de noviembre de 2018, en su cuenta de Twitter que "*Mueller es un conflictivo fiscal fuera de control*", y que "*la prensa fabricó un aura de santo en torno al fiscal independiente Robert Mueller*" (Forbes, 2018). Para el fin del 2018, 22 meses (o 674 días) habían transcurrido desde que Mueller asumió el cargo de la fiscalía especial. En total 34 personas y empresas habían sido acusados en la investigación de Mueller sobre la interferencia rusa en las elecciones estadounidenses de 2016 (Taylor y Morris, 2018). De las cuales, cinco vinculados al equipo de campaña de Trump, de los cuales cinco había condenados (Michael Cohen, George Papadopoulos, Alexander Van Der Zwaan, Richard Pinedo y Paul Manafort). Dos se

habían declarado culpables en la investigación (Michael Flynn y Rick Gates) y acordaron acuerdos de cooperación. Por último, se estimaba que, hasta ese momento, la pesquisa alcanzaba el costo de $ 25 millones de dólares (PBS, 2018).

En este punto, Helderman et al. (2018), periodistas del *Washington Post*, indicaron que la investigación de Mueller se había centrado en cuatro principales ejes:

1. *Vínculos financieros ilícitos:* relacionado con los tratos financieros de los integrantes del equipo de campaña del presidente Trump, como Manafort, Flyn y Gates, en aspectos como la consultoría política y vínculos con empresas de Ucrania.
2. *Interferencia rusa:* Con relación a los vínculos de los integrantes del equipo de campaña de Trump, con IRA, Wikileaks, así como las trece personas y tres compañías con origen en Rusia, que acusaban de intervenir en la campaña presidencial de 2016, mediante la circulación de noticias falsas, campañas de desprestigio y hackeo de correos electrónicos demócratas.
3. *Coordinación de equipo de campaña y agentes del gobierno Rusia:* con las declaraciones de Papadoupolus y Manafort, así como las sospechas de reunión de Trump Jr. Y Jared Kuschner. Mueller buscaba encontrar evidencia tangible de coordinación entre los asociados de Trump y el gobierno ruso, para determinar si hay evidencia de que la campaña de Trump conspiró con Rusia durante las elecciones de 2016.
4. *Obstrucción de la justicia:* La fiscalía se centran en las acciones de Trump y sus asociados, dado que el presidente utilizó su posición para minar múltiples intentos de investigación a los colaboradores de su campaña y su familia.

El año 2018 cerraría con Mueller como un fiscal especial, fuertemente empoderado, y cercando al presidente Trump. Del mismo modo, Mueller indicó que las principales labores de investigación ya se habían realizado y presentaría su informe al Departamento de Justicia en el primer trimestre del 2019.

4.1.2.2 Año 2019

El 23 marzo 2019, después de una investigación de 22 meses, cargos contra 37 acusados y siete declaraciones de culpabilidad y una condena en el juicio, el Departamento de Justicia anunció que la investigación del fiscal especial sobre la interferencia de Rusia en las elecciones, de Robert Mueller, había concluido. Para esto, y con base en lo acordado al momento de la creación de la fiscalía, Mueller presentó un informe confidencial al fiscal general William Barr en el que detalla las decisiones que tomó equipo en torno a la decisión para enjuiciar o no al presidente Trump (Herb y Jarret, 2019). El *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016* presentado constó de dos partes.

El primer volumen presentaba la evidencia identificada por parte de agentes del gobierno de Rusia para influir en las elecciones. Este apartado incluyó las acciones de los integrantes del equipo de campaña de Trump a esta actividad. Sin embargo, el documento concluyó que no existían pruebas suficientes para acusar al presidente y su equipo de campaña de una conspiración más amplia y coordinada con actores del gobierno extranjero. Por otra parte, el segundo volumen del informe presentaba los resultados y el análisis en torno a actos de obstrucción a la justicia que involucra al presidente Trump y personas cercanas a él (Kim, 2019).

A pesar de la gran expectativa, que había generado en opinión pública internacional la investigación de la Fiscalía Especial, el resumen del informe publicado por el Departamento de Justicia sobre la investigación del presidente de los Estados Unidos llegó a la conclusión de que no existía evidencia tangible de que alguna persona de la campaña de Trump o cualquier persona asociado a él, haya conspirado o coordinado acciones con Rusia con el fin de influir en los resultados de la elección (Le Monde Diplomatique, 2019). Para la opinión pública, los primeros elementos del informe Mueller representaron una derrota para el partido Demócrata y los medios de comunicación. También, la crítica arreció contra los costes del Russiangate, que para este punto se consideraba oscilaban en los 40 millones de dólares (Ferrero, 2019).

No obstante, de que no existía evidencia de conspiración entre personajes cercanos a la campaña de Trump y su familia, el equipo de 13 abogados y 40 agentes del FBI que lideró Muller, indicó que existía evidencia para acusar en al menos por diez actos al presidente por el delio de obstrucción de justicia. Del mismo modo, los integrantes del partido democráta defendieron la investigación, a razón de las 37 personas acusadas durante todo el proceso, entre las que se encontraban los asesores electorales como Roger Stone y Paul Manafort (Tamanes, 2019). No obstante, de esto, Trump respondió con satisfacción ante el resultado del informe Mueller, e incluso utilizó esto para reforzar su posición presidencial y referirse a la oposición como: "*unos desubicados que se obsesionaron con la trama rusa para quedar eximidos sobre sus propios errores."*

Frente a esto, la líder del Partido Demócrata en la Cámara de Representantes, Nancy Pelosi, anunció que promovería una audiencia para discutir la versión pública del Informe Mueller, en este recinto. Del mismo modo, la líder demócrata indicó que: "*el reporte tenía autoridad para que el Congreso contuviera la autoridad de un presidente corrupto, para proteger la integridad de la administración de la justicia, acorde al sistema constitucional de pesos y contrapesos y el principio de que ninguna persona está por encima de la ley en los Estados Unidos*" (Cillizza, 2029). Con lo cual, el 24 de abril, Pelosi promovió una conferencia de prensa en la que convocó a todos los representantes del Partido Demócrata una audiencia en el Congreso de los Estados Unidos, para que Mueller presentará los hallazgos de su informe. Frente a esto, el grupo más conservador y leal a Trump del Partido Republicano, indicó que los demócratas buscaban imponer una sanción de carácter político frente a Trump, después del fin de una investigación que había terminado y lo había exonerado.

No obstante, el 29 mayo de ese mismo año, el fiscal especial Robert Mueller presentó una conferencia de prensa en el Departamento de Justicia, con el fin de explicar las principales conclusiones de su investigación. En ella, Mueller declaró que, según las directrices del Departamento de Justicia, acusar al presidente Donald Trump de un crimen no era una opción a razón de que "[no se tenía] *certeza de que el presidente claramente cometió un crimen".* Sin embargo, indicó que su pesquisa concluía que Rusia interfirió en las elecciones de 2016 "*de forma sistemática y de gran alcance*" y destacó que se encontraron diez momentos en

que Trump pudo haber intentado detener la investigación y podrían ser catalogados como actos de obstrucción de justicia (BBC Mundo, 2019**)**. Sin embargo, a pesar de este evento, los demócratas lucharon porque Mueller se presentará en la Cámara de Representantes, audiencia que se programó para realizarse en Capitol Hill, para el día 24 de julio.

En la Cámara de Representantes Mueller declaró que su investigación nunca declaró a Trump como "*exonerado*" de una posible obstrucción a la justicia. A la par de refrendar que Rusia trabajó para interferir el resultado de las elecciones de 2016 en nombre de Trump, pero no pudo identificar evidencia concreta de colusión criminal. Al ser cuestionado por los congresistas, Mueller se negó repetidamente a añadir algo más que lo que dice su informe de 448 páginas. Por su parte, el periodista de CCN, Chris Cillizza (2019) indicó como ambos bandos de cada partido politizaron fuertemente la audiencia, que en múltiples ocasiones evitó que el Fiscal Especial pudiera declarar sin tensiones sus respuestas. A pesar de este contexto adverso, Mueller bajo juramento, aseguró que su reporte daba evidencia concreta de las siguientes acciones por parte del equipo de campaña de Trump (Siddiqui, 2019):

- Los rusos habían liderado una campaña para inclinar las elecciones de 2016 a favor de Trump y cometieron crímenes para lograr ese objetivo.
- La campaña de Trump fue receptiva a la ayuda de los rusos.
- Donald Trump Jr. dijo que le "encantaría" recibir información sobre Hillary Clinton del gobierno ruso.
- Como candidato, Trump instó públicamente a los rusos a piratear los correos electrónicos de Clinton.
- Trump persiguió un lucrativo proyecto de la Torre Trump en Moscú durante la campaña.
- Varios altos funcionarios de la administración y la campaña de Trump fueron condenados por mentir a los investigadores sobre sus contactos con los rusos.

Dichas declaraciones, así como las cercanías de personajes del equipo de campaña de Trump con el gobierno de Ucrania, serían utilizados como un argumentó por parte de los demócratas para retomar una acusación por retener $400 millones en ayuda militar aprobada por el

Congreso para presionar al nuevo presidente de Ucrania, Volodímir Zelenski, con el fin de que iniciará una investigación en torno al y el hijo del líder demócrata Joe Biden, ex presidente de los Estado Unidos, y quien se perfilaba como su oponente para las elecciones de 2020 (BBC, 2019b).

La petición de Trump arreció en los medios, a razón de que el presidente deseaba usar el hecho de que Hunter Biden era miembro de la junta de una compañía de gas ucraniana, y Trump deseaba politizar este asunto, a su favor en el marco de la carrera presidencial para 2020. Frente a este acto, el 4 de septiembre, la presidenta de la Cámara de Representantes, Nancy Pelosi, promovió una investigación de juicio político contra Trump por la vinculación de su campaña con Rusia. Frente a lo cual la Casa Blanca se ve en la necesidad de publicar una transcripción de la llamada telefónica de julio al día siguiente. No obstante, el 26 de septiembre, Pelosi publica la denuncia en la Cámara de Representantes y alega que Trump usó "*el poder de su oficina para solicitar la interferencia de un país extranjero"* en las elecciones presidenciales de 2020. Con lo cual se le adjudicaban actos de obstrucción de justicia y vínculos con agentes extranjeros, del mismo modo que presentó el informe Mueller. Frente esta acusación, la prensa contraria al presidente Trump dio fuerte difusión al tema, a tal grado que el 17 de octubre, el jefe de gabinete de la Casa Blanca, Mick Mulvaney, tuvo que salir a dar una declaración pública, en la que admitió que se retuvo la ayuda militar a Ucrania en parte para presionar a Kiev para que investigara las acusaciones que involucraban a los demócratas y las elecciones de 2016. Evento que utilizaría el Partido Demócrata para promover la amenaza de un proceso de *impeachment* en contra de Donald Trump (SudOuest, 2019).

En este contexto, el 9 de diciembre los demócratas de la Cámara de Representantes anunciaron dos artículos de acusación contra el presidente Donald Trump, declarando que "*traicionó a la nación*" con sus acciones hacia Ucrania mientras avanzaban hacia procedimientos. Los cargos específicos dirigidos a destituir al 45º presidente de Estados Unidos: abuso de poder y obstrucción al Congreso (Mascaro y Jalonick, 2019a).Diez días después, Donald Trump fue acusado por la Cámara de Representantes de Estados Unidos por juicio político, con el fin de iniciar un proceso de destitución, convirtiéndose en el tercer

presidente ejecutivo estadounidense en ser acusado formalmente en virtud del último recurso de la Constitución para delitos graves y faltas (Mascaro y Jalonick, 2019b).

La histórica votación se dividió a lo largo de las líneas partidistas de los demócratas y republicanos, a la par que polarizó a la nación. Los cargos imputados al 45 ° presidente de los Estados Unidos expresaban que él había abusado del poder del ejecutivo para reclutar a un gobierno extranjero para investigar a un rival político antes de las elecciones de 2020. Posteriormente, la Cámara de Representantes aprobó un segundo cargo, que obstruyó al Congreso poder iniciar una investigación. A pesar de que los demócratas ganaron la votación para iniciar una investigación contra Trump en la Cámara de Representantes. Los Republicanos no permitirían que el *impeachment* prosperará en el Senado (Wolfe, 2019). No obstante, los tiempos políticos del cierre de año impidieron que el *impeachment* prosperará.

4.1.2.3 Años 2020 y 2021

El *impeachment* de Trump tuvo que esperar para ser atendido en el Senado hasta el 5 de febrero de 2020. No obstante, a pesar de los esfuerzos y acusaciones por la Cámara de Representantes, el Senado liderado por los republicanos absolvió de juicio a Trump. Con este acto los senadores declararon a Trump no culpable del primer artículo de juicio político, abuso de poder, por un recuento de 52-48 legisladores. Así como de no culpable del segundo artículo de juicio político, obstrucción del Congreso, por un recuento de 53-47 en la votación (The Guardian, 2020).

En este contexto, el Departamento de Justicia sorprendió por ampliar acusaciones en contra integrantes del equipo de Trump, como Flyn y Stone, y personalidades que no se encontraban dentro de los 37 acusados, entre estas destacan los siguientes eventos:

- El 10 de febrero, el Departamento de Justicia cesó a un juez que sentenció a Roger J. Stone Jr., hasta 40 de prisión por mentirle al Congreso y manipular a un testigo para evitar que los investigadores descubran cómo Trump en la campaña del 2016 intentó beneficiarse de los documentos demócratas robados (The New York Times, 2020).

- El 30 de abril de 2020, se decidió adjudicar un nuevo cargo a Flynn, por hacer declaraciones al agente del FBI Edward William Priestap, con los cargos de supresión de evidencia y sesgo de información (New York Post, 2020).
- En septiembre de 2020, el Departamento de Justicia acusó a Brian Murphy, un alto funcionario en la oficina de Inteligencia y Análisis del Departamento de Seguridad Interior, por obedecer al jefe interino de dicha institución Chad Wolf, para dejar de proveer análisis de inteligencia sobre la amenaza de interferencia rusa en Estados Unidos. También, Murphy acepto haber modificar un documento oficial de la inteligencia estadounidense sobre los grupos de supremacía blanca "*para atenuar la peligrosidad de esta amenaza e incluir información sobre la importancia de los grupos violentos de izquierda*" en el contexto de la elección presidencial de 2020 (El Universal, 2020a).

Estos episodios empezaron a ser señalados por parte de integrantes del Partido Demócrata, como eventos que causaban una profunda preocupación, a razón de que temían que los cargos criminales o los informes públicos emitidos tan cerca de las elecciones de 2020 pudieran afectar el voto de la elección del 3 noviembre. En la que Joe Biden se perfilaba como claro ganador. Sin embargo, ninguno de estos eventos evitó que como resultado de las elecciones Biden alcanzará 306 votos electorales frente a los 232 de Trump obtenidos por Trump. Con lo cual se convirtió en el 46.º presidente de los Estados Unidos el 4 de noviembre de 2020.

No obstante, del resultado, Trump estaba lejos de quedarse cruzado de brazos frente al resultado, con lo que empezó una serie de actos erráticos hasta el día de la sucesión presidencial el 20 de enero. Con lo cual, el presidente aún en funciones utilizó el resto del año para difundir desinformación sobre los resultados, sosteniendo falsamente que ganó la elección y que esta "*la elección estaba siendo robada*".

Del mismo modo, expresó iniciar emprender acciones penales a funcionarios del Gobierno para que encuentren "*votos perdidos*", lo que representaba una amenaza del presidente a funcionarios de menor jerarquía. Dichas declaraciones, hicieron crecer un ánimo de apoyo a favor de Trump, que explotó el 6 de enero, después de un discurso en el que incitó a sus

seguidores a tomar el Capitolio. El cual desencadenó, una insurrección instigada por el mismo presidente, en la que sus seguidores asaltaron el Congreso de Estados, con lo cual pusieron en peligro la seguridad de los legisladores y otras autoridades, que culminó con el resultado de cinco muertes.

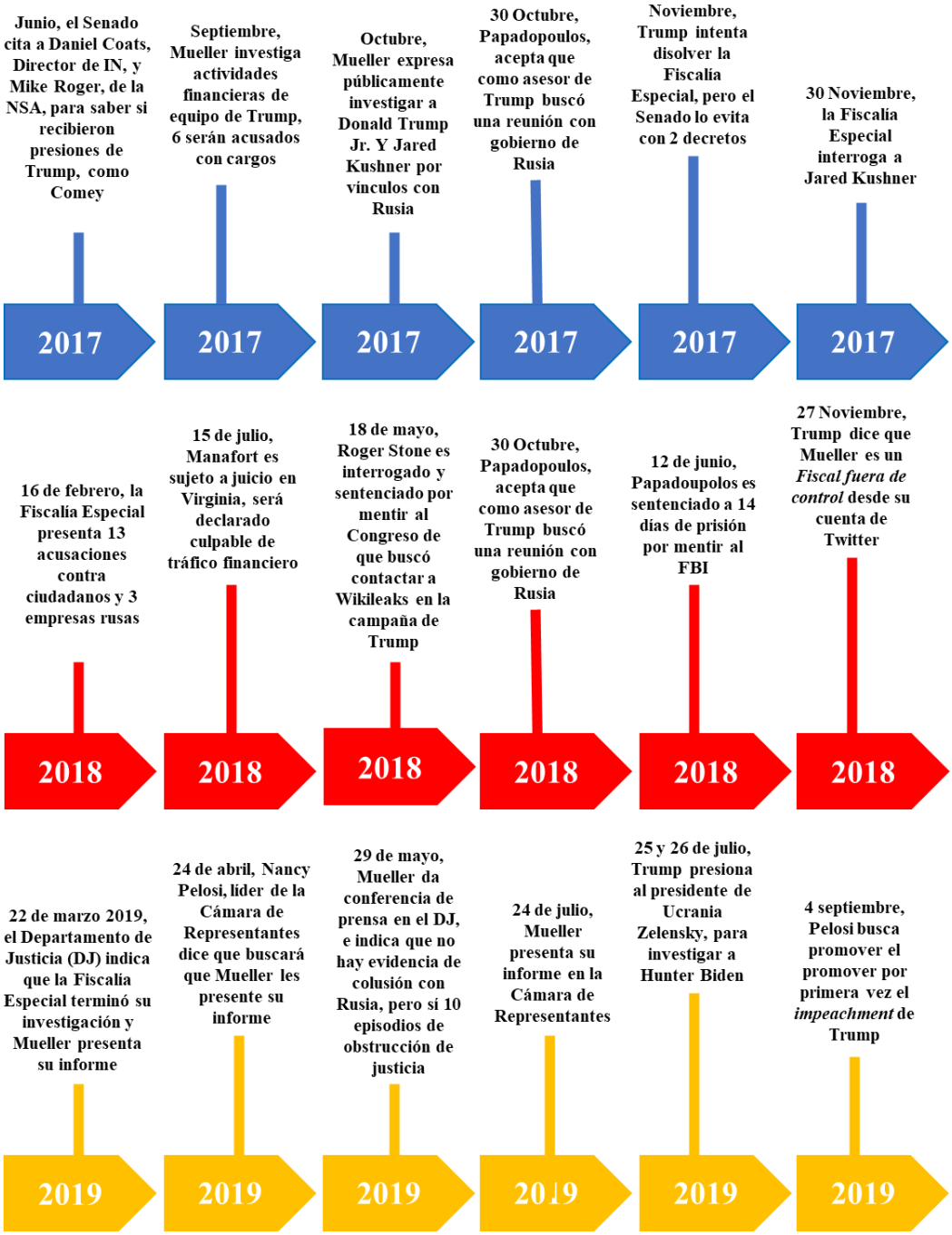
Días posteriores al asalto del Capitolio, la líder demócrata, instó a la Cámara de Representantes y al Comité Judicial de la misma, a elaborar un informe sobre el comportamiento del presidente. Del mismo modo lo acusó de "*no actuar para detener la insurrección*". Del mismo modo que "*ignoró y rechazó repetidamente sus súplicas y las de Chuck Schumer de dirigirse a sus seguidores para que abandonaran el Capitolio*" y siguió animando a sus seguidores. A la par, que horas después de que empezara la sublevación, emitió un mensaje en vídeo, en el que insistió en la falsedad de que la elección les había sido robada, y dijo a sus seguidores que asaltaron el capítulo que agradecía sus actos y apoyo. palabras eran "totalmente apropiadas".

Frente a esto, Pelosi evocó la base jurídica de la 14° enmienda de la Constitución, que prohíbe a cualquier "*funcionario de Estados Unidos que ha tomado parte en una insurrección o rebelión*" ocupar cargo público alguno. Con lo cual, se inició un segundo proceso de *impeachment* en los últimos días del gobierno de Trump, cuyo fin indicaban los demócratas no era evitar "*daños pasados, sino una protección contra males futuros*". A razón de que "*un presidente capaz de fomentar una insurrección es capaz de mayores males*". En ese sentido, Pelosi y el ala de los demócratas, promovieron hasta el último día del gobierno de Trump el segundo *impeachment*, en esta ocasión, por el delito de "*incitación a la insurrección*" por el asalto al Capitolio (Guimón, 2021).

El cuál se votó el 14 de enero en la Cámara de Representantes, y triunfó con un total de 232 votos a favor, sobre 197 en contra. Sin embargo, la sucesión presidencial evitó que el proceso fuera votado en el Senado, y finalmente, el 20 de enero de 2021 Biden, tomó posesión como el 46° presidente de los Estados Unidos (Pardo, 2021). Por último, el Senado anularía el proceso de *impeachment* el 13 de febrero con un total de con un total 57 votos, a favor de la condena, y 43 en contra, que no alcanzaron mayoría de dos tercios de los legisladores para

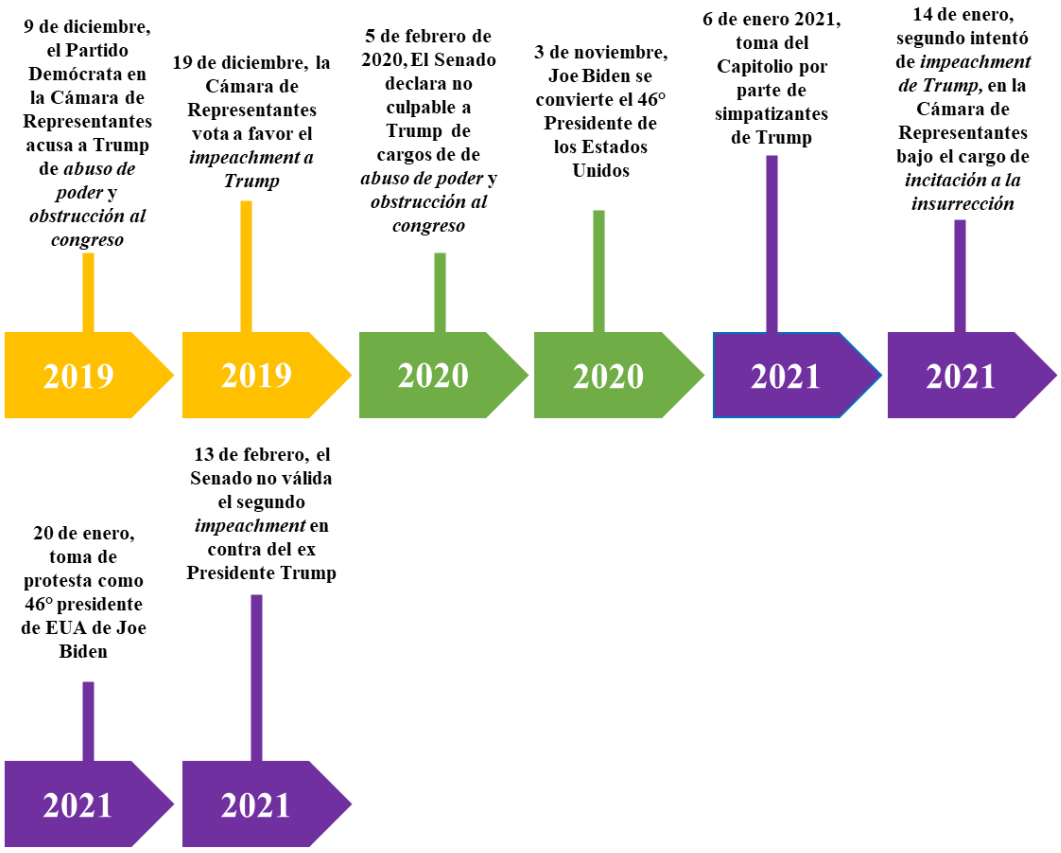
validar este proceso (Mars, 2021). A continuación, en la figura 47 se presenta una línea del tiempo con los principales eventos asociados a esta trama.

Figura 47. Línea del tiempo de la cronología de la trama *Investigación del Fiscal Especial* e *Impeachment de Trump*. (Parte 1).



Fuente: Elaboración propia.

Figura 47. Línea del tiempo de la cronología de la trama *Investigación del Fiscal Especial* e *Impeachment de Trump*. (Parte 2).



Fuente: Elaboración propia.

4.1.3 Trama SolarWinds

La trama SolarWinds es trascendental en la comprensión de la evidencia final del *Informe Mueller*, a razón de que este documento expresó que no encontró evidencia concreta para probar la colaboración y colusión entre el equipo de campaña de Donald Trump y agentes del Gobierno Ruso, durante las elecciones de 2016. Sin embargo, un hecho del que siempre se tuvo certeza, por parte de la Fiscalía Especial, es que agentes de origen ruso o cercanos a este país habían intervenido de forma coordinada y sistemática para afectar los resultados de la elección presidencial. Del mismo modo, que se consideraba tenían las capacidades de influir en el proceso electoral de 2020. Un aspecto trascendental, es que con la presentación del informe Mueller, la investigación en contra de Donald Trump se centró en los episodios de obstrucción de justicia por parte el entonces presidente de los Estados Unidos de América.

Mientras se dejó completamente de lado una investigación más profunda sobre las cibercapacidades y modo de operación, en que los agentes o ciber atacantes, supuestamente de origen ruso, habían ejecutado una serie de ciberoperaciones para influir en las elecciones de 2016.

En este contexto, destaca que los sucesos del ciberataque a SolarWinds se extiende desde inicios de 2019, atravesando la elección presidencial de 2020, y el primer año de gobierno de Joe Biden. Del mismo modo, que la cada vez mayor evidencia sobre el ataque, se hizo más fuerte y evidente durante los últimos días del gobierno de Trump. Por otra parte, si bien durante las elecciones de 2016, Mueller argumentó que la estrategia de Rusia supuso el uso de desinformación para afectar a la opinión pública y los electores de los Estados Unidos, la evidencia en torno a SolarWinds supone un modo sofisticado y capacidad de acción por parte de una APT de origen ruso, para afectar a instituciones gubernamentales y privadas, vinculadas a las más altas esferas del gobierno estadounidense. En ese sentido, se presenta una recapitulación de los eventos más trascendentales en torno al ciberataque de Solar Winds en esta sección.

4.1.3.1 Año 2019

Los informes empresariales de SolarWinds, indican que, en enero de 2019, un equipo de piratas informáticos se adentró al sistema de la compañía de software. En este contexto, es importante mencionar que SolarWinds es una empresa estadounidense que desarrolla sistemas informáticos para la administración de redes e infraestructura de tecnología de la información en los Estados Unidos. Hasta 2019, se estimaba que tenía alrededor de 300,000 clientes, entre los que destacaban las 500 empresas más grandes de los Estados Unidos, ranqueadas por la revista Fortune, así como un número importante de agencias federales del gobierno de Washington D.C. (Tucker, 2021), con lo cual una vulneración a esta empresa compromete gran cantidad de la información de múltiples actores involucrados en la ciberseguridad, con carácter de seguridad nacional de los Estados Unidos.

Una vez infiltrado con un código malicioso el sistema de SolarWinds, la empresa detectó que fue hasta el 4 de septiembre que un actor con intención de vulnerarlo accedió al mismo (Ramakrishna, 2021). Y entre el 12 de septiembre y el 4 de noviembre fue que este actor de

amenazas inyectó el código de prueba y realizó una ejecución de prueba (Ramakrishna, 2021). Posteriormente, en diciembre los piratas informáticos accedieron al menos a una de las cuentas de Office 365 de SolarWinds y saltaron a otras cuentas del mismo servicio utilizadas por la empresa. Según declaraciones de Sudhakar Ramakrishna, el director ejecutivo de la empresa, con esta acción los piratas informáticos comprometieron las cuentas de correo electrónica de la empresa y otros usuarios de esta (McMillan, 2021).

4.1.3.1 Año 2020

Una vez penetrado el sistema de SolarWinds y vulneradas las credenciales de acceso de la cuenta de Office 365 de la empresa, el siguiente paso de los piratas informáticos fue atacar a la firma de ciberseguridad FireEye, una de las empresas líder en detección de ciber ataques de los Estados Unidos tanto en el ámbito privado, como gubernamental. FireEye utilizaba servicios y sistemas informáticos de Solar Winds, y según sus declaraciones, sus sistemas sufrieron un ciber incidente el 8 de diciembre de 2020. En este punto, la firma destacó que, por el modo de operación del comando de piratas informáticos, no se trataba de una pequeña célula de programadores, sino de una APT, es decir de un comando cibernético patrocinados por algún Estado-Nación. FireEye destaco que la APT irrumpió en su red interna y robaron las herramientas de prueba de penetración de su Equipo Rojo, comando encargado de realizar pruebas de penetración o intentos de ciberataques a sistemas de empresas privadas o gobiernos que contratan sus servicios (Panettieri, 2020a). Con conocimiento de este evento, el 12 de diciembre, FireEye alertó al entonces director ejecutivo de SolarWinds, Kevin Thompson, de que el sistema desarrollado por su empresa de nombre *Orion*, utilizado por 33.000 clientes de Solarwinds, incluidas empresas e instituciones de gobierno (Bing, 2020), contenía una vulnerabilidad como resultado de un ataque cibernético (SolarWinds, 2020). Frente a este evento, la Casa Blanca convocó a una reunión de emergencia del Consejo de Seguridad Nacional con el fin de discutir un ciberataque que violó la seguridad de la información y ciberseguridad de múltiples agencias gubernamentales y empresas de los Estados Unidos (Bing, 2020).

Como consecuencia de la reunión, el 15 de diciembre de 2020, la directiva de emergencia de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA por sus siglas en inglés), parte del Departamento de Seguridad Nacional de los Estados Unidos, emitió la directiva de

emergencia 21-01, que ordena a las agencias federales apagar SolarWinds y el sistema Orion debido a una amenaza de seguridad importante (Kass, 2020). En este contexto, la empresa mando a sus usuarios un aviso de seguridad en el que describía el ataque a la plataforma y las medidas defensivas asociadas para evitar vulneración. Por su parte, FireEye indicó a los usuarios que los atacantes se habían aprovechado de la cadena de suministro de SolarWinds para comprometer a múltiples víctimas globales (FireEye, 2020). Entre las empresas más reconocidas que utilizaban Orion, y se habían visto comprometidas, se encontraban Microsoft, que ofreció una guía de ciberseguridad frente al incidente a sus usuarios. Para este punto, la cobertura de los medios de comunicación hablaba de un informe inicial realizado por el CISA que indicaba que el ciberataque de SolarWinds, a través de Orion, indicaba que una APT de origen ruso había estado monitoreando el tráfico de correo electrónico interno en los departamentos del Tesoro y Comercio de los Estados Unidos, y que esto sólo podía ser la punta del iceberg (Bing, 2020).

Posteriormente, el 15 de diciembre de 2020, SolarWinds lanzó corrección de software para los usuarios que utilizaban Orion (Ramakrishna, 2021). Y se confirmó como víctimas del ataque a los Departamentos de Comercio y del Tesoro de los Estados Unidos. En pocas horas, también se añado el Departamento de Seguridad Nacional, los Institutos Nacionales de Salud y el Departamento de Estado (Volz y McMillan, 2020). Ante la creciente expectativa de los alcances del ataque un grupo bipartidista de seis senadores solicitaron al FBI y la CISA que presentaran un informe al Congreso sobre el impacto del ciberataque de SolarWinds en las agencias gubernamentales de los Estados Unidos. En concreto, los legisladores buscaban responder seis preguntas, entre las que destacaban: 1) ¿cuántas agencias se vieron afectadas?, 2) ¿cómo el FBI y CISA trabajaron juntos para abordar el ataque y si las agencias no implementaron la *Federal Information Security Management Act of 2002* (FISMA) u otras leyes cibernéticas? A la par de que los senadores requisitaron también quieren una sesión informativa adicional sobre el incidente (White, 2020).

Finalmente, SolarWinds detecto el 16 de diciembre el nombre de dominio malicioso clave utilizado en el ataque, e indicó que los expertos en seguridad habían apagado el código, con lo cual ya no existía amenaza de ciberexplotación en los sistemas que utilizaban Orion (KrebsOnSecurity, 2020). A pesar de esto, la editorial del *New York Times* presentó en

portada ese día las declaraciones de Thomas P. Bossert, exasesor de seguridad nacional del presidente Trump, quien indicó que: "*es difícil exagerar la magnitud de esta violación de la seguridad nacional* (New York Times, 2020). Del mismo modo, destaca que en esta jornada el FBI inicio la investigación y comenzó a reunir las fuentes de inteligecia para atribuir, perseguir e interrumpir a los actores de amenazas responsables en el incidente de SolarWinds. (CISA, 2020).

Al día siguiente, el CERT de los Estados Unidos emitiría una alerta, a razón de que Microsoft descubrió que más de 40 de sus clientes habían podido ser víctimas a través del sistema Orion. De los cuales, aproximadamente el 44 por ciento de estos eran proveedores de servicios de TI, empresas de software o tecnología. Con lo cual Microsoft describió la necesidad de una "*respuesta de seguridad cibernética fuerte y global"* (Kovar y Johnson, 2020). Entre los afectados estaban cinco proveedores de soluciones de TI y firmas de consultoría de fama global como Deloitte, Digital Sense, ITPS, Netdecisions y Stratus Network, los cuales habían sido vulnerados desde principios de este 2020 (Poulsen, McMillan y Volz, 2020). También, en esta misma jornada, se encontró evidencia de que la APT rusa accedieron a los sistemas de la Administración Nacional de Seguridad Nuclear, que mantiene las reservas de armas nucleares de EE. UU. (Bertrand y Wolf, 2020).

En este contexto, la casa Blanca convocó a una segunda reunión a puerta cerrada para analizar la violación de SolarWinds y Orion, las víctimas del ataque, las posibles consecuencias y una posible respuesta. (Bloomberg, 2020). En esta, Microsoft presentó una investigación e indicó que detectaron códigos binarios maliciosos de Solar Winds en sus sistemas, los cuales ya habían sido aislados y eliminados Del mismo modo, externaron que encontraron evidencia de acceso a servicios de producción o datos de clientes. O algún indicio de que sus sistemas fueron utilizado para atacar a otros. Frente a estos eventos, el presidente electo Joe Biden prometió elevar la seguridad cibernética como un "*imperativo*" cuando asumiera su cargo. Del mismo modo, indico que "*no se quedará de brazos cruzados*" frente a los ataques cibernéticos luego de una brecha masiva que afectó al gobierno de los EE. UU. Mientras, el presidente Trump no hizo ningún comentario público sobre el ataque. (Chalfant, M. y Maggie M., 2020).

El 19 de diciembre, el secretario de Estado de EE. UU., Mike Pompeo, en una declaración pública culpó a Rusia por el ataque informático a SolarWinds y el sistema Orion, que comprometió a numerosas agencias federales y corporaciones de los Estados Unidos. A pesar de esto, el presidente Trump se mostró escéptico ante el creciente consenso en Washington sobre el país origen de la APT (Panettieri, 2020b). Y para el 21 de diciembre, el Departamento del Tesoro de EE. UU. Dio una declaración, en la que indicó que el ataque afectó sus sistemas no clasificados, aunque según su titular, Steven Mnuchin, no se detectó ninguna afectación (Reuters, 2020). Por último, se indicó que docenas de cuentas de correo electrónico en el Departamento del Tesoro se vieron comprometidas, entre las que se encontraban las utilizadas por los funcionarios de más alto rango del departamento (Tucker, 2020).

El cierre de los efectos de SolarWinds se daría el 30 de diciembre cuando la CISA actualizó su guía sobre la vulnerabilidad de SolarWinds y el sistema Orion. Co la que incitó a todas las agencias federales que operan versiones de la plataforma a que identificaran si poseían una "*versión afectadas*" o no de la misma. Por su parte, la Agencia de Seguridad Nacional (NSA) examinó la versión más reciente de Orion y comprobó que elimina el código malicioso previamente identificado (CISA, 2020).

4.1.3.1 Año 2021

La trama SolarWinds continuó el 5 de enero de 2021, con la acusación pública y formal de agencias de inteligencia de los Estados Unidos, como la CISA, el FBI, la NSA y la Oficina del Director de Inteligencia Nacional a la Federación Rusa de estar vinculada al ciberataque de SolarWinds a través de una APT (Miller, 2021a). Posteriormente, Kaspersky dijo que el hackeo de SolarWinds y el sistema Orion se asemejaba al malware vinculado a un grupo de hackers conocido como *Turla*, que según autoridades de Estonia opera en nombre del Servicio Federal de Seguridad de la Federación de Rusia o FSB por su acrónimo en ruso (Stubs, 2021). Por su parte, el Departamento de Trabajo indicó que ya preparaba un informe de empleos y otra información sensible al mercado sobre la economía de EE. UU., que fue violado en el hackeo de SolarWinds (Morath y Chaney, 2021).

En este contexto, sería hasta después de la toma de protesta del presidente Joe Biden, el 22 de enero, que el jefe del ejecutivo indicaría que la Casa Blanca contrataría a un grupo de

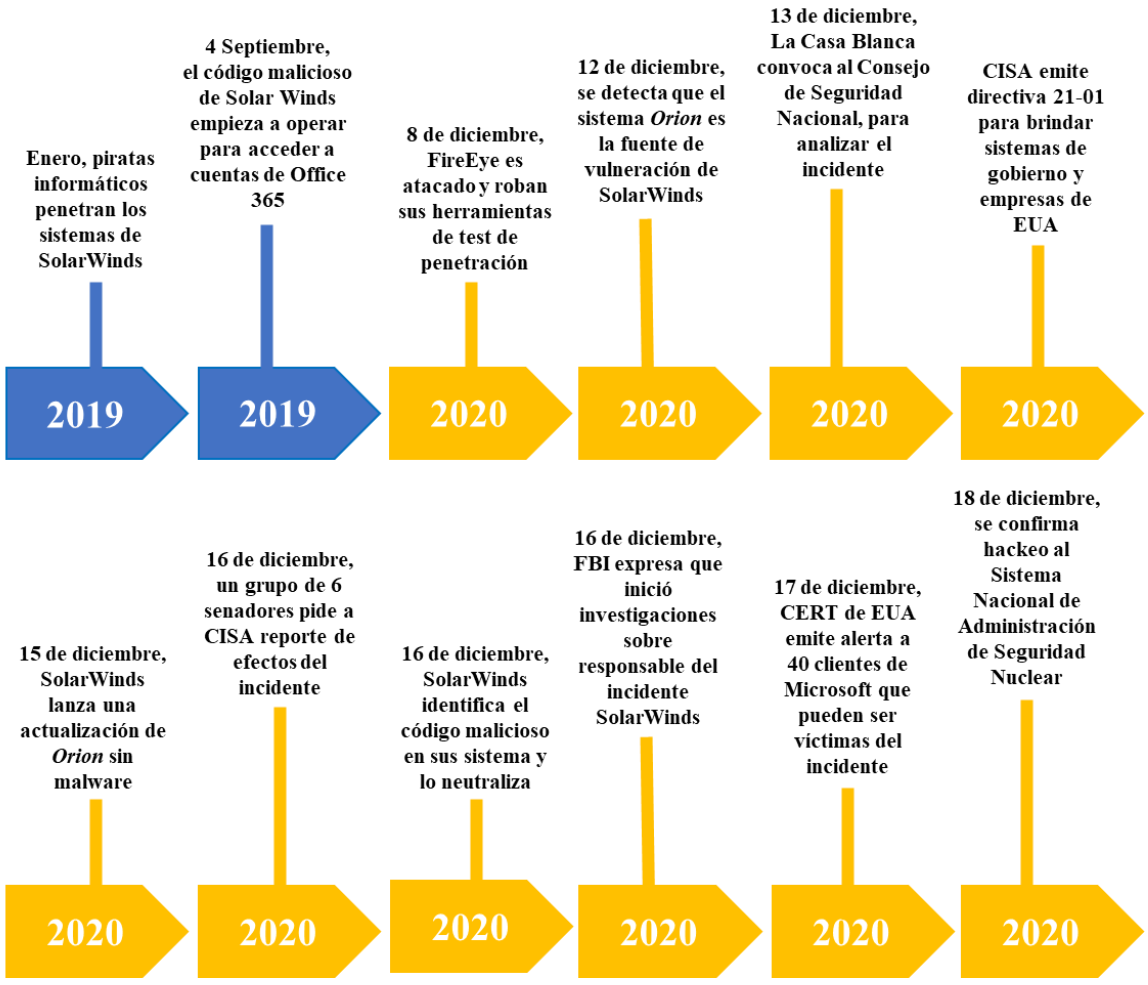
veteranos de la seguridad nacional con una gran experiencia en cibernética, para que el gobierno de los Estados Unidos pudiera recuperarse de los ataques informáticos relacionados con SolarWinds y Orion (Reuters, 2021). La investigación corrió a cargo de Anne Neuberger, la asesora adjunta de seguridad nacional para tecnología cibernética y de emergencia de la Casa Blanca (Sunderman, 2021). Y entre los hallazgos más trascendentales, identificaron que un segundo grupo de piratas informáticos, con sospechas de origen en China, aparte de la APT rusa habían podido aprovechar la vulnerabilidad para ingresar a las computadoras del gobierno de EE. UU. (Bing *et al.*, 2021). Finalmente, Neuberger, indicó que la revisión federal del hackeo de SolarWinds, se encontraba en sus primeras etapas y tardaría varios meses en completarse. Asimismo, expresó que el ataque comprometió a nueve agencias federales y unas 100 empresas privadas (Betz, 2021).

Posteriormente, sería hasta el 23 de febrero que el Comité de Inteligencia del Senado llevó a cabo una audiencia sobre la violación de SolarWinds. En dicha reunión se convocó al director ejecutivo de la empresa Sudhakar Ramakrishna, a testificar. A la par de testigos como el presidente de Microsoft, Brad Smith, el director ejecutivo de FireEye, Kevin Mandia, y el presidente y director ejecutivo de CrowdStrike, George Kurtz (Miller, 2021b). Como consecuencia de la reunión, la administración Biden indicó que impartiría sanciones y otras medidas para castigar a Rusia por acciones que van más allá de la extensa campaña de ciberespionaje de SolarWinds, para incluir una variedad de actividades cibernéticas con el fin de vulnerar a los Estados Unidos (The Washington Post, 2021).

Por último, el 29 de marzo de 2021, el equipo de Neuberger indicó que la APT de Rusia obtuvo acceso a cuentas de correo electrónico del jefe del Departamento de Seguridad Nacional de la administración Trump y miembros del personal de seguridad cibernética del departamento cuyos trabajos incluían la caza de amenazas de países extranjeros (Panettieri, 2021). Frente a esto, el 15 de abril diez diplomáticos fueron expulsados como parte de un nuevo paquete de sanciones anunciado por el presidente de Estados Unidos. Además, esa misma fecha se aplicaron sanciones contra empresarios y empresas rusas. Esto, en represalia por la interferencia de Moscú en las elecciones y el ciber ataque a SolarWind (Roth, A & Borger, 2021). Finalmente, el 30 de julio la firma de ciberseguridad con sede en California RiskIQ Inc., presentó en un informe publicó que e grupo de piratas informáticos involucrados

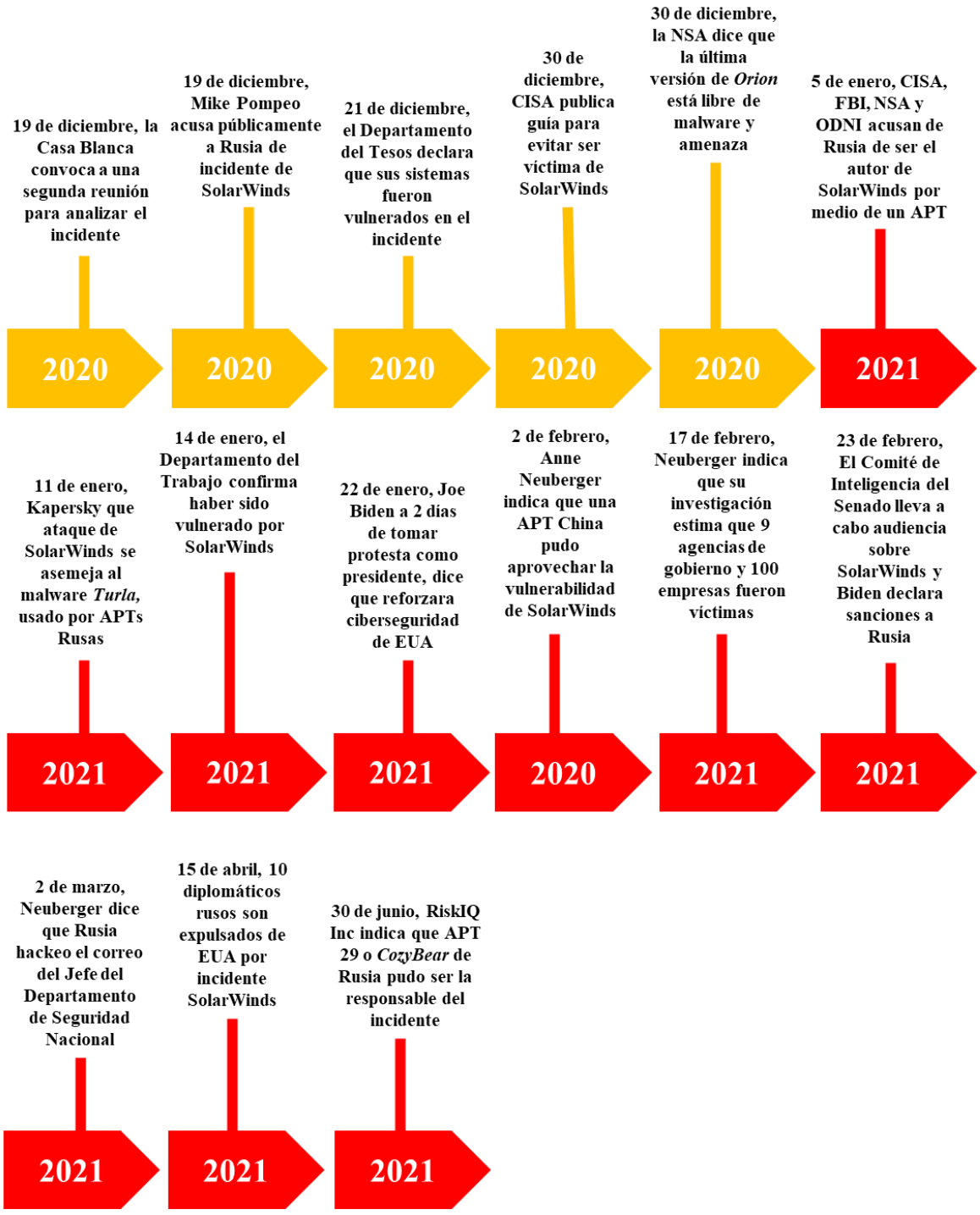
en el caso SolarWinds, casi con total certeza, había sido APT29 o *Cozy Bear*. Sobre el cual agencias gubernamentales de seguridad nacional de Reino Unido y Canadá consideran forma parte de los servicios de inteligencia rusos. Del mismo modo, se creía que dicho grupo también estuvo presuntamente involucrado en el ataque de 2016 al Comité Nacional Demócrata durante la campaña electoral que llevó a Trump a la presidencia (Gallagher, 2021). A continuación, en la figura 48 se presenta una línea del tiempo con los principales eventos asociados a esta trama.

Figura 48. Línea del tiempo de la cronología de la trama *SolarWinds* (Parte 1).



Fuente: Elaboración propia.

Figura 48. Línea del tiempo de la cronología de la trama *SolarWinds* (Parte 2).



Fuente: Elaboración propia.

4.2 Análisis del *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016*

Complementario a nuestro análisis de fuentes abiertas, en la presente sección se realiza un análisis del contenido del *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016,* presentado por el Fiscal Especial Robert Mueller el 18 de abril de 2019. En el cuál se presentan los resultados de su investigación especial en torno a los nexos de Donald Trump con agentes del gobierno ruso, y cómo pudo orquestarse una ciber operación de esta nación que inclinó la balanza de la disputa electoral a un triunfo de dicho candidato.

Sobre la decisión de estudiar este documento, se especifica que el documento de 448 páginas está abierto al público con fragmentos de información clasificada, presenta un panorama más amplio sobre los hallazgos de la investigación sobre la interferencia de Rusia en las elecciones de 2016 y los episodios de obstrucción de justicia por parte del presidente Trump. En ese sentido, se pretende analizar cada uno de los dos volúmenes, con la finalidad de encontrar hallazgos no identificados en el análisis de fuentes abiertas, que den más información sobre las tramas de Russiangate, Investigación del Fiscal Especial e *Impeachment* y SolarWinds.

4.2.1 Estructura del Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016

Como se especificó en la sección anterior, el Informe Mueller se divide en dos diferentes volúmenes. El primero corresponde a presentar los hallazgos de la investigación sobre la interferencia de Rusia en las elecciones de 2016. Este volumen consta de un total de 199 páginas divido en cinco secciones, como se presenta en la tabla 28.

Tabla 28. Estructura del Volumen I del Informe Mueller.

Sección	Páginas
I. La investigación del fiscal especial.	11 – 14.
II. Campaña de "medidas activas" rusas en redes sociales. A. Estrucutura de la Agencia de Investigación de Internet (IRA) B. Financiamiento y supervisión de Concord y Prigozhin. C. Los objetivos de IRA en las elecciones estadounidenses.	14- 35.

III. Operaciones rusas de hackeo y *dumping.* A. La Dirección Principal de Inteligencia del Estado Mayor General del Ejército Ruso (GRU) hackea direcamente a Hillary Clinton. B. Diseminación de los materiales hackeados. C. Ciberoperaciones adicionales de la GRU. D. La campaña de Trump y la diseminación de los materiales hackeados.	36 - 65.
IV. Vinculos del Gobierno Ruso con contactos de la campaña de Donald Trump. A. Periodo de campaña (septiembre 2015 – 8 de noviembre de 2016). B. Post elección y contactos en el periodo de transición.	66 – 173.
V. Decisión de enjuiciamiento y declinaciones. A. Campaña de "medidas activas" rusas en redes sociales. B. Operaciones rusas de hackeo y *dumping.* C. Alcance y contactos del gobierno ruso. D. Declaraciones falsas y obstrucción de la investigación.	173 – 199.

Fuente: Elaboración propia con base a Mueller (2019).

En este sentido, se argumenta que los principales hallazgos del Volumen I se centran en presentar la evidencia en torno a los esquemas de operación, de actores y organismos del origen ruso, para afectar en la campaña electoral de 2016. Mientras que, en segunda instancia, busca identificar evidencia de colusión entre el equipo de campaña de Donald Trump, y autoridades rusas, para que el candidato republicano se beneficiara durante el proceso electoral en una época posterior a esta. Por último, el volumen cierra presentando la decisión de la Fiscalía Especial, con base estos dos ejes de investigación, por enjuiciar o no al presidente.

Respecto al Volumen II del Informe Mueller, se especifica que éste está abocado a analizar en primera instancia el marco legal de obstrucción de justicia, mediante el cuál se podría juzgar como indebida la conducta del presidente, en torno a actos de investigación, sobre la trama del *Russiangate* y una serie de decisiones y acciones que ejerció, para entorpecer el trabajo del Fiscal Especial, en torno a este proceso. De esta forma, la segunda parte del volumen analiza la conducta del presidente, con base a evidencia factual y probatoria, para identificar si existen elementos que permitan identificar en su conducta un acto de obstrucción de justica, desde los inicios del proceso de campaña, el periodo de transición, las

pólemicas en torno al despido de Micahel Flyn y la forma en que pidió a funcionarios del gobierno de los Estados Unidos o personalidades cercana a él, que no colaboraran con la Fiscalía Especial. Por último, de nueva cuenta, el volumen cierra con un análisis presentado por el equipo de Robert Mueller, para establecer la decisión de enjuiciar a o no al presidente. La estructura completa del Volumen II, puede observarse en la tabla 29.

Tabla 29. Estructura del Volumen II del Informe Mueller.

Sección	Páginas
I. Marco Legal y evidencia probatoria. A. Marco legal de la obstrucción de justicia. B. Consideraciones evidenciarias einvestigativas.	9-14.
II. Resultados factuales de la investigación de obstrucción de justicia. A. La campaña de respuesta a los reportes sobre apoyo de Rusia a Trump. B. La conducta del presidente concerniente a la investigación de Michael Flynn. C. La reacción del presidente a la confirmación pública del FBI de la investigación sobre Rusia. D. Eventos que preceden y rodean el despido de Comey director del FBI. E. Esfuerzos del presidente por acotar la investigación del Fiscal Especial. F. Esfuerzos del presidente para prevenir la disfusión e E-mails del 9 de junio de2016, entre autoridades rusas y el equipo de campaña de Donald Trump. G. Esfuerzos intensificados del presidente para que el fiscal general se haga cargo de la investigación. H. El presidente redobla los esfuerzos para que el Fiscal General se haga cargo de la investigación. I. El presidente ordena a McGahan que niegue que el haya intentado despedir al Fiscal Especial. J. La conducta del presidente hacia la Flynn y Manafort. K. La conducta del presidente que involucra a Michael Cohen. L. Cuestiones fácticas generales.	15-158.
III. Defensas legales a la aplicación de la condición de obstrucción de la justicia al presidente. A. Defensas legales de la aplicación de las disposiciones de obstrucción de la justicia a la conducta investigada. B. Defensas constitucionales para aplicar un estatus de obstrucción de la justicia a la conducta del presidente.	159-181.

Fuente: Elaboración propia con base a Mueller (2019).

Una vez descrita esta estructura, en la siguiente sección se presenta un análisis de los principales contenidos de cada volumen del reporte Mueller.

4.2.1.1 Análisis del Volumen I

El Volumen I del *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016* se centra en presentar la evidencia, por parte de la Fiscalía Especial, de cómo el gobierno ruso interfirió en las elecciones presidenciales de manera sistemática y bien estructurada. El documento destaca que la evidencia de las operaciones del gobierno ruso comenzó a aparecer a mediados de 2016. De forma más concreta, a partir de junio, cuándo el Comité Nacional Demócrata y su equipo de respuesta cibernética anunciaron públicamente que hackers rusos habían comprometido su red informática e información sensible del partido y la candidata electoral Hillary Clinton. En ese sentido, el reporte externo que, a finales de julio del 2016, un gobierno extranjero contactó al FBI para informar que el asesor de Trump, George Papadopoulos, había sugerido tener indicaciones del gobierno ruso para apoyar a la campaña de Trump mediante la divulgación de información perjudicial de la entonces candidata Hillary Clinton.

Posteriormente en otoño del 2017, agencias federales anunciaron que el gobierno ruso realizó robo y divulgación de información para interferir con las elecciones estadounidenses. Frente a esto, los esfuerzos de investigación de la interferencia rusa en las elecciones llevaron en mayo del 2017 al nombramiento del Fiscal Especial Robert Mueller. Sobre este episodio, el reporte Mueller (2016) detalla que Rusia interfirió mediante dos operaciones. La primera, Rusia llevó a cabo campañas en redes sociales para favorecer al candidato Trump y afectar la reputación de la candidata Hillary Clinton. En segundo lugar, Rusia llevó a cabo operaciones informáticas contra entidades, empleados y voluntarios de la campaña de Clinton a fin de robar información. De igual forma, se identificaron numerosos vínculos entre el gobierno ruso y la campaña de Trump. Por lo que el informe Mueller describe las acciones y eventos encontrados respaldados por evidencia. Asimismo, al evaluar la evidencia de acción colectiva la Fiscalía Especial aplicó el marco de la ley de conspiración, y no de colusión. Por tanto, el enfoque fue analizar las cuestiones de responsabilidad penal conjunta (Mueller, 2016).

También, es importante mencionar que un actor central analizado en el Volumen 1, es la organización rusa, *Internet Research Agency* (IRA), la cual llevó a cabo las primeras operaciones de interferencia rusa en las redes sociales. Y cuyo bjetivo era diseñar y provocar campañas de polarización política y social, en el marco de las elecciones de 2016. El informe indica que IRA recibió fondos del oligarca ruso Yevgeniy Prigozhin, mismo quien tiene vínculos con el presidente Vladimir Putin para dicha acción. A la par que las operaciones de IRA incluyeron la compra de anuncios políticos en redes sociales a nombre de personas estadounidenses. Así como la organización de mítines para favorecer la campaña de Trump. A pesar de esto, la investigación no reveló evidencia de personas estadounidenses que conspiraron con IRA. Ni siquiera los personajes del equipo de campaña de Trump que, durante varios puntos de la elección, estuvieron en contacto con diferentes personalidades rusas. En este contexto, en la tabla 30, se presentan los principales elementos obtenidos, en cada una de las tres diferentes secciones del volumen, que presentan información adicional y complementaria a la obtenida en la revisión de fuentes abiertas.

Tabla 30. Principales hallazgos del Volumen I.

Operaciones rusas de hackeos.	● A principios del 2016 el gobierno ruso empleó una segunda forma de interferencia: intrusiones cibernéticas (piratería) y liberación de información pirateada que fuera perjudicial para la campaña de Clinton. ● El servicio de inteligencia ruso conocido como la *Dirección Principal de Inteligencia del Estado Mayor del Ejército Ruso* (GRU) llevó a cabo estas operaciones. ● En marzo del 2016, la GRU comenzó a piratear cuentas de correo electrónico de empleados de la campaña de Clinton, incluidos el presidente de campaña, John Podesta. ● En abril de 2016, GRU pirateó al Comité de Campaña del Congreso Demócrata (DCCC) y al Comité Nacional Demócrata (DNC). ● GRU utilizó a actores ficticios como *DCLeacks*, *Guccifer 2.0* para publicar la información, más tarde, la información se compartió en WikiLeaks. ● La campaña Trump mostró interés en las publicaciones de WikiLeaks y fue receptiva al apoyo que le brindó al candidato republicano.
Contactos rusos con campaña de Trump	● La campaña en redes sociales y las operaciones de GRU coincidieron con una serie de contactos entre funcionarios de la campaña Trump y personas vinculadas con el gobierno ruso. ● La investigación dictamina que si bien, Rusia estaba interesada en que Trump ganara la elección; no hay ninguna prueba concluyente de que miembros de la campaña Trump conspiraron con este país. ● Los contactos rusos consistieron mayormente en conexiones comerciales, ofertas de asistencia a la campaña, e invitaciones para que Trump y Putin se reunieran en un futuro.

	● Algunos de los primeros contactos fueron entre un proyecto inmobiliario entre la Organización Trump en Rusia, conocido como *Trump Tower Moscow*. ● En la primavera de 2016, el asesor de política exterior de campaña, G. Papadopoulos se puso en contacto con Joseph Mifsud, quien le comunicó que el gobierno ruso tenía información comprometedora de Hillary Clinton, que podía ser de su interés. ● El 9 de junio de 2016, un abogado ruso se reunió con altos funcionarios de la campaña de Trump, J. Kushner y el presidente de campaña, P. Manafort para entregar "*documentos e información oficiales que incriminarían a Hillary"*. ● Días después, una firma de ciberseguridad y el DNC anunciaron que hackers del gobierno ruso se habían infiltrado en sus sistemas y extraido información. ● El 2 de agosto de 2016, P. Manafort se reunió en Nueva York con su socio comercial Konstantin Kilimnik, quien el FBI acusara de tener vínculos con la inteligencia rusa. Kilimnik solicitó la reunión para entregarle a Manafort un plan de paz para Ucrania. Ambos creían que, si Trump fuera presidente, avalaría el plan. ● El 29 de diciembre de 2016, el presidente Obama impuso sanciones a Rusia por haber interferido en las elecciones. El asesor entrante de Seguridad Nacional, Michael Flynn llamó al embajador ruso Sergey Kislyak y le pidió que Rusia no empeorara la situación en respuesta a las sanciones. Al día siguiente, Putin anunció que Rusia no tomaría represalias por las sanciones en ese momento.
Las decisiones a cargo del asesor especial.	● La oficina del Fiscal Especial determinó que las dos operaciones de Rusia en las elecciones del 2016 violaron la ley penal de EE. UU. Múltiples personas y entidades involucradas han sido acusadas de participar en actos de conspiración contra EE. UU. ● Los oficiales de inteligencia rusos que llevaron a cabo la piratería en las computadoras del Partido Demócrata y las cuentas de correo de Clinton, además del delito de conspiración, se les acusa de haber violado el estatuto federal de intrusión informática. ● El ex asesor de seguridad nacional, M. Flynn, se declaró culpable de mentir sobre sus interacciones con el embajador ruso Kislyak durante la transición del gobierno. ● G. Papadopoulos, se declaró culpable de mentir a la investigación sobre sus interacciones con el profesor J. Mifsud., M. Cohen se declaró culpable de hacer declaraciones falsas al congreso sobre el proyecto de la Torre Trump en Moscú. De igual forma, se encontró que Manafort había mentido a la oficina del fiscal en lo que se refirió a sus comunicaciones con Kilimnik sobre el plan de paz en Ucrania.
Investigación del consejero especial	● El Fiscal Especial estuvo autorizado para realizar la investigación que intentó llevar a cabo el ex director del FBI, J. Comey. Y también estuvo autorizado para investigar cualquier relación y/o coordinación entre el gobierno ruso e individuos de la campaña de Trump. ● El Fiscal Especial estuvo autorizado desde su nombramiento para investigar las denuncias contra tres funcionarios de la campaña de Trump, Carter Page, Paul Manafort y George Papadopoulos. ● Para llevar a cabo la investigación, la Fiscalía Especial reunió a un equipo que en su mayor punto se conformó por 19 abogados, 5 de ellos

	provenientes del sector privado, mientras 14 fueron designados del Departamento de Justicia. ● Durante la investigación la Fiscalía Especial emitió más de 2.800 citaciones bajo auspicios del gran jurado reunido en el Distrito de Columbia. Se ejecutaron más de 500 órdenes de registro e incautación, se obtuvo más de 230 pedidos de registro de comunicaciones, y realizaron entrevistas a más de 500 testigos ● Desde sus inicios, la oficina del Fiscal Especuial, reconoció que su investigación podría ayudar a identificar información de inteligencia extranjera y contrainteligencia para fines de Seguridad Nacional. Por lo cual, la División de Contrainteligencia del FBI se reunió con ellos regularmente.
Medidas de Rusia en la campaña en redes sociales.	● La primera forma de influencia rusa en las elecciones provino de la empresa *Internet Research Agency* (IRA). Dicha organización fue fundada por Yevgeniy Prigozhin, otra compañía que él controlaba era *Concord Management and Consulting LLCC* y *Concord Catering*, estas fueron las 3 empresas acusadas por la Fiscalía Especial. ● IRA condujo operaciones en las redes sociales teniendo como objetivo a largas audiencias de cibernautas estadounidenses. El propósito, era crear discordia en las redes sociales en temas relacionados con el sistema político de EE. UU. ● Trabajadores de IRA se hicieron pasar en redes sociales por personas estadounidenses. También, las actividades de IRA incluyeron comprar anuncios que repercutieron en la imagen de Clinton. ● De igual manera, trabajadores de IRA estaban en comunicación con líderes de *rallies* pro-Trump. Se destaca que ocultaron su nacionalidad rusa y se hicieron pasar por estadounidenses. ● Para 2016, IRA había alcanzado a millones de ciudadanos estadounidenses por medio de las redes sociales. Los trabajadores de IRA controlaban grupos de Facebook, cuentas de Instagram y Twitter. ● Facebook identificó 470 grupos controlados por IRA y más de 80,000 cuentas. Mediante esto, se alcanzó a 126 millones de usuarios en Facebook. ● En Twitter se identificaron 3,814 cuentas controladas por IRA y 1.4 millones de usuarios que estuvieron en contacto con dichas cuentas.
Estructura de IRA y forma de operación durante la elección presidencial de 2016.	● La estructura de IRA se creó en 2014, al interior de los Estados Unidos. Pronto, empezó a esconder sus actividades y sus operaciones en el país, que se según la Fiscalía Especial, formaban parte de una operación a gran escala llamada "Project Lakha." ● Numerosos medios reportaron los lazos entre Putin y el fundador de IRA, Prigozhin. También, la Fiscalía Especual detectó evidencia fotográfica de los dos estando juntos. ● El departamento de IRA que ejecuto las operaciones se llamaba "*Translator*", estaba subdividido en diferentes funciones y operaciones en redes sociales, que iban desde análisis, creación de contenido, y equipo de soporte técnico. ● Empleados de IRA viajaron a EE. UU. con el objetivo de recolectar información e inteligencia. En junio del 2014, 4 empleados de IRA aplicaron para trabajar en el Departamento de Estado de EE. UU. ● En mayo 2016, empleados de IRA se hicieron pasar por activistas sociales en grupos de Facebook con el objetivo de reclutar internautas estadounidenses.

	● Docenas de empleados de IRA controlaban a los usuarios falsos de internet, así como las páginas de redes sociales. Dichos empleados eran designados como "especialistas", los cuales incluía a personas enfocadas en Facebook, Youtube o Twitter, más tarde se agregarían especialistas en Tumblr e Instagram. ● En una primera etapa, IRA creaba cuentas falsas de personas supuestamente estadounidenses. Más tarde, IRA se enfocó en crear grupos que conglomeran a grandes cantidades de usuarios, dichos grupos tendrían relación con cuestiones políticas y sociales. ● Los grupos y cuentas que creaba IRA estaban enfocados en cuestiones antimigrantes, anti-movimiento black lives matters, o en favor del movimiento Tea Party, entre otros. ● La Fiscalía Especial encontró fragmentos de un documento interno de IRA que presentana a los colaboradores de su campaña, como operar. Durante las elecciones del 2016, IRA intensificó sus actividades en grupos para el "aseguramiento de las fronteras". En adicional, era imperativo alentar la crítica a Hillary Clinton. ● Los trabajadores de IRA sabían que su propósito era influenciar las elecciones de EE.UU. Los grupos de Facebook creados por IRA cubrían una gran variedad de temas políticos relacionados con la perspectiva conservadora. ● Acorde a Facebook, para esto, IRA pagó más de 3,500 anuncios de publicidad, gastando más de $100,000 USD. Haciendo un recuento total, alcanzó a más de 10 millones de ciudadanos estadounidenses mediante las redes sociales. ● Las operaciones en Twitter involucraron dos estrategias: 1) Empleados de IRA crearon perfiles haciéndose pasar por ciudadanos estadounidenses, 2) Creación de redes de bots para extender su contenido. ● En 2018, Twitter identificó 3,814 cuentas asociadas con IRA, de las cuales, durante las elecciones habían realizado 175,993 publicaciones en relación con las elecciones. Twitter anunció que aproximadamente 1.4 millones de usuarios reales habían estado en contacto con cuentas controladas por IRA. ● IRA organizaba y promovía rallies políticos pro-Trump en las redes sociales. La Fiscalía Especual identificó docenas de rallies organizados por IR. Algunos rallies tenían apenas unos cuantos participantes, mientras otros lograron juntar centenas de ciudadanos. ● Además de manejar las redes sociales, los especialistas igual estaban encargados en reclutar a estadounidenses para difundir la información y organizar los rallies ● Las personas reclutadas eran contactadas por Twitter, Facebook e Instagram. Se identificó que los usuarios pertenecían a un amplio espectro político. Entre lo cuales se destacaban personas que apoyaban el movimiento Black Matter US o Black First. Otros, fueron de grupos conservadores o moderados. ● La oficina identificó dos formas de interacción de IRA con los miembros de la campaña Trump: 1) Miembros de campaña interactúan con el contenido de IRA, esto fue "*compartiendo*" las publicaciones de Facebook o retwitteando . 2) En algunos casos, miembros de IRA que se hacía pasar por estadounidenses, se comunicaban de manera directa con miembros de la campaña Trump para coordinar rallies. ● Se destaca que múltiples publicaciones de IRA fueron compartidas por líderes de opinión pública, entre los cuales se destacan Donald Trump Jr, Eric Trump, Kellyanne Conway o Brad Parscale.

	● En síntesis, la investigación establece que Rusia interfirió en las elecciones del 2016 con "*medidas activas*" con IRA y otras organizaciones fundadas y controladas por Prigozhin.
Hackeo ruso y dumping de operaciones	● En marzo del 2016, unidades del Directorio Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GRU) hackearon computadoras y correos de empleados y voluntarios de la campaña Clinton, incluyendo el líder de campaña, John Podesta. ● En abril de 2016, GRU realizó hackeos en contra del *Democratic Congressional Campaing Comitte* (DCCC) y en contra del Comité Nacional Demócrata (DNC). ● La información robada se publicó a nombre de personajes ficticios como *DCLeaks* y *Guccifer 2.0.* Más tarde, se publicaría en WikiLeaks. ● La campaña de Trump mostró interés en las publicaciones de WikiLeaks y se identificó que dos Unidades militares del GRU fueron las encargadas de los hackeos al DCCC, DNC y campaña Clinton. Las Unidades fueron la 26165 y 74455. ● La Unidad 26165 del GRU, es una ciber unidad dedicada a atacar objetivos militares, políticos y gubernamentales fuera de Rusia. Dicha unidad está subdividida en dos departamentos, una dedicada al desarrollo de softwares maliciosos especializados (*malware*), mientras que la otra está dedicada a la creación de grandes campañas de *spear phishing*. Esta unidad fue la responsable de los hackeos al DCCC, DNC y la campaña Clinton. ● La Unidad 74455 del GRU, está relacionada a múltiples operaciones cibernéticas. Dicha unidad asistió en la difusión de documentos robados por la Unidad 26165, así como la promoción de contenido anti-Clinton en redes sociales. Algunos miembros de esta unidad hackearon computadoras de algunos políticos de EE. UU. ● Las Unidades utilizaban tecnología especializada para recopilar información estratégica de los sitios web demócratas. Del 10 al 15 de marzo, la Unidad 26165 mando 90 correos *spear phishing.* ● La Unidad 26165 implantó en el DCC y en el DNC malwares personalizados conocidos como "*X-Agent*" y "*X -Tunnel*" ● *X-Agent* fue una herramienta multifuncional de hackeo que registraba movimientos del teclado, capturas de pantalla, así como más información de la computadora infiltrada. *X-Tunnel* fue una herramienta que creó una conexión encriptada entre las víctimas del DCCC y DNC para que el controlador del GRU fuera capaz de mover datos de gran tamaño mediante las computadoras. ● Otro malware utilizado fue "*AMS PANEL*" sirvió como centro de monitoreo de las operaciones. Además, se identificó que estaba en la región de Arizona. ● Sobre *DCLeaks*, se encontró que la Unidad 26165 pagó por este dominio con bitcoins que tenían minando. La página publicó los correos robados de las víctimas. Para controlar el acceso, algunas páginas eran protegidas con contraseñas por un periodo de tiempo. Además de los correos, *DCLeaks* filtró información financiera, datos relacionados con la campaña Clinton, entre otros archivos. De igual forma, se utilizó Facebook y Twitter para divulgar la información robada. Finalmente, se tiene registro que DCLeaks se comunicó con reporteros estadounidenses mediante correos y twitter. *DCLeaks* estuvo operando hasta marzo del 2017 ● Sobre *Guccifer 2.0*, que operaba como un Blog de *WordPress*, se encontró que la página era controlada por la Unidad 74455. *Guccifer 2.0*

	estaba ligada a tags de: *some hundred sheets, illuminati, worldwide known*. *Guccifer 2.0* fue utilizado para publicar información y documentos robados del DNC y DCCC.

Fuente: Elaboración propia con base a Mueller (2019).

4.2.1.2 Análisis del Volumen II

El Volumen II del *Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016* se centra en presentar la evidencia, por parte de la fiscalía especial, en como a partir de 2017, el presidente de los Estados Unidos tomó una variedad de acciones hacia la investigación en curso del FBI sobre la interferencia de Rusia en dicho proceso electoral. Estos eventos, plantearon dudas en el marco jurídico y constitucional de los Estados Unidos sobre si el presidente Trump había realizado actos de obstrucción de justicia, abusando de su posición como titular del poder ejecutivo. En este contexto, la orden que nombró fiscal especial a Robert Mueller otorgó jurisdicción a él y su equipo para investigar asuntos que surgieran directamente de la investigación del FBI, incluido si el presidente había obstruido la justicia en relación con investigaciones relacionadas con este episodio.

De esta forma, es importante destacar el marco legal respecto al delito obstrucción de justica que contempla la investigación, con base a lo establecido en la Orden de Nombramiento del 17 de mayo de 2017 otorgado a Robert Mueller, como titular de la Fiscalía Especial. Que le otorgaron facultades para investigar delitos federales cometidos en el curso de y con la intención interferir con la investigación de la fiscalía, como perjurio, obstrucción de la justicia, destrucción de pruebas e intimidación de testigos. Según el reporte Mueller, tres elementos básicos son comunes para investigar un acto de obstrucción de justicia: (1) un acto de obstrucción; (2) un nexo entre el acto obstructivo y un procedimiento oficial; y (3) una intención corrupta. El reporte define cada uno de los actos de la siguiente manera:

- *Acto obstructivo.* Según el Informe Mueller (2019) es: "*toda conducta corrupta capaz de producir un efecto que impida la debida administración de la justicia, independientemente de los medios empleados*".
- *Nexo con un procedimiento oficial pendiente o contemplado:* Según la ley de obstrucción de la justicia generalmente requiere un nexo o conexión con un procedimiento oficial. Según el informe Mueller (2019) puede incluir una conexión con un procedimiento "*pendiente*" de una agencia federal o una investigación o

investigación del Congreso. Bajo ambos estatutos, el gobierno debe demostrar "*una relación en el tiempo, causalidad o lógica*" entre el acto obstructivo y el procedimiento o investigación que se debe obstaculizar.

- *Intención Corrupta:* Implica el elemento de intención para la obstrucción de la justicia y significa actuar "*a sabiendas y deshonestamente*" o "*con un motivo impropio*" para impedir una investigación por parte de un funcionario público.

En consecuencia, el volumen analiza y presenta evidencias factuales, de episodios en los cuales Donald Trump intentó impedir que la investigación de la fiscalía especial siguiera su curso. Del mismo modo, el informe resume la investigación de obstrucción de la justicia del presidente con una serie de consideraciones, que se presentan a continuación:

1) Con base en la evidencia de este volumen, la Fiscalía Especial tomó una decisión sobre el enjuiciamiento o declinación de este proceso contra el presidente Trump. De esta forma, se decidió no proceder con un enjuiciamiento.
2) La opinión de la Oficina de Consejo Legal (OLC), de la fiscalía especial, concluye que un presidente en ejercicio no puede ser procesado, reconoce que es permisible una investigación criminal durante el mandato del presidente. También, reconoce que un presidente no tiene inmunidad después de que deja el cargo.
3) Se consideró evaluar la conducta que se investiga bajo los manuales y estándares de justicia que rigen las decisiones de enjuiciamiento y rechazo en los Estados Unidos, pero la Fiscalía Especial decidió no aplicar un enfoque que potencialmente podría resultar en un juicio en el que se presentará que el presidente cometió delitos.
4) El OLC razonó que, sería muy difícil preservar el secreto de una acusación, y si una acusación se hacía pública, el estigma y el oprobio podrían poner en peligro la capacidad del presidente de gobernar hasta el fin de su mandato.

5) La evidencia obtenida acerca de las acciones y la intención del presidente presentó problemas difíciles que impiden determinar de manera concluyente que no ocurrió ninguna conducta criminal. En consecuencia, si bien este informe no concluye que el presidente cometió un delito, tampoco lo exonera.

Asimismo, se destaca que la segunda parte del Volumen consta de tres partes. En la sección I, se proporciona una descripción general de los principios de obstrucción de la justicia y resume ciertas investigaciones, pruebas y consideraciones sobre la conducta de Trump. La sección II, establece los resultados fácticos de la investigación de obstrucción y analiza la evidencia. Posteriormente, la Sección III aborda las defensas legales y constitucionales en torno a los episodios de obstrucción de justicia. En el tabla 31se presenta un análisis de los puntos más trascendentales, en el marco del *Russiangate* que fueron identificados en el Volumen II.

Tabla 31. Principales hallazgos del Volumen II

La respuesta de la campaña de Trump a los informes sobre el apoyo de Rusia	• Trump cuestionó si la alianza de la OTAN era obsoleta, y elogió a Putin como un "líder fuerte". La prensa informó que los analistas y comentaristas políticos rusos percibieron a Trump como favorable a Rusia. • A partir de febrero de 2016, y continuando durante el verano, los medios informaron que varios asesores de campaña de Trump parecían tener vínculos con Rusia. Por ejemplo, el asesor de campaña Michael Flynn estaba sentado junto a Vladimir Putin en una gala de RT en Moscú en diciembre de 2015. El asesor de política exterior Carter Page tenía vínculos con una empresa de gas estatal rusa. Por último, el presidente de la campaña, Paul Manafort, había trabajado para el expresidente ucraniano respaldado por Rusia: Viktor Yanukovych. • Trump negó tener negocios y conexiones con Rusia incluso a pesar de que, en junio de 2016, el equipo de campaña de Trump estaba trabajando en los permisos para un rascacielos en Rusia llamado la *Trump Tower Moscow*. Después de la elección, el presidente tenía preocupaciones sobre la interferencia rusa en cuanto a la legitimidad de su elección. *Posibles episodios de obstrucción de justicia:* • Durante la campaña de 2016, los medios de comunicación plantearon preguntas sobre una posible conexión entre la campaña de Trump y Rusia. Estas se intensificaron después de que WikiLeaks publicara

	correos electrónicos dañinos contra el Partido Demócrata que, según se informó, habían sido pirateados por Rusia. • Después de las elecciones, cuando persistieron las dudas sobre posibles vínculos entre Rusia y la Campaña Trump, el presidente electo continuó negando cualquier conexión con Rusia. La interferencia podría ser considerada por parte de la sociedad estadounidense como acto que podría cuestionar la legitimidad de su elección.
Conducta que involucra al director del FBI Comey y Michael Flynn.	• A mediados de enero de 2017, el asesor de seguridad nacional entrante Michael Flynn, le negó falsamente al vicepresidente y otros funcionarios de la administración y agentes del FBI, que había hablado con el embajador ruso Sergey Kislyak sobre la respuesta de Rusia a las sanciones de la Casa Blanca, por su interferencia electoral. • El 27 de enero el presidente invitó al director del FBI, James Comey a una cena privada en la Casa Blanca y le dijo que necesitaba su lealtad. Mas tarde, el 14 de febrero, el día después de que el presidente solicitó la renuncia de Flynn. *Posibles episodios de obstrucción de justicia:* • La reunión del presidente del 14 de febrero de 2017 con Comey en la que, según informes, el presidente le pidió a Comey que no siguiera investigando a Flynn. • Las solicitudes privadas del presidente a Comey para que hiciera público el hecho de que el presidente no era objeto de una investigación del FBI y para eliminar lo que el presidente consideraba una nube. • Durante la transición presidencial, el Asesor de Seguridad Nacional entrante Michael Flynn hizo dos llamadas telefónicas con el embajador ruso en los Estados Unidos sobre la respuesta rusa a las sanciones estadounidenses impuestas debido a la interferencia electoral de Rusia. La prensa informó sobre los contactos de Flynn con el embajador ruso, Flynn mintió a los funcionarios entrantes de la Administración diciendo que no había discutido las sanciones en las llamadas.
La reacción del presidente a la continuación de la investigación de sobre Rusia.	• En una sesión informativa el 6 de enero de 2017, la comunidad de inteligencia publicó la versión de su evaluación, que concluyó con gran confianza que Rusia había intervenido en las elecciones a través de una variedad de medios con el objetivo de dañar a Clinton. La evaluación concluyó que el presidente Vladimir Putin y el gobierno ruso había desarrollado una clara preferencia por Trump. • En febrero de 2017, el fiscal general Jeff Sessions comenzó a evaluar si tenía que atenerse a las investigaciones relacionadas con la campaña debido a su papel en la campaña Trump.

	• Después de las sesiones se anunció su reacusación el 2 de marzo, el presidente expresó su enojo por la decisión y dijo a los asesores que debería tener un Fiscal General que lo protegiera. • En marzo Comey confesó públicamente que el FBI investigaba los esfuerzos rusos en las elecciones de 2016. En los días siguientes, el presidente alcanzó al Director de Inteligencia Nacional y a los líderes de la Agencia Central de Inteligencia (CIA) y la Agencia de Seguridad Nacional (NSA) para preguntarles qué podrían hacer para disipar públicamente la sugerencia de que el presidente tenía alguna conexión con el esfuerzo ruso de interferencia en las elecciones. *Posibles episodios de obstrucción de justicia:* • El contacto del presidente con el Director de Inteligencia Nacional y los directores de la Agencia de Seguridad Nacional (NSA) y la Agencia Central de Inteligencia (CIA) acerca de la investigación del FBI sobre Rusia, para negar que lo investigaban.
El despido de James Comey por parte del presidente.	• El 3 de mayo de 2017, Comey testificó en una audiencia del Congreso, pero se negó a responder preguntas sobre si el presidente estaba personalmente bajo investigación. • A los pocos días, el presidente decidió despedir a Comey. En la carta de despido, que fue escrita para su divulgación pública, sostuvo que la decisión se tomo con base a recomendaciones independientes del Fiscal General y Fiscal General Adjunto, a razón de que había descuidado la investigación del correo electrónico de Hillary Clinton. *Posibles episodios de obstrucción de justicia:* • Los fundamentos expresados por el presidente para la rescisión de Comey, el 9 de mayo de 2017, incluidas declaraciones que podrían entenderse razonablemente como un reconocimiento de que la investigación del FBI, sobre Rusia, fue un factor en la rescisión de Comey.
Esfuerzos para restringir la investigación del fiscal especial.	• El 17 de junio de 2017, el presidente llamó a McGahn y le indicó que llamara al Fiscal General Interino, para decirle que el Fiscal Especial tenía conflictos de intereses y debía ser destituido. McGahn no llevó a cabo la instrucción, sin embargo, decidió renunciar por esta orden. • Dos días después de que Trump diera la orden a McGahn para que el fiscal especial fuera destituido, el presidente hizo otro intento de afectar el curso de la investigación de Rusia. El 19 de junio, se reunió personalmente en la Oficina Oval con su ex director de campaña Corey Lewandowski, un asesor de confianza fuera del gobierno, y dictó un mensaje para que Lewandowski lo entregará a la opinión pública.

	● El mensaje decía que, a pesar de su acusación de la investigación de Rusia, la investigación fue "*muy injusta*" para el presidente y que el no había hecho realizado ningún ílicito. Lewandowski le dijo al presidente que el mensaje se entregaría pronto. Sin embargo, él no quiso transmitir el mensaje del presidente personalmente, por lo que le pidió al alto funcionario de la Casa Blanca, Rick Dearborn, que se lo entregara a los medios de comunicación. Dearborn se sintió incómodo con la tarea y no la cumplió. ● Durante 2017, el presidente siguió instando a Sessions a que revocara su recusación de investigaciones relacionadas con la campaña y consideró reemplazar Sessions con un Fiscal General que no sería recusado. Sessions no ofreció garantías ni promesas al presidente de que el Departamento de Justicia cumpliría con esa solicitud. El 7 de noviembre de 2018, el día después de las elecciones intermedias, el presidente reemplazó a Sessions con el jefe de gabinete como Fiscal General Interino. *Posibles episodios de obstrucción de justicia:* ● El presidente le dijo a Sessions que debía renunciar a su cargo de Fiscal General. Sessions acordó presentar su renuncia y abandonó el Despacho Oval. El presidente le devolvió la carta a Sessions con una anotación que decía: "No aceptado". ● La destitución de Sessions, por parte del presidente, por no apoyarlo en terminar la labores de la Fiscalía Especial, de forma abrupta, el 7 de noviembre de 2018, el día después de las elecciones intermedias, el presidente reemplazó a Sessions con el jefe de gabinete de Sessions como Fiscal General Interino.
Esfuerzos para prevenir la divulgación pública de pruebas.	● En el verano de 2017, el presidente se enteró de que los medios de comunicación estaban haciendo preguntas sobre la reunión del 9 de junio de 2016, en Trump Tower entre altos funcionarios de campaña, incluido Donald Trump Jr., y un abogado ruso. ● En dicha reunión, el abogado ruso ofreció información perjudicial sobre Hillary Clinton como parte de Rusia y su apoyo del gobierno a Trump. Sobre esto, el presidente ordenó a su equio que no divulgaran públicamente los correos electrónicos de dicha reunión. ● Más tarde, el entonces candidato editó un comunicado de prensa para borrar la participación de su hijo Donald Trump Jr., borrando una línea que reconoció que el partició en la reunión. Del mismo modo, en el comunicado sólo se indicó que la reunión tuvo como fin un programa adopción de niños de Ucrania y Rusia, y no se citó nada del apoyo ofrecido para dañar la figura de Hillary Clinton. *Posibles episodios de obstrucción de justicia:*

	• La participación informada del presidente en la emisión de una declaración sobre la reunión de la Torre Trump del 9 de junio de 2016, entre rusos y altos funcionarios de la Campaña Trump, que dijo que la reunión era sobre adopción y omitió que los rusos habían ofrecido a proporcionar a la Campaña Trump información despectiva sobre Hillary Clinton. • Los asesores de comunicaciones Hope Hicks y Josh Raffel recordaron haber hablado con Jared Kushner e Ivanka Trump que los correos electrónicos eran dañinos e inevitablemente serían filtrados. Ambos lr advirtieron que la mejor estrategia era publicar de forma proactiva los correos electrónicos a la prensa. El 11 de julio de 2017, Trump Jr. publicó imágenes redactadas de los correos electrónicos que configuraron la reunión del 9 de junio. Con lo que se demostró que la se había mentido sobre los temas tratados en la reunión.

Fuente: Elaboración propia Mueller (2019).

4.2.1.2.2 Análisis de episodios de obstrucción de justicia vinculados a la trama del Russiangate

El análisis del Informe Mueller, en torno a casos de obstrucción de justicia por parte del presidente Trump, encontró un total de diez casos episodios ejecutados por su equipo de campaña, equipo de transición e integrantes de su gobierno. En ese sentido, para fines de la investigación de este documento se localizaron un total de nueve que se enmarcan en la trama del *Russiangate* y presentaron acciones de Trump por evitar o interponerse ante una investigación de sus vínculos con agentes o actores del gobierno ruso.

En ese sentido, y con base al marco legal que aborda el documento del informe Mueller, en torno a las categorías de *acto obstructivo, nexo con un procedimiento oficial pendiente o contemplado* e *intención corrupta* en la tabla 32 se presenta el análisis presentado por la fiscalía especial en torno a cada uno de estos eventos, que se considera son de utilidad e información adicional para las tramas del análisis de fuentes abiertas de *Russiangate* e *Investigación del Fiscal Especial e Impeachment de Trump.*

Tabla 32. Análisis de episodios de obstrucción de justicia por actos o acciones del presidente Trump según el informe Mueller.

La reacción del presidente a la confirmación pública del	***Análisis*** • Al analizar la reacción del presidente a la recusación de Sessions y las solicitudes que hizo para Coats, Pompeo, Rogers y Comey, la

FBI sobre la investigación rusa.	siguiente evidencia es relevante para los elementos de obstrucción de la justicia: ● *Acto obstructivo:* La evidencia muestra que, después del 20 de marzo de 2017, el presidente se acercó repetidamente a los líderes de las agencias de inteligencia para discutir la investigación. Pero los testigos tenían recuerdos diferentes del contenido preciso de esos acercamientos. ● *Nexo con un procedimiento:* En el momento de los acercamientos del presidente Trump a los líderes de las agencias de inteligencia a finales de marzo y principios de abril de 2017, la investigación del FBI sobre Rusia no implicaba procedimientos de gran jurado. Los alcances, sin embargo, vinieron después y fueron en respuesta al anuncio de Comey del 20 de marzo de 2017 de que el FBI, como parte de su misión de contrainteligencia, estaba llevando a cabo una investigación sobre la interferencia rusa en las elecciones presidenciales de 2016. ● *Intención:* La evidencia no establece que el presidente solicitó a los líderes de las agencias de inteligencia que detuvieran o interfirieran con la investigación del FBI sobre Rusia y el presidente dijo afirmativamente a Comey que si "*algún actor*" ruso estaba involucrado en interferencia electoral "*sería bueno saberlo*". ● La evidencia muestra que el presidente se centró en la investigación de Rusia y las implicaciones para su presidencia y, específicamente, con el fin de disipar cualquier sugerencia de que estaba bajo investigación o tenía vínculos con Rusia.
Eventos previos y en torno al despido del director del FBI, Comey.	***Análisis.*** ● *Acto obstructivo:* El acto de despedir a Comey eliminó al individuo que supervisaba la investigación del FBI sobre Rusia. El presidente sabía que Comey estaba personalmente involucrado en la investigación de inteligencia del FBI. ● *Nexo con un procedimiento:* Un conjunto de pruebas demuestran que un procedimiento de gran jurado o un enjuiciamiento penal derivado de una investigación del FBI fue objetivamente previsible, y efectivamente, contemplado por el presidente cuando destituyó a Comey. Con lo cuál su lógica era anular esa posibilidad y terminar la investigación en torno a Rusia. ● *Intención:* Hay pruebas sustanciales que indican que el catalizador de la decisión del presidente de despedir a Comey fue su falta de voluntad para declarar públicamente que el no estaba personalmente bajo investigación, a pesar de las reiteradas solicitudes del presidente de que Comey hiciera tal anuncio.
	Análisis.

Los esfuerzos del presidente para destituir al fiscal especial.	● *Acto obstructivo:* Al igual que con el despido de Comey por parte del presidente, el intento de remover el Fiscal Especial calificaría como un acto obstructivo, si obstruyera naturalmente la investigación y cualquier procedimiento del gran jurado que pudiera derivarse de la investigación. ● *Nexo con un procedimiento oficial:* Para satisfacer el requisito del procedimiento, era necesario establecer un nexo entre el acto del presidente de tratar de rescindir a Mueller y un procedimiento de gran jurado pendiente o previsible. ● *Intención:* Hay pruebas sustanciales que indican que los intentos del presidente de retirar a los abogados especiales estaban vinculados a la supervisión del Fiscal Especial de las investigaciones que involucran a la conducta del presidente y, más inmediatamente, a los informes de que el presidente estaba siendo investigado por posible obstrucción de la justicia.
Los esfuerzos del presidente para reducir la investigación del fiscal especial.	***Análisis*** ● *Acto obstructivo:* El esfuerzo del presidente de enviar un mensaje a Sessions a través de Lewandowski calificaría como un acto obstructivo si obstruyera naturalmente la investigación y cualquier procedimiento del gran jurado que pueda surgir de la investigación. ● *Nexo con un procedimiento oficial:* cuando el presidente tuvo una reunión personal inicial con Lewandowski. La investigación supervisada por el Fiscal Especial era de conocimiento público. En el momento de la reunión de seguimiento del presidente con Lewandowski. Para satisfacer el requisito de nexo, sería necesario demostrar que limitar la investigación del fiscal especial tendría un efecto natural y probable de impedir el procedimiento del gran jurado. ● *Intención:* Hay pruebas sustanciales que indican que el esfuerzo del presidente por limitar a Sessions y el alcance de la investigación del Fiscal Especial a futuras interferencias electorales tenía la intención de evitar un mayor escrutinio investigativo de la conducta del presidente y de su campaña.
Los esfuerzos del presidente para evitar la divulgación de correos electrónicos sobre la reunión del 9 de junio de 2016 entre rusos y altos funcionarios de campaña.	***Análisis*** ● *Acto obstructivo.* En al menos tres ocasiones entre el 29 de junio de 2017 y el 9 de julio de 2017, el presidente ordenó a Hicks y a otros que no divulgaran públicamente información sobre la reunión del 9 de noviembre de 2016 entre altos funcionarios de campaña y un abogado ruso. ● *Nexo con un procedimiento oficial:* cuando el presidente intentó evitar la divulgación pública de los correos electrónicos relacionados con la reunión del 9 de junio, la existencia de una investigación del

	gran jurado supervisada por el fiscal especial era de conocimiento público, y a él le habían dicho que los correos electrónicos responden a las consultas del Congreso. Para satisfacer el requisito de nexo, sería necesario demostrar que la prevención de la liberación de los correos electrónicos al público tendría el efecto natural y probable de obstaculizar los procedimientos del gran jurado o las investigaciones del Congreso. ● *Intención.* La evidencia establece la participación sustancial del presidente en la estrategia de comunicación relacionada con la información sobre las conexiones de su campaña con Rusia y su deseo de minimizar las divulgaciones públicas sobre esas conexiones.
Los esfuerzos adicionales del presidente para que el Fiscal General se haga cargo de la investigación.	***Análisis*** ● *Acto obstructivo.* Para determinar si los esfuerzos del presidente contra el Fiscal General podrían calificar como un acto obstructivo, sería necesario evaluar la evidencia sobre sí naturalmente, esas acciones obstaculizarían la investigación de Rusia. ● *Intención.* Existe evidencia de que al menos uno de los propósitos de la conducta del presidente hacia Sessions iba a hacer que asumiera el control de la investigación de Rusia y la supervisara en una manera que restringiría su alcance.
El presidente ordena a McGahn que niegue que el presidente haya intentado despedir al asesor especial.	***Análisis*** ● *Acto obstructivo.* Los repetidos esfuerzos del presidente para lograr que McGahn creara una declaración que negara que el presidente le hubiera ordenado que destituyera al fiscal especial califica como un acto obstructivo, si tuviese la tendencia natural a impedir que McGahn testificara con sinceridad o socavar su credibilidad como testigo potencial. ● *Intención.* Evidencia sustancial indica que al instar repetidamente a McGahn a disputar que se le ordenó que se destituyera al fiscal especial, el presidente actuó con el propósito de influir en el testimonio de McGahn con el fin de desviar o prevenir un mayor escrutinio de la conducta hacia la investigación.

Fuente: Elaboración propia Mueller (2019).

Revisados los episodios, el Informe Mueller (2019) presenta las cuestiones de hecho fundamentales en torno a cada episodio, citando que parte de su conducta, en cada uno de los episodios, no implicó la autoridad constitucional del presidente para cuestiones de obstrucción de la justicia. Esto a razón, que con base a un análisis fáctico y con evidencia de pruebas de esta conducta, los actos del presidente eran aparentemente lícitos, con la

particulaidad que su posición como titular del Poder Ejecutivo le brindaron un poder único para influir en los procedimientos oficiales, oficiales subordinados y testigos potenciales. Ante esto es importante considerar que muchos casos de obstrucción de justica involucran el intento o el encubrimiento real de un crimen. Sin emnbargo, el Informe Mueller (2019) no identificó evidencia de que el presidente haya estado involucrado en un crimen subyacente relacionado con la interferencia electoral rusa. Sin embargo, esta apunta a un rango de otros posibles motivos personales que animaron la conducta del presidente. Por último, se destaca que la mayoría de los actos del presidente dirigidos a testigos, incluido el desaliento de cooperación con el gobierno y sugerencias de posibles indultos futuros, ocurrieron en público. También, los incidentes a menudo se llevaron a cabo a través de reuniones individuales en que el presidente trató de utilizar su poder oficial fuera de los canales habituales. Aunque los hechos involucraron actos discretos, ese patrón arroja luz sobre la naturaleza de los actos del presidente y las inferencias que pueden extraerse sobre su intención. Del mismo modo, los esfuerzos del presidente para influir en la investigación fueron en su mayoría infructuosos, pero eso es en gran parte porque las personas que rodeaban al presidente se negaron a cumplir órdenes o acceder a sus peticiones.

Por último, el análisis de la Fiscalía Especial instó al Congreso de los Estados Unidos, a que con base a la evidencia identicada investigara y tipificara como delito ciertas conductas obstructivas del presidente, como soborno de perjurio, intimidación de testigos o fabricación de pruebas. A razón de que el marco legal de los Estados Unidos en torno a obstrucción de justicia, indica que el Congreso tiene la autoridad para imponer las restricciones limitadas a la conducta oficial del titular del poder ejecutivo para proteger la integridad de funciones importantes de las otras ramas del gobierno. Con lo cual, la fiscalía especial externó que no había conclusiones sobre la conducta del presidente. Y, en consecuencia, si bien el Reporte Mueller (2019) no concluyó que el presidente cometió un crimen, tampoco lo exonera de esto, con lo cuál invitó al Congreso a tomar cartas en el asunto. Acción que fue atendida por la Cámara de Representantes, y el ala democráta del mismo, para iniciar el proceso de *impeachment* contra el presidente Trump en dos ocasiones durante su mandato.

4.3 Análisis de cibercapacidades y ciberpoder de la Federación Rusa y los Estados Unidos de América

La tercera parte de nuestro análisis se centra en abordar las cibercapacidades de los Estados Unidos y Rusia, en torno a buenas prácticas internacionales de ciberseguridad, así como para realizar ciber operaciones de ofensa y defensa, a través del ciberespacio. En este apartado, serán de interés las métricas del NCSI (2019), GCI (2018), y el NCPI (2020). La finalidad de este ejercicio es valorar la evidencia presentada por el análisis de fuentes abiertas y el análisis al Informe Mueller (2019), en torno a la posibilidad del gobierno de Rusia para influir en las elecciones presidencial es de 2016. En ese sentido, es importante destacar que, hasta el momento, la capacidad operativa de Rusia para ejecutar ciber operaciones en Estados Unidos se divide en las siguientes dos vertientes:

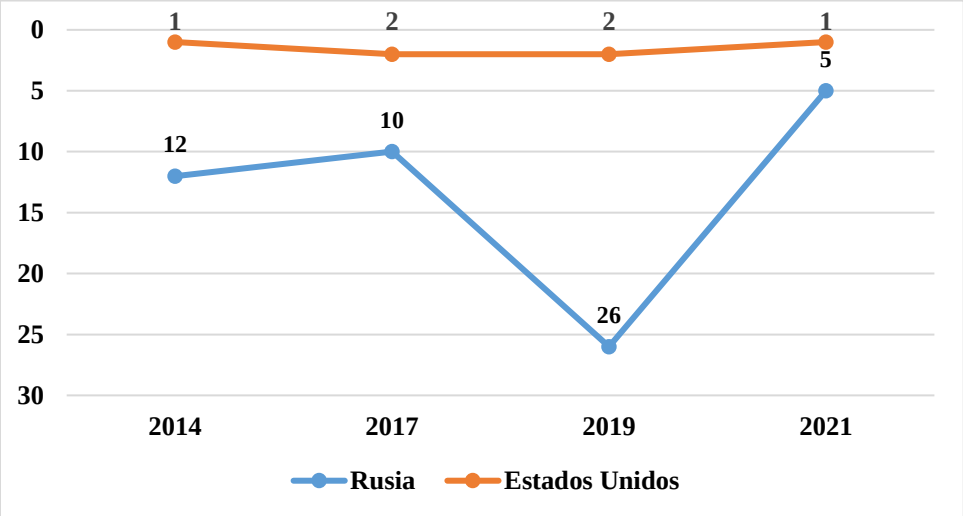
1) La capacidad e influir en la opinión pública y ciudadananía, a través de operaciones bien estructuradas que fomenten la desinformación y el incremento de los radicalismos políticos, a través de redes sociales y eventos (*rallies*) en el marco del proceso electoral de 2016, aspecto que forma parte de la trama del *Russiangate* y de la investigación del Informe Mueller (2019).
2) La capacidad de intervenir los sistemas informáticos de las empresas más importantes del país e instituciones del más alto nivel del gobierno de los Estados Unidos. Esto enmarcado en la detección del ciberataque a *SolarWinds*, a través del sistema Orion, que implica un ciber ataque con fines de ciber explotación. Es decir, con la finalidad de espiar y recopilar fuentes de información, con la finalidad de ejecutar acciones de inteligencia y contra inteligencia por parte del gobierno de Rusia en contra de los Estados Unidos, con la finalidad de alcanzar una ventaja estrátregica desde el dominio del ciberespacio.

De esta forma, en la primera sección de este apartado, abordaremos lo que presenta el análisis de cibercapacidades en torno a métricas centradas en buenas prácticas multilaterales de cibserseguridad, de índices como GCI (2019) y el NCSI (2018). Mientras, que, en segunda instancia, analizaremos el ciberpoder de cada uno de estos dos actores, planteado en el NCPI (2020), así como la estructura del cibercomando de cada uno de los dos países.

4.3.1 Global Cybersecurity Index (GCI)

Como se mencionó en el capítulo dos esta investigación, el GCI (2018) es una media promovida por la ITU, vinculada a la Agenda Global de Ciberseguridad de la ITU, la cual se ve reflejada en cinco pilares y 25 indicadores, para analizar el compromiso de los Estados-Nación con este documento. Del mismo modo, es importante, enmarcar que el GCI (2018) está abocado a fomentar la cooperación internacional de las naciones y partes interesadas (actores estatales o actores no estatales organizados) para garantizar la gobernanza y buena regulación del ciberespacio. En ese sentido, los cinco pilares del GCI (2018) vinculados a las dimensiones de *Marco Legal, Medidas Técnicas, Estructura Organizacional, Desarrollo de capacidades y Cooperación internacional*, se enmarcan en la comprensión teórica de un paradigma cercano a la visión liberalista, que buscan promover el multilateralismo internacional, en aras de promover un ciberespacio seguro para los Estados-Nación. Desde la creación de la AGC, el estudio global que presenta la ponderación GCI se ha publicado en un total de cuatro ocasiones, durante los años 2014, 2017, 2019 y 2021. En la figura 49, se obtuvo las diferentes ponderaciones que obtuvieron Estados Unidos y Rusia en los cuatro diferentes estudios.

Figura 49. Progresión de la ponderación de GCI de Rusia y Estados Unidos para el periodo (2014-2021).



Fuente: Elaboración propia con base en GCI (2014, 2017, 2019 y 2020).

La primera observación de interés, con base a las ponderaciones obtenidas por ambos países, para el periodo 2014-2021, presenta un análisis con un claro mejor posicionamiento de los Estados Unidos, con base a los cinco pilares de la AGC, lo que se puede ver en el hecho de que este país ha estado en las primeras posiciones en las cuatro ocasiones que el estudio ha sido levantado. Sobre esto, el GCI (2017) destaca que si bien para esta medición, los Estados Unidos de América, retrocedieron una posición, se destaca que el país tiene los puntajes más altos en los pilares de desarrollo de capacidades y marco legal para atención de ciberdelitos y ciber incidentes. A la par que destaca sus iniciativas de cooperación cibernética en el marco de organismos como la OTAN. Que se vio reflejado en la creación de asociaciones interinstitucionales importantes, con la firma del Acuerdo de Intercambio de Información Multilateral (MISA) que comprometió a los departamentos de defensa, salud, justicia, energía y la comunidad de inteligencia, a trabajar e intercambiar información de seguridad cibernética con sus socios atlánticos. Con lo cual, este país afianzó mecanismos de cooperación internacional en el marco de esta alianza militar.

Por su parte, el GCI (2019) destaca que si bien, nuevamente Estados Unidos, se ubica en la segunda posición, el país tiene el primer lugar, con el puntaje más alto, nuevamente en el pilar de marco legal, a razón de su amplia gama lesgislaciones y códigos para la procuración de justicia frente a ciber delitos. A la par, que la nación es utilizada como referencia para analizar a los 25 países de la región de Asia-Pacífico, que son incluidos en dicha edición del estudio. Derivado de que su ENCS y las políticas gubernamentales y estructuras legislativas de ciberseguridad de Estados Unidos, representan un modelo óptimo de madurez cibernética para evaluar las diversas facetas en que se encuentran las naciones asiaticas. Por último, el GCI (2020) destaca que el regresó de Estados Unidos a la posición número 1, se vincula al reforzamiento de sus legislaciones nacionales, frente a fenómenos de desinformación y polarización social, y el reforzamiento de su ENCS de 2020.

En contraposición, para el caso de la Rusia, destaca que este país inició en la posición doce del GCI (2014), y subió dos posiciones en la siguiente medición. Para después retroceder abrupatamente en el GCI (2019) hasta la posición número veintiseis. Sin embargo, para el GCI (2021) la nación da un repunte de 21 posiciones hasta consolidarse en el lugar número cinco, solo cuatro lugares por detrás de Estados Unidos. En este contexto, el GCI (2017)

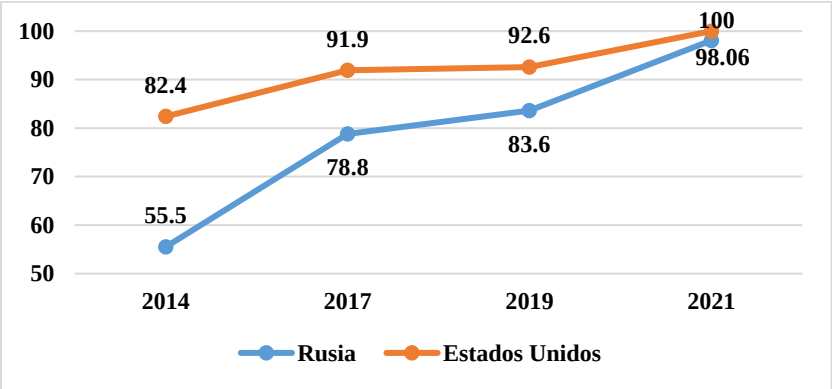
expresa que Rusia, ocupó el segundo lugar en la región euroasíatica, sólo por detrás de Estonia, y avanzó dos posiciones en el ranking global, a razón de que obtuvo la mejor puntuación en la dimensión de desarrollo de capacidades.

Esto como resultado de su compromiso con desarrollo de estándares de ciberseguridad a nivel nacional, hasta la promoción de una conciencia pública de su industria nacional de ciberseguridad, con empresas representativas a nivel internacional como Kaspersky Labs, con los pilares de la AGC. Por otra parte, se destaca la aplicación de una doctrina de defensa de ciberseguridad, introducida en su Estrategia de Seguridad Nacional, del año 2000, que es utilizada de manera concreta en el desarrollo de sus diplomacia y relaciones exteriores.

No obstante, la caída en 16 posiciones que presenta el GCI (2019), indica que se debe a que Rusia obtuvo un amplio retroceso en la dimensión de cooperación internacional. Lo que puede estar asociado al auge de la difusión en la prensa internacional de sus supuestas ciberoperaciones, con especial énfasis a su intervención en el proceso electoral de Estados Unidos y los resultados de la investigación del Informe Mueller. De hecho, esta edición, la nación fue superado por Uzbekistán, en este pilar. Sin embargo, el informe destaca que el país obtuvo el puntaje más alto de la región euroasíatica, con importantes mejoras en el pilar de marco legal. A razón de la creación de una legislación para mejorar la regulación para la prevención y gestión del fraude en el uso de sistemas de pago electrónico.

En este sentido, es importante destacar que las cuatro ediciones del GCI permiten observa que Rusia ha sido una nación que mejora de forma constante y progresiva, con base a sus compromisos con AGC, al pasar de una ponderación de 55.5, de un total de 100 puntos, en 2014, hasta una calificación de 98.06 en 2020. Y si bien Estados Unidos, también ha presentado mejora constante, la evolución de su adversario muestra un avance más importante que por la potencia americana, como se puede observar en la figura 50.

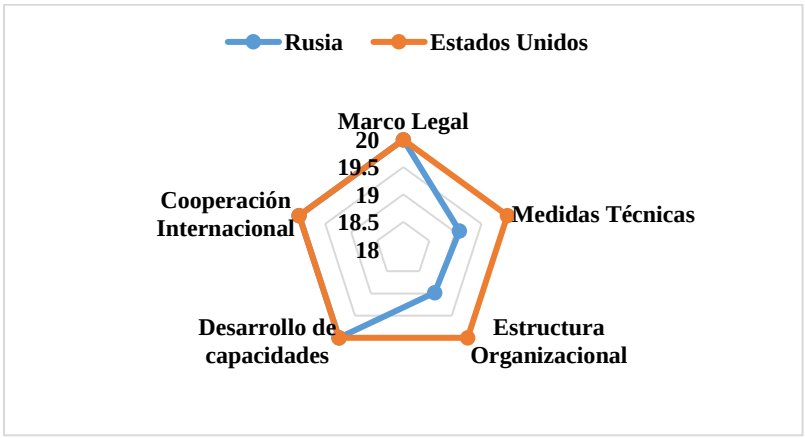
Figura 50. Progresión de ponderación global de Rusia y Estados Unidos GCI 2014-2021.



Fuente: Elaboración propia con base GCI (2014:2021).

Por último, el GCI (2021) no presenta una explicación más amplia de su repunte en 21 posiciones en el ranking global, sino que solamente indica que esto se debe a su mejora en los pilares de marco legal, cooperación internacional y desarrollo de capacidades. En este punto, es importante mencionar que una particularidad que presenta el GCI (2020), es que permite ver en cada uno de los cinco pilares, el comparativo de las diferencias que existen entre Estados Unidos (con ponderación de 100 puntos de un total de 100) y Rusia (con ponderación 98.06 puntos, de un total de cien. Lo cuál se presenta en la figura 51 que demuestra que para esta medición, Rusia sólo presentó un pequeño rezago respecto a Estados Unidos en la dimensiones de medidas técnicas y estructura organizacional.

Figura 51. Comparativo entre Estados Unidos y Rusia en los cinco pilares del GCI (2020).

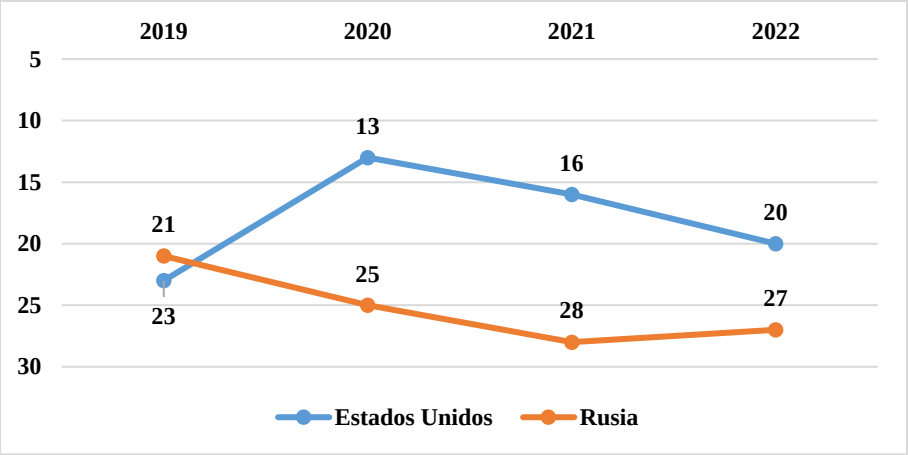


Fuente: Elaboración propia con base en GCI (2020).

4.3.2 National Cybersecurity Index (NCSI)

Como se indicó, de igual forma, en el capítulo dos esta investigación, el NCSI (2018) es un instrumento que mide las capacidades de resiliencia, y en forma discreta, de disuasión de los Estados-Nación a través de un total de 12 indicadores que son *política, amenazas, educación, aportación global, nivel de desarrollo digital, protección de servicios esenciales, identificación electrónica y confidencialidad de servicios, protección de datos personales, respuesta a ciber incidentes, administración de ciber crisis, política de lucha contra el crimen y capacidad de operaciones militares.* Es importante destacar que la versión más reciente del NSCI (2022), presenta la progresión de ambos países, en el ranking global para el periodo 2019-2022. En ese sentido, en la figura 52 puede observarse estos cambios, dónde se observa que entre los años 2019 y 2022 Rusia pasó de la posición 21 a la 27. Mientras que Estados Unidos avanzó 3 lugares en el mismo periodo.

Figura 52. Progresión de ponderación global de Rusia y Estados Unidos NSCI 2019-2022.



Fuente: Elaboración propia con base NCSI (2022).

Sin embargo, es importante destacar que el NCSI (2018) sólo ha publicado una edición en forma de informe con los resultados del conjunto de países que son analizados. Pero, dentro de la plataforma de internet de la medición, se encuenta un total de cuatro levantamientos en los que se ha realizado y actualizado la información de este, hasta el año 2022. Para analizar, esto, el NCSI (2022) divide al total de indicadores en tres diferentes grupos, que son:

- *Indicadores Generales de Ciberseguridad:* Desarrollo de Política, Delimitación de Amenazas, Desarrollo de Educación y Contribución Global.

- *Indicadores línea de base de ciberseguridad:* Protección de Servicios Digitales, Protección de Servicios Esenciales, Identificación E y confiabilidad de servicios y Protección Personal de datos.
- *Indicadores de Manejo admisitración de crisis e incidentes:* Desarrollo de CIRC, Administración de Crisis, Política contra Cibercrimen y Operaciones Militares en el ciberespacio.

En ese sentido en la tabla 33, se presenta el total los resultados de las actualizaciones realizadas a Rusia y Estados Unidos en esta métrica. Observando los datos de esta, se encontró que la información referente al levantamiento del 19/07/2017, presenta varias inconsistencias, vinculadas al hecho de que se asignan en múltiples indicadores calificaciones de cero a ambos países. Esta condición cambia a partir del segundo levantamiento, que corresponde al año de la publicación del informe del NCSI (2018). Por esta razón la primera asignación, corresponde más ausencia de información, que a una descripción real de las cibercapacidades de los países en dicho periodo. Por lo cuál los cambios significativos, se empiezan a considerar desde la tercera actualización y se señalan en rojo.

Tabla 33. Progresión de Rusia y Estados Unidos en los indicadores del NCSI (2012).

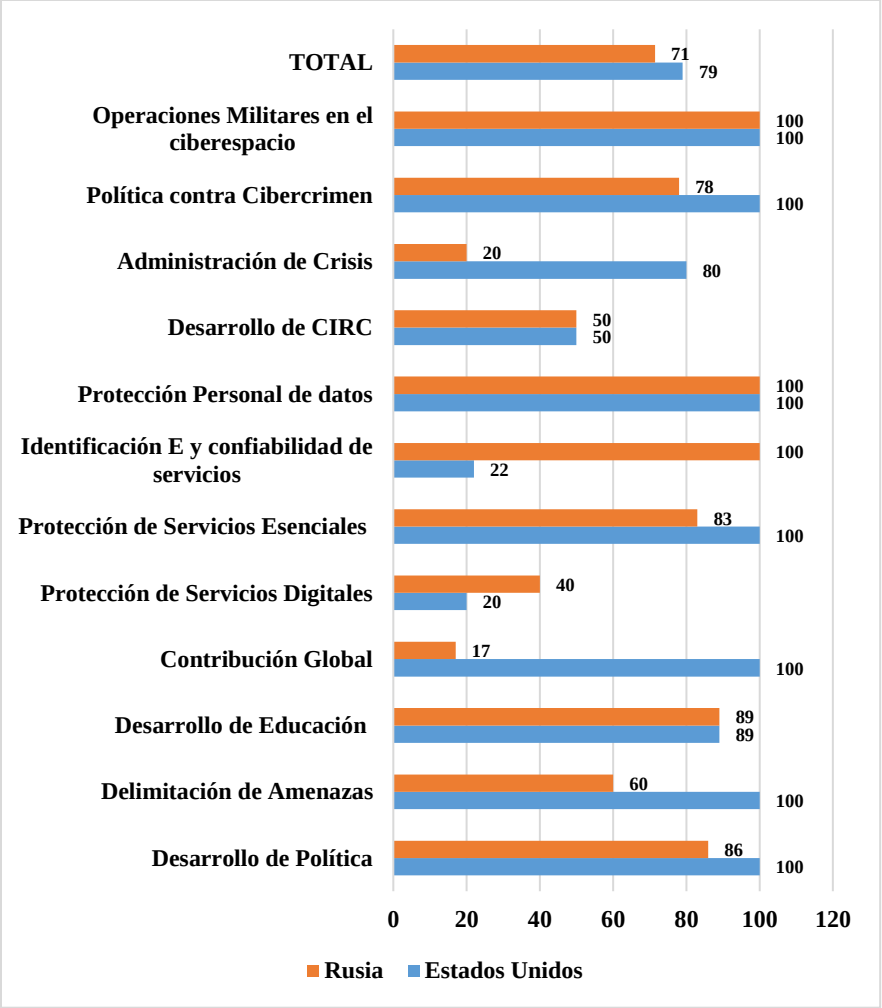
		19/07/2017	09/05/2018	26/10/2018	23/11/2021
Rusia	**Indicadores Generales de Ciberseguridad**				
	Desarrollo de Política	14	86	86	86
	Delimitación de Amenazas	60	60	60	60
	Desarrollo de Educación	67	89	89	89
	Contribución Global	17	17	17	17
	Indicadores línea de base de ciberseguridad				
	Protección de Servicios Digitales	0	40	40	40
	Protección de Servicios Esenciales	0	67	67	83
	Identificación E y confiabilidad de servicios	78	89	89	100
	Protección Personal de datos	100	100	100	100
	Indicadores de Manejo admisitración de crisis e incidentes				
	Desarrollo de CIRC	50	50	50	50
	Administración de Crisis	0	0	20	20
	Política contra Cibercrimen	78	78	78	78
	Operaciones Militares en el ciberespacio	0	50	50	100
Estados Unidos	**Indicadores Generales de Cberseguridad**				
	Desarrollo de Política	14	86	86	86
	Delimitación de Amenazas	60	60	60	60

	Desarrollo de Educación	67	89	89	89
	Contribución Global	17	17	17	17
	Indicadores línea de base de ciberseguridad				
	Protección de Servicios Digitales	0	40	40	40
	Protección de Servicios Esenciales	0	67	67	83
	Identificación E y confiabilidad de servicios	78	89	89	100
	Protección Personal de datos	100	100	100	100
	Indicadores de Manejo admisitración de crisis e incidentes				
	Desarrollo de CIRC	50	50	50	50
	Administración de Crisis	0	0	20	20
	Política contra Cibercrimen	78	78	78	78
	Operaciones Militares en el ciberespacio	0	50	50	100

Fuente: Elaboración propia con base NCSI (2022).

Derivado de este análisis, se identificó que, para el caso concreto de los países de interés, la principal progresión de Rusia se dio en los indicadores de *Protección de Servicios Esenciales*, al pasar de un puntaje de 67 a 83 puntos, *Administración de Crisis*, al pasar de 0 a 20, y *Operaciones Militares en el ciberespacio,* al pasar de 50 a 100. Mientras que Estados Unidos, avanzó en las dimensiones de *Identificación E y confiabilidad de servicios*, al pasar de 89 a 100 puntos, y en *Operaciones Militares en el ciberespacio,* al pasar de 50 a 100 puntos. Con lo cuál, de forma semejante al GCI, para el periodo 2014-2021, Rusia ha demostrado un crecimiento más acelerado en su desarrollo de cibercapacidades en esta métrica. En ese sentido, de forma similar al GCI (2021), se utilizó la actualización más reciente del NCSI (2022), para hacer un comparativo entre en ambos países que se presenta en la figura 53, en él se puede observarse que Estados Unidos supera a Rusia con base a la métrica del NCSI (2022), con una ponderación de 79 contra 71 puntos. Con base la medición, destaca que la nación euroasiática supera a su oponente en dos dimensiones, la de protección de servicios digitales (con una ponderación de 40 puntos contra 20) e identificación electrónica y confiablidad de servicios (100 contra 22 puntos). Mientras que Estados Unidos sobrepasa a Rusia en las dimensiones de administración de crisis (80 puntos contra 20), política de cibercrimen (100 puntos contra 78), protección de servicios esencial (100 puntos contra 83), contribución global (100 puntos contra 17) delimitación de amenazas (100 puntos contra 60) y desarrollo de política (100 puntos contra 78). Un aspecto de trascendencia es el indicar que de para el NCSI (2022), Rusia está muy mal evaluado en la dimensión de contribución global y administración de crisis, con lo cual, según esta métrica, el país tiene pocas capacidades de resiliencia frente a un ciberataque.

Figura 53. Desarrollo de ciber capacidades según en NCSI (2019) de Rusia y Estados Unidos.



Fuente: Elaboración propia con base NCSI (2022).

4.3.3 National Cyber Power Index (NCPI)

Cómo se indicó en el capítulo 3 de esta investigación, el NCPI (2020) esta centrado en presentar un análisis en torno al ciberpoder que poseen un total de treinta países del mundo, con base a siete objetivos vinculados a la seguridad nacional y la política exterior. El NCPI resalta por encima del GCI y el NCSI, a razón de que profundiza en las capacidades de defensa y ofensa de los países, con el fin de ser una medida de ciberpoder y potencial comprobado de los Estados-Nación para atacar a otra nación, o protegerse de una agresión de frente a un ciberataque.

En este punto, es importante destacar que el NCPI (2020) se engloba en una tradición más neorrealista, al considera al ciber poder como la capacidad efectiva de utilizar el ciberespacio para alcanzar objetivos nacionales. A la par de que ha expresado que considera como potencias del ciberespacio a un total de cinco países, que son Estados Unidos, China, Reino Unido, Rusia e Israel. En este sentido, de una ponderación que va del 0 al 100 en la tabla 34 se presenta la ponderación que asigna el NCPI (2020) a estos cinco países.

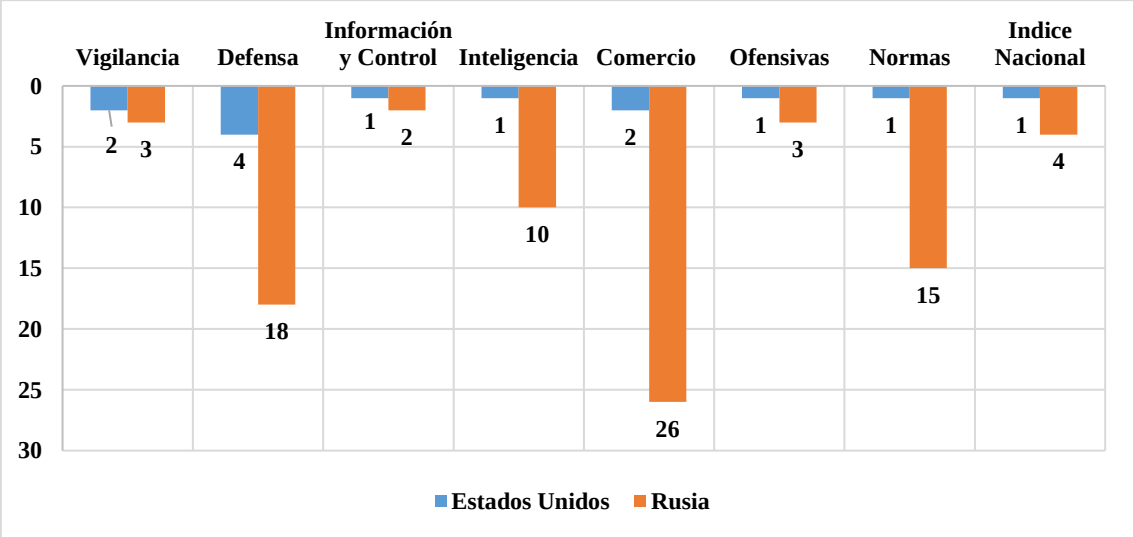
Tabla 34. Ponderación del a las 5 potencias del ciberespacio según el NCPI (2020).

No.	País	Ponderación
1	Estados Unidos	50
2	China	42
3	Reino Unido	36
4	Rusia	24
5	Israel	15

Fuente Elaboración propia con base NCPI (2020).

Al realizar un comparativo entre Estados Unidos y Rusia, se observa un mejor posicionamiento del primero en las ocho dimensiones que contempla la métrica. Con lo cuál se indica que esta nación tiene el ciberpoder más completo, con base a la metodología del NCPI (2020). Mientras se presenta que Rusia se posiciona mejores dimensiones de vigilancia, información y control y ofensiva. Como puede observarse en la figura 54.

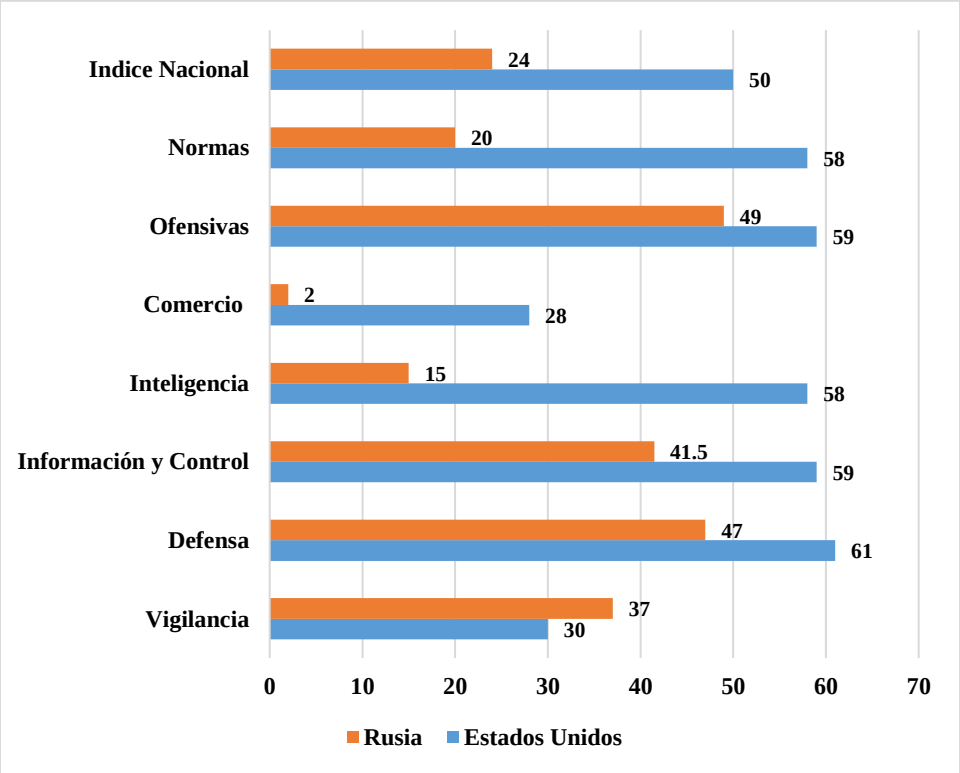
Figura 54. Ranking de Rusia y Estados Unidos en las 8 dimensiones del NCPI (2020).



Fuente NCPI (2020).

Por otra parte, cuándo se analiza la ponderación que asigna el NCPI (2020) a ambas naciones en las ocho dimensiones. Se encuentra que la métrica expresa que Estados Unidos prácticamente duplica con su calificación el ciber poder de Rusia. Y se encuentra mejor posicionado que este país, en un total de siete dimensiones. Sólo en la dimensión de vigilancia, Rusia logra superar a Estados Unidos (con un total de 37 puntos contra 30) como puede observarse en la Figura 55.

Figura 55. Ponderación de Rusia y Estados Unidos en las 8 dimensiones del NCPI (2020).



Fuente: Elaboración propia con base al NCPI (2020).

Un aspecto fundamental para resaltar en los resultados del NCPI (2020), es el hecho de que presenta altas ponderaciones para Rusia en las dimensiones de capacidad efectiva de ofensiva (49 puntos de un total de 100) y defensa (47 puntos de 100). Con lo cuál no subestima las capacidades para ejecutar ciber operaciones por este país. Sin embargo, un aspecto fundamental y crucial, al momento de la publicación de este informe, que se enmarca en esta investigación es el hecho de que, durante 2020, aún no se conocían los alcances reales del ciberataque de SolarWinds, con lo cuál, de existir una nueva edición de este reporte, se augura una progresión e incrementó en la comprensión del ciberpoder de Rusia.

4.3.4 Estructura de los ciber operaciones y ciber comandos de Rusia y Estados Unidos

Del mismo modo, el NCPI (2020) destaca que tanto Rusia como Estados Unidos, poseen las mejores estructuras de ciberoperaciones y cibercomandos del mundo, en la figura 56 se presenta la estructura del cibercomando de los Estados Unidos con base a información del US Cyber Command (2022).

Figura 56. Estructura del cibercomando de Estados Unidos.

Fuente: Elaboración propia con base en US Cyber Command (2022).

En la figura 56 se puede observar que la estructura tiene como ejes centrales al Departamento de Defensa (DD) y al Director Nacional de Inteligencia (DNI). El DD se vincula principalmente con instituciones de las Fuerzas Armadas y avocadas a la Seguridad Nacional, la cuál divide sus operaciones en tres diferentes ejes. El primero compone la estructura de la NSA, y la Dirección de Inteligencia de Señales (*Signal Intelligence Directorate* o SID por sus siglas en inglés), quienes colaboran estrechamente con la empresa privada *Sirius Sigint Solutions*. En conjunto estos tres actores conforman la Sección 3 (S3), cuyo objetivo es ejecutar ciber operaciones las cuales son denominadas *Tailored Access Operations* u Operaciones de acceso a la medida. Esta unidad cibernética es denominada bajo diferentes alías como *Platinum*, *Longhorm*, o *Unit8200* y divide sus operaciones en seis diferentes unidades, que son: i) *Requerimientos y Objetivos*, ii) *Centro de operaciones remotas,* iii) *Tecnología de data network,* iv) *Red de Telecomunicaciones,* v) *Tecnología de acceso de operaciones,* vi) *Infraestructura de la misión.*

El segundo eje está integrado por el Comando de Operaciones Especiales (*Special Operations Command* o SOCOM por sus siglas en inglés), el Comando Conjunto de Operaciones Especiales (*Joint Special Operations Command* o JSOC) y la unidad Actividad de Apoyo de Inteligencia (*Intelligence Support Activity* o ISA por sus siglas en inglés). En conjunto estas tres unidades están centradas en recolectar información para inteligencia para las operaciones militares. Por último, el último eje está vinculado al Comando Cibernético de los Estados Unidos (*US Cyber Command),* que es el encargado de atender los ataques de Día Zero provenientes de APTs extranjeras.

Respecto a la estructura del Directorio Nacional de Inteligencia, este se divide en dos ejes. El primero está integrado por la CIA y el Directorio para la Innovación Digital (*Directorate for Digital Innovation* o DDI por sus siglas en inglés), que en conjunto conforman el Centro para la Ciber Inteligencia (*Center For Cyber Intelligence* o CCI por sus siglas en inglés). EL CCI se subvide en tres diferentes grupos que son: i) *Operaciones de Computo*, ii) *Ingenieros de Desarrollo*, y iii) *Grupos de Acceso Físico*, quienes se encargan del análisis de inteligencia de los ciberataques de Día Zero en los sistemas informáticos públicos y privados de los Estados Unidos.

Mientas que el segundo eje se confortma por el FBI, la Rama de Ciencia y Tecnología (*Science and Technology Branch* o STB por sus siglas en inglés), y la Dirección de Tecnología Operativa (*Operational Technology Division* o OTD por sus siglas en inglés), las cuales conforman la Unidad de Operaciones Remotas (*Remote Operations Unit* o ROU por sus siglas en inglés), cuyo objetivo es brindar capacidades de computo para explotación de redes en dispositivos móviles como *Smartphones, laptops* o PCs.

El Ciber Comando de la Federación Rusa presenta una estructura más compleja que la estadounidense, el cual está liderado por cuatro actores estratégicos: i) el Ministerio de Defensa, ii) el Presidente de la Federación Rusa, iii) el Servicio Federal de Seguridad y iv) el Servicio de Inteligencia Exterior. En el caso de la estructura liderada por el Ministerio de Defensa se indica que este opera en conjunto con otros tres actores que son el Estado Mayor de las Fuerzas Armadas Rusas, el Directorio Principal del Estado Mayor de las Fuerzas Armadas Rusas, y la Unidad de Inteligencia Electrónica y Señales. En conjunto, estas cuatro instancias supervisan el trabajo de cuatro unidades encargadas de ejecutar acciones clave para las ciberoperaciones, que son:

i. *Unidad 74455 o Centro Principal de Tecnologías*, cuyo objetivo es recopilación de información para inteligencia militar rusa
ii. *Unidad 29155 o Centro de formación de especialistas para fines especiales*, cuyo objetivo se centra en ejecutar operaciones para desestabilizar países europeos.
iii. *Unidad 54777 o 72° Centro de Servicios Especiales*, que es un centro primario de GRU y cuyo objetivo se aplica a aplicar estrategias de desinfomración o de guerra psicológica.
iv. *Unidad 26165 85° Principal Centro de Servicios Especiales*, cuyo objetivo está centrado en ejecutar operaciones de inteligencia militar, operaciones de ciber criptografía y coordinar grupos de hackeo.

En conjunto, estas cuatro unidades, suelen operar como un APT denominado con el nombre de *Sadworm*, o bajo los alias de *Telebots, Voodoo, Bear* o *Iron Viking*. Del mismo modo, es importante destacar que en el marco de nuestro análisis del Informe Mueller (2019) se indica que la Unidad 54777 y la Unidad 26165, se considera estuvieron involucradas en las

ciberoperaciones a través de redes sociales para polarizas a la sociedad estadounidense en el marco de las elecciones presidenciales de de 2016.

Respecto al segundo eje, destaca el involucramiento directo en las ciberoperaciones del presidente de la Federación Rusa, quien está en estrecha coordinación con el Servicio de Protección Federal (SFP) y el Servicio Especial de Comunicaciones de Rusia (SECR).Estos tres actores están encargados de coordinar y supervisar el desempeño de las ciber operaciones que ejecutan los equipos cibernéticos o APTs más famosos de Rusia, que son:

i. APT 28 o también conocida bajo el alias de *STRONTIUM*,
ii. APT 29 o Coze Bear, también conocida bajo los alias de *CozyCary, The Dukes* o *GozyDuke,* y finalmente,
iii. Energetic Bear conocida bajos los alias de *DragonFly, Koala Team, Iron Liberty, Crouching Yeti* y *Group 24.*

En este sentido, es importante destacar que con base al informe de RiskIQ Inc, de junio de 2020, señalado en la revisión de fuentes abiertas, CozyBear o APT 29 estuvieron involucrados en la cibero operación que vulneró la seguridad cibernética de SolarWinds y el sistema *Orion.* Del mismo modo, que destaca el involucramiento directo de la máxima instancia de autoridad del gobierno ruso, el presidente, en la coordinación y supervisión de estas operaciones.

En relación con el tercer eje de las ciberoperaciones rusas, se destaca que esté está liderado por el Servicio Federal de Seguridad (SFS), en coordinación con el Servicio de Contra Inteligencia (SCI) y el Departamento de Seguridad de Cómputo y de Información (SCI), y su acción está más avocada a recopilación de inteligencia para la seguridad interna y combatir fenómenos como el terrorismo. Para esto el equipo cuenta con dos unidades de acción:

i. *Unidad 64829 18° Centro de seguridad de la información*, que tiene como función ejecutar la interceptación legal de telecomunicaciones y redes telefónicas que operan en Rusia (denonimado bajo el acronimo SORM), así como realizar acciones de busqueda y vigilancia de objetivos de peligro a la seguridad interna.
ii. *Unidad 71330 Centro 16°*, cuyo objetivo: se centra en operar las instalaciones de inteligencia de señales o centros de recepción de información en Rusia.

En el último eje se destaca el liderazgo del Servicio de Inteligencia Exterior, con objetivo de coordinar servicios de inteligencia externa enfocado principalmente en asuntos civiles. Se especula, esta institución coordina un total de nueve directorados, sobre los cuales se tiene noción de su objetivo, mientras que de otros no se tiene certeza de sus funciones, estos son:

i. *Directorado PR.* Objetivo: Inteligencia política.
ii. *Directorado S.* Objetivo: Inteligencia Ilegal
iii. *Directorado X*. Objetivo: Inteligencia Técnica y Científica
iv. *Directorado OT.* Sin conocimiento de su función.
v. *Directorado R.* Objetivo: Planeación de operaciones y análisis
vi. *Directorado I.* Sin conocimiento de su función.
vii. *Directorado Económico.* Objetivo: Inteligencia Económica
viii. *Directorado KR Contra inteligencia Externa*. Objetivo: Infiltraciones en inteligencias extranjeras.,
ix. *Centro de Ciber operaciones COC*. Objetivo: ejecutas y coordinar operaciones en objetivos extranjeros. Sobre este último, destaca que esta en estrecha colaboración con las APTs o equipos de ejecución de ciberoperaciones de Rusia.

La estructura compleja del Ciber Comando de Rusia, permite deducir que esta nación posee las capacidades efectivas de vulnerar la soberanía nacional de los Estados Unidos, en los dos esquemas de operación presentados:

1. Por su capacidad de influir en la opinión pública y ciudadananía, a través de operaciones bien estructuradas con base a la trama del Russiangate y de la investigación del Informe Mueller (2019), y;
2. Por su capacidad de intervenir los sistemas informáticos de empresas más importantes e instituciones del más alto nivel del gobierno de los Estados Unidos, con, la detección del ciberataque a SolarWinds, a través del sistema Orion, que implica un ciber ataque con fines de ciber explotación, con base a nuestra revisión de fuentes abiertas.

Por último en la figura 57 se presenta la posible estructura del Ciber Comando de la Federación con base a información del CCD COE Tallin de un estudio de Hakala y Melnychuk (2021) y Jasper (2020).

Figura 57. Estructura del Ciber Comando de Rusia.

Fuente: Elaboración propia con base en CCD COE Tallin (2021) y Jasper (2020).

4.4 Entrevistas a especialistas sobre materia de ciber poder

La última parte de nuestro análisis de estudio de caso correspondió a la realización de un total de diez entrevistas con especialistas en ciberseguridad del ámbito de las Américas, y la realización de un análisis de teoría fundamentada de los comentarios estratégicos obtenidos en cada conversatorio, con el fin de generar un análisis sobre la viabilidad de la intromisión de Rusia en las elecciones de Estados Unidos de 2016. Y si está puede ser considerado una violación a la soberanía nacional y la consolidación del dominio del ciberespacio para realizar esta acción. Para esto, se procedió a realizar una *Guía de entrevista semiestructurada* que puede observarse en el Anexo 1 de esta investigación de tesis.

Del mismo modo, se indica que la entrevistas se realizaron entre el 25 de mayo de mayo y el 28 de septiembre de 2021. La lista completa de los expertos que fueron entrevistados se puede observar en la tabla 34, con su nombre completo, país de origen o radicación, así como su adscripción.

Tabla 34. Datos de los diez expertos en materia de ciberseguridad entrevistados.

No.	Nombre del entrevistado	País	Adscripción	Fecha de entrevista
1	Edgardo Glavinich	Argentina	Universidad de la Plata, Argetina.	25 de mayo de 2021
2	Carolina Sancho Hirane	Chile	Instituto de Estudios Internacionales de la Universidad de Chile	01 de julio de 2021
3	Aristides Contreras	Colombia	Comunidad Internacional en Gestion de Riesgos y Seguridad (COLADCA).	10 de julio de 2021
4	Breno Pauli Medeiros	Brasil	Colegio de la Defensa de Brasil	12 de julio de 2021
5	Ricardo Magno Texeira	Brasil	Policia Federal del Brasil	15 de julio de 2021
6	María Luisa Parraguez	México	Tecnologico de Monterrey.	01 de agosto de 2021.
7	Boris Saavedra	Estados Unidos	Centro de Estudios Hemifericos William J. Perry, de la Universidad de la Defensa de los Estados Unidos.	15 de agosto de 2021.
8	Mariano Bartolomé	Estados Unidos / Argentina	Colegio Interamericano de Defensa	01 de septiembre de 2021
9	Sandra Palma	Honduras	Unidad de Transparencia y Acceso a la Información Pública de Honduras	14 de septiembre de 2021
10	Gianncarlo Delgado	Perú	Centro de Altos Estudios Nacionales del Perú.	28 de septiembre de 2021

Fuente: Elaboración propia.

La estructura de la entrevista estuvo centrada en los siguientes cinco ejes de discusión, para probar la hipótesis de esta investigación, que son:

- Amenazas e impactos que puedan afectar la Seguridad Nacional desde el ciberespacio
- Ciberpoder y Ciber resiliencia
- Soberanía y ciberespacio
- Filtraciones a la información
- Ciberespacio y procesos políticos

Una vez realizadas las entrevistas, se procedió a transcribirlas y sistematizar la información de estas. A continuación, se presentan los principales hallazgos, con base a los resultados por cada uno de los ejes temáticos.

4.4.1 Amenazas e impactos que puedan afectar la Seguridad Nacional

En el ámbito de la comprensión de las amenezas a la Seguridad Nacional, es importante mencionar que hubo un consenso entre los entrevistados en considerar a la Declaración sobre Seguridad de las Américas (DSA), de la Organización de los Estados Americanos, como un referente que puede enmarcar al ciberespacio como un nuevo dominio de securitización. De acuerdo con los comentarios de Sancho (2021), este documento, representa una base y materialización de los conceptos de escuela crítica y ampliacionista de la seguridad nacional de Buzan, Wever y De Wilde, (1998). La trascendencia de este documento oscila en el hecho de enmarcar a los ciberataques como amenazas de carácter semejante a fenómenos como el terrorismo, la delincuencia organizada, la corrupción o el lavado de dinero, etc.

No obstante, de esta condición, los comentarios de Bartolomé (2020) indican que, si bien la DSA (2003) ha sido una guía para presentar el panorama de las nuevas amenazas a la seguridad nacional, los Estados-Nación, deben tomar acciones estrategicas en torno a la edificación de una política de seguridad nacional que cree mecanismos de prevención de vulnerabilidad de los países (Bartolomé, 2013). En ese sentido, si las naciones no identifican los riesgos y amenazas del ciberespacio, desde su comprensión intersubjetiva de la seguridad nacional, estarán imposibilitados de crear mecanismos para contener amenazas y vulnerabilidades en este dominio. En adicción a estos comentarios, Sancho (2011) indicó que en las naciones de América Latina existen problemas de discusión semántica para definir los

problemas y las amenazas a la seguridad nacional, aunque intenten adherirse a la declaración de la OEA. Pero a pesar de las diferencias de pensamiento, a nivel regional se coincide que los ciberataques son un tipo de fenómeno que pueden afectar la seguridad de un país (Sancho, 2017).

Del mismo modo, Bartolomé (2021) destaca que el ciberespacio sirve como medio para reinventar la delimitación de las amenazas de seguridad nacional, provienentes de la época de la Guerra Fría. Sin embargo, con excepción de Estados Unidos y Canadá, en América Latina es complicado hacer una valoración de amenazas a la seguridad nacional dado que es una zona de paz si se estudia bajo el paradigma tradicional de seguridad nacional (Bartolomé, 2006). A la par que la situación se complica en el ámbito de la ciberseguridad, porque los agresores o atacantes puede ser agentes no estatales, como lo son la criminalidad, terrorismo y grupos privados. De esta forma, el ciberespacio es un campo en donde se manifiestan y consuman las nuevas amenazas vinculadas a estos actores. En este sentido, en el ámbito de la ciberseguridad, las infraestructuras críticas nacionales, adquieren particular relevancia, ya que de ellas depende el funcionamiento normal de las sociedades y son el punto máximo de una amenaza, que, a través de un ciberataque, puede impactar en la seguridad nacional, esta visión se complemente con los comentarios de Kello (2013), Klimburg (2013) y Hughes (2010).

En este punto Glavinich (2021) enfatizó que las infraestructuras críticas de las naciones están interconectadas con el bienestar de la sociedad y en el ámbito de las relaciones y política exterior de los países. De esta forma, las infraestructuras críticas se deben de proteger como prioridad del enfoque de la ciberseguridad con perspectiva de seguridad nacional. Este componente, se complemento por lo citado por Contreras (2021) al especificar que son precisamente los ciberataques a insfraestructuras criticas nacionales los más trascedentales para la seguridad nacional, a razón que sus efectos están fuertemente relacionados con el espacio físico, con lo cuál destaco que en el *Global Risk 2020* el Foro Económico Mundial, estableció a los los ciberataques como la principal amenaza global. En el marco de esta problemática Parraguez (2021), destacó que Estados Unidos destaca a nivel global y en las Américas, por ser un país que tiene identificadas y enlistadas 16 áreas de infraestructura crítica nacional, entre las cuales se destacan aeropuertos, puertos, suministros de agua, e

incluso su sistema electoral. La visión estrategia se acopla a los comentarios en torno al ciber poder de Nye (2010) y Kello (2012). Por último, se vierten comentarios derivados de las entrevistas considerados estrátegicos en el marco de este topico.

Tabla 35. Comentarios estratégicos del eje de discusión amenazas e impactos que puedan afectar la Seguridad Nacional.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Carolina Sancho Hirane	▪ Las problemáticas de un país no se remiten a una demarcación territorial nacional, se debe de tener una visión compartida dado que una misma vulneración puede afectar a dos o más naciones de manera simultánea. Es decir, la interconexión que existe entre Estados puede significar vulneración en la seguridad nacional de cada uno. ▪ El ciberespacio puede ser un ambiente en donde otras situaciones puedan verse afectadas. Por ejemplo, las armas de destrucción masiva que son controladas por sistemas informáticos, mismos que pueden ser dañados teniendo como consecuencia que se activen dichas armas. Por tanto, en el ciberespacio se pueden desarrollar actividades que afecten de manera explícita o indirecta a la seguridad de los Estados.
2	Aristides Contreras	▪ El espacio cibernético se ha vuelto un espacio de oportunidad para grupos delictivos, que utilizan la plataforma para consumar amenazas a la seguridad nacional.
3	Breno Pauli Medeiros	▪ Un ciberataque es un intento de un Estado-Nación de entrar a la infraestructura crítica y de información de otro Estado. Esta violación de información puede tener efectos en esferas físicas y causar una afectación a la soberanía y estabilidad de la nación.
4	Mariano Bartolomé	▪ Las nuevas concepciones de seguridad valoran tanto amenazas internas como externas; además, no solo involucra a los militares, si no que también se incluyen a otras esferas del Estado, así como a la esfera privada. ▪ Las vulnerabilidades de las infraestructuras críticas nacionales representan el mayor nivel de vulneración a la seguridad nacional de los Estados-Nación, por las repercusiones e impacto que tienen en la vida de las personas. ▪ Las amenazas contemporáneas acentúan mucho la necesidad de generar una mayor cooperación interestatal entre estados, dado que los nuevos

No.	Nombre del entrevistado	Comentarios estrátegicos:
		riesgos tienen una naturaleza transnacional. Esto aplica a los ciberataques y sus efectos que pueden afectar a gran cantidad de Estados-Nación.
5	Gianncarlo Delgado	▪ Es una problemática que cerca del 80% de la infraestructura crítica regional esté privatizada. Se destaca que los ciudadanos tienen mayor sensación de seguridad con el sector privado, que con el sector público en lo que se refiere al manejo de la información. Hecho que también representa una problemática.

Fuente: Elaboración propia.

4.4.2 Ciberpoder y Ciber resiliencia

En el análisis vinculado al concepto de ciberpoder, destacaron las definiciones presentadas por Bartolome (2021), al expresar que este representa la habilidad de tener resultados deseados para los Estados-Nación, mediante la utilización de herramientas cibernéticas. Estas definiciones conceptuales son cercanas al concepto de Sheldon (2012) y Kuehl (2009). En complementación Contreras (2021) indicó que el ciberpoder estaba igualmente relacionado con el nivel de madurez que tiene el marco jurídico y reglamentario en lo referente a la seguridad cibernética de una nación, a la par que entre los elementos de ciberpoder pueden incluirse aspectos como: 1) el nivel de madurez en el marco jurídico nacional, 2) modelos de seguridad y de privacidad de la información, 3) política de ciberseguridad y ciberdefensa, y 4) política de seguridad digital que evoluciona a una política nacional de confianza. En este sentido, el reflejo del ciberpoder es un Estado-Nación, está estrechamente relación con la consolidación de sus cibercapacidades. Esto vincula a métricas internacionales como el GCI (2021), NCSI (2018) en NCPI (2020).

Sumado al desarrollo de ciberpoder, vinculado a la cibercapacidades, Saavedra (2021) indicó que la construcción del poder en el ciberespacio se ha cimentado en el dominio de la información, no únicamente en la fuerza militar o política. Lo cual ha tenido como resultado que las grandes potencias concentren sus esfuerzos en el desarrollo de nuevas tecnologías como lo son el 5G, el Big Data, la Computación Cuántica y la Inteligencia Artificial (IA). Con lo cuál se espera que, en el futuro cercano, estas tecnologías emergentes tengan un impacto directo en la ciberseguridad y por tanto en temas de seguridad nacional. En sí, la

clara barrera que marcará en el futuro cercano entre las potencias del ciberespacio y el resto de las naciones será la consolidación de estas nuevas tecnologías en el panorama de la política internacional. Con lo que habla de una clara diferenciación de potencias del ciberespacio que abordan Nye (2012) y Kello (2013), así como la métrica del NCPI (2021)

En relación con el contexto de diferenciación de actores desde el ciberpoder, Glavinich (2021) destacó que una de las mayores amenazas actuales y previsibles en torno al ciberespacio, será la falta de gobernanza al interior del dominio. En complemento a este comentario, Delgado (2021) indica que, en la actulidad, hay gran cantidad de naciones que escatiman en ejercer y demostrar el ciberpoder y la fortaleza que detentan al interior del ciberspacio. Por ejemplo, se citan casos de regiones como Europa y Asia, con un buen desarrollo de ciberapaciadades. Mientras que países como Rusia, Estados Unidos e Israel también develan su capacidad de realizar ciber operaciones en el entorno digital, desde una perspectiva mitilar. En este contexto, Pauli (2021) destacó las asimetrías de capacidades que existen entre los actores estatales y no estatales en el ciberespacio. Con lo cual es importante crear ciber resiliencia en contra de agresiones de Estados-Nación, grupos criminales o de espionaje, etc (Pauli-Medeiros y Goldoni, 2020).

En esta lógica, Sancho (2012) indica que los Estados-Nación, deben de avocar sus cibercapacidades en aras de evitar cuatro diferentes clasificaciones de incidentes en el ciberespacio: 1) ciberataques 2) ciberdelitos 3) ciberespionaje, y 4) ciberguerra. En esta clasificación, destaca que los ciberataques y ciberdelitos están principalmente relacionados con gobiernos estatales locales. Mientras que el ciberespionaje y la ciberguerra están conectados con dimensiones de seguridad nacional. La clasificación es cercana a la delimitada por autores como Pessiri (2019), Bendovschi (2016) y Tabansky (2011). Por otra parte, en torno a la categoría de ciberguerra, es ambigua, y describe de forma concreta el uso del ciberespacio para realizar la guerra de la misma forma que se utiliza el poder marítimo y el áereo. No se puede perder de vista que las guerras siguen siendo una decisión política de usar el poder nacional. Consiguientemente, es un error reducir el concepto de ciberguerra a un nuevo tipo de guerra. Con la cual los comentarios de Sancho (2021) están en sintonía con la visión de Van Creveld (1991).

En la lógica de los tipos de amenaza Parraguez (2021) destacó la importancia de consolidar las capacidades de resiliencia, por parte de los Estados-Nación, para su defensa nacional. Y que, si bien no es viable crear una protección que garanticé el cien por ciento de protección, los países deben de mantener al menos dos capacidades: 1) garantizar la seguridad de los sistemas críticos, y 2) tener un margen de capacidades de reacción frente al incidente, aunque se traté de un incidente de *Z Day Attack* o día zero. En ese sentido, la resilicienca implica también un nivel de aprendizaje frente a los ciberincidentes, con la finalidad de mejorar los sistemas para el futuro. En adición, Saavedra (2021) especifico que la resiliencia es el eje central del desarrollo de una ENCS, y una vez que se parta de la noción de seguridad nacional, que debe resguardarse en el ciberespacio, deben de consolidarse las asociaciones estrátegicas entre las partes interesadas para operacionalizar la estrategia. Por último, dentro de este eje temático, destacaron los comentarios de Palma (2021), que indicó que la construcción de ciberpoder, también debe asociarse a la inclusión de la ciudadanía y el foratelecimiento de los derechos fundamentales de las personas. Una visión cercana a la visión liberalista, en torno al ciberpoder y ciberseguridad de autores como Petallides (2012) y Kundnani (2017).

Tabla 36. Comentarios estratégico del eje de discusión de ciberpoder y ciber resiliencia.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Boris Saavedra	▪ En el desarrollo de estrategias de Seguridad Nacional no se debe limitar únicamente a las tecnologías presentes, es vital tener en consideración las tecnologías futuras. Esto marcará la diferencia entre los países que sean potencias del ciberespacio y aquellos que sólo se límiten al desarrollo de cibercapacidades. ▪ El primer elemento clave en el desarrollo de una estrategia de ciberseguridad es la resiliencia. El segundo elemento clave es el desarrollo de la asociación público-privado. Este punto es complicado de lograr dado la diferencia de objetivos que existen entre los actores. Por un lado, el sector privado funciona por principios de ganancia mientras que el gobierno busca el bien común.
2	Mariano Bartolome	▪ El ciberpoder igualmente está relacionado con la capacidad de alcanzar objetivos y lograr resultados esperados en diversos ámbitos utilizando el ciberespacio como herramienta. ▪ Ciber resiliencia es la capacidad que tiene un determinado actor para recuperarse de un ataque sufrido y volver a tener operaciones normales.

No.	Nombre del entrevistado	Comentarios estrátegicos:
3	Giancarlo Delgado	▪ El ciberpoder es como una nación demuestra su fortaleza como país dentro del ciberespacio. Se compara con la compra de armamentos, los cuales no necesariamente son para utilizar, pero si para denotar el poderío militar.
4	Carolina Sancho	▪ El ciberpoder pueden ser evaluado desde variables como el nivel de dependencia al ciberespacio, penetración de las TICs, tipos de dependencias relacionadas con el ciberespacio, autonomía en el ciberespacio e incluso el grado de libertad de información que hay en el quinto dominio y el nivel de control o restricción que existe a los ciudadanos en el ciberespacio.
5	María Luisa Parraguez	▪ La ciber resiliencia implica tener la capacidad de contener un ciber incidente y de seguir operando. En otras palabras, es la capacidad de reaccionar. De igual forma este elemento está relacionado con el ciberpoder y cibercapacidad que tiene cada nación. ▪
6	Ricardo Magno Texeira	▪ El ciberpoder está relacionado con la capacidad de dominación que tienen un Estado frente otro Estado en el ciberespacio, teniendo relación con el alcance y poder tecnológico que tiene cada nación. ▪ Ciberpoder es la capacidad del Estado de ser resiliente en el ciberespacio; es decir, tener la resistencia de recibir ataques y al mismo tiempo poder mantener su continuidad operativa en los servicios.
7	Edgardo Glavinich	▪ En el ciberpoder la relación entre lo físico y lo intangible del ciberespacio no tienen un equilibrio. Pues si bien, los dos pueden influir en sus respectivas esferas, se valora que hoy en día lo digital tiene mayor influencia en lo físico.
8	Sandra Palma	▪ El ciberpoder requiere también de un sistema de poderes separado para que las estrategias sean más transparentes y se inclinen más hacia la ciberdefensa. No sólo debe avocarse a prevenir ciberataques, contener ciberdelitos o realizar operaciones militares en el ciberespacio. Debe tener igualmente una dimensión avocada a la promoción de los derechos humanos y bienestar de las personas.

Fuente: Elaboración propia.

4.4.3 Soberanía y ciberespacio

El análisis en torno a la comprensión de la soberanía partió de los comentarios estrátegicos de Pauli (2021), al indicar que en el ciberespacio la soberanía tradicional no existe como es entendida en el espacio material. Lo anterior, a razón de que por la propia naturaleza global del ciberespacio desafía el concepto de soberanía, sobre todo la noción del territorio físico. En este sentido, se acepta que la soberanía está en sintonía con las percepciones de actores como Glanville (2013) y McFarlane y Sabahdze (2013), de una concepción postwesphaliana en torno al concepto en cuestiones de ciberseguridad. No obstante, a pesar de que este componente de la soberanía no existe en el dominio, esto no implica que la soberanía no pueda ser ejercida en el ciberespacio. Lo anterior a razón, de que el nivel físico, es decir los componentes materiales, del internet, están situados en espacio territorial, y se ajustan a leyes nacionales. Por otra parte, el componente virtual, del internet, tiene repercusiones en el mundo físico, y si se ve afectado el componente físico de un Estado-Nación, por un suceso acontecido en el ciberespacio, igualmente se estaría impactando la esfera de la soberanía nacional. Esta visión se acopla a la propuesta de esta investigación en torno a denominar estos eventos como *hechos ciberfísicos* (Aguilar-Antonio, 2019).

En ese sentido, Bartolome (2021) indica que los Estados-Nación pueden argumentar ejecutar una acción a través del ciberespacio, con la finalidad de resguardad su soberanía, seguridad nacional e intereses de política exterior. Y en los hechos países como Estados Unidos, Rusia, China y Reino Unido. No obstante, hablar de un nivel de agresión, para la soberanía de un país, es aún un territorio brumoso y difícil de delimitar teóricamente. A razón de que cuándo se habla de ciberguerra, los conceptos de *jus in bello, jus ad bellum*, o el derecho internacional humanitario, no son fáciles de delimitar en el contexto de un ciber incidente, ataque o agresión (Bartolomé, 2019).

En un ámbito divergente a la concepción de la seguridad nacional, Contreras (2021) indicó que la soberanía también se materializa en el ciberespacio, a través del nivel de responsabilidad que tienen los gobiernos de los Estados-Nación para resguardar el Estado de Derecho e imperio de la ley. Con lo cual, la creación de controles jurídicos igualmente implica la extensión de la soberanía nacional al dominio. Es precisamente, esta visión de la soberanía del ciberespacio, la que está más arraigada al concepto de gobernanza global que

al concepto de gobernanza tradicional, también es considerara por métricas como el GCI (2022).

Mientras que para Glavinich (2021) es la que se promueve a través de instrumentos de cooperación internacional como lo son NCSI, la AGC o el Convenio de Budapest, cuya finalidad es fomentar la gobernanza global. Con esto re verifica que dentro del ciberespacio aún existen esquemas mediante los cuales se puede argumentar que la soberanía de las naciones es efectiva, principalmente en estos ámbitos de legislaciones nacionales y locales, para crear un marco de procuración de justicia contra ciber delitos, incidentes de seguridad de informática y ataques a infraestructura crítica nacional. En la tabla 37 se presentan los comentarios estrátegicos obtenidos de este eje de información.

Tabla 37. Comentarios estratégicos del eje de discusión de ciberpoder y ciber resiliencia.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Brenno Pauli	▪ Se parte de la premisa que la soberanía tradicional no existe en el ciberespacio. Incluso, la propia naturaleza global del ciberespacio desafía el concepto de soberanía, sobre todo por no haber un territorio físico.
2	Carolina Sancho	▪ Los ataques en el ciberespacio y la necesidad de ciberdefensa están bajo la línea de pensamiento de derecho a legítima defensa. ▪ El problema con los ciberataques que vulneran la soberanía es la respectiva autoría de estos. Puesto que se necesitaría que el Estado que efectuó el ataque lo reconociera, situación que no va a suceder.
3	Edgardo Glavinich	▪ La soberanía física puede ser vulnerada desde el ciberespacio, sobre todo cuando no se sabe de donde es el origen. Un ejemplo de esto sería un ataque cibernético a una planta potabilizadora de agua, si bien es un ataque digital, repercute en lo físico. ▪ Se puede crear una soberanía artificial en el quinto dominio. Siendo China un ejemplo de esto en donde ha cortado la libertad de sus ciudadanos en el ciberespacio.
4	María Luisa Parraguez	▪ Naciones Unidas ha intentado regular el ciberespacio mediante acuerdos. No obstante, esto no ha sido posible ya que hay una división de países dentro de la organización, dado que por un lado se encuentra

No.	Nombre del entrevistado	Comentarios estrátegicos:
		EE. UU con sus respectivos aliados y por el otro China, Rusia y Cuba. Se comenta que esta división ha imposibilitado la firma de un acuerdo que regule el ciberespacio.

Fuente: Elaboración propia.

4.4.4 Filtraciones a la información

En este eje de análisis, el caso de Wikileaks y las filtraciones de información por parte de la NSA de Edward Snowden fueron referenciados por múltiples entrevistados como fue el caso de Bartolome (2021), Glavinich (2021), Delgado (2021), Parraguez (2021) y Sancho (2021). Los comentarios se avocaron a señalar la importancia de ambos incidentes, para demostrar el potencial de vulnerar la soberanía de los Estados-Nación a través de las fugas de información. Del mismo modo, se identificó la fragilidad que pueden acontencer en los sistemas de seguridad nacional, por la debilidad del componente humano, o por la figura de los *insider,* asociada a un elemento del sistema de seguridad nacional, que es clave para la filtración de información.

De esta forma, las vulneraciones a la soberanía, como consecuencia de las fugas de información, implican una falla sistemática dentro de los sistemas de seguridad nacional. A la par que también se han transformado en herramientas para la renovación de los cuerpos de inteligencia y encontrar de forma visible las fallas que detentan estas estructuras. En este marco, será determinante la visión en torno a la protección de información que detente cada nación, así como su ENCS, a razón de que los países que prioricen la seguridad nacional, por encima de los derechos digitales o el desarrollo económico, establecerán que hay información de las naciones que debe mantenerse clasificada a fin de garantizar la soberanía de un país, incluso si esto implica contener algunas libertades de la sociedad civil y las empresas.

En el caso concreo del estudio de caso de esta investigación, y la vinculación a la filtración de los correos del Comité Nacional Democráta y la correspondencia entre Hillary Clinton, se indicó que se aceptaba como un hecho polarizador la difusión de esta información, que afectó la vida política interna de los Estados Unidos, en el marco de la elección presidencial de 2016. Del mismo modo, destacaron las visiones de Delgado (2021) y Bartolomé (2021) sobre

la ciberexplotación de información en el incidente SolarWinds, que presentan el panorama de ciberexplotación de parte de Rusia, para obtener información de inteligencia para obtener ventajas estrátegicas frente a Estados Unidos en el ciberespacio. Los comentarios estrátegicos de este eje de discusión se presentan en la tabla 38.

Tabla 38. Comentarios estratégicos del eje de discusión de filtraciones de información.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Arístides Contreras	▪ Se menciona que los insiders son un punto determinante de riesgo en las fugas de información, pues la extracción de datos no solo puede provenir del interior si no también puede ser creada desde las mismas organizaciones.
2	Mariano Bartolomé	▪ Hay filtraciones de información que tienen el potencial de dañar la seguridad nacional de un Estado. Esto puede ser sobre todo en el caso que se filtre información de alto nivel, información de bunkers de guerra, de las tecnologías militares, etcétera. ▪ Las fugas de información, como lo fue el caso de Snowden, representan un ataque a la soberanía nacional.
3	Edgardo Glavinich	▪ WikiLeaks se ha convertido en una herramienta para la renovación de cuerpos de inteligencia internos. ▪ En los casos de fugas de información como con Snowden y WikiLeaks, estos han servido para que el sistema sea adaptado a reparar las anomalías. Estos casos son donde el sistema aprende de dichas fugas -o anomalías-, se adapta y se fortalece.
4	Gianncarlo Delgado	▪ Existe una diferencia entre el sector privado y el sector público en lo que se refiere a lidiar con las fugas de información. Dado que el sector privado establecerá juicios y demandas que posiblemente terminarán en cárcel. Se denota que los juicios tienden a ser cortos. Por otro lado, cuando se habla de robar información a un estado, normalmente está más relacionado con persecución política.
5	Ricardo Magno Texeira	▪ Los casos de fuga de información tienen un impacto muy grande en en la toma de decisiones y la reputación de los Estados-Nación, que puede generar inestabilidad política.

No.	Nombre del entrevistado	Comentarios estrátegicos:
		▪ Los ataques que resultan en fugas de información tienen, como fin exponer que los gobiernos no están preparados para proteger los datos de los ciudadanos o están sobrepasando esferas de sus derechos digitales.

Fuente: Elaboración propia.

4.4.5 Ciberespacio y procesos políticos

En torno a la disución del potencial del ciberespacio, para influencia en procesos políticos Bartolomé (2021) y Pauli (2021), indicaron que a pesar de que existen grandes referentes como el impacto del robo de información y los servicios de consultoría política, que ofrecía la empresa Cambridge Analytica, estos casos no representan una afectación a la soberanía nacional. Lo que rescata de este caso es el mal uso de los datos personales de los usuarios en la red. Sin embargo, al consultar su opinión sobre las operaciones sistemáticas y bien estructuradas, realizadas por el IRA en el marco del *Russiangate* ambos indicaron que estos eventos si pueden considerarse una violación a la soberanía nacional, ya que un país externo influyó de manera directa en los asuntos internos de otro país, vulnerando así su soberanía.

En este marco, Bartolomé (2021) indica que la incidencia rusa puede evaluarse en tres aspectos, por un lado, en lo referente el hackeo de las cuentas del Comité Demócrata y los cercanos a Clinton, que si causó un impacto en la intención de voto hacía Hillary Clinton y ayudó a Trump. En segunda instancia, están las campañas de información en redes sociales para influir al electorado. Las cuales tenían como fin impactar en diferentes sectores políticos, para polarizar el marco de la elección y el perfil que tuviera el potencial votante. Finalmente, la evidencia en torno a SolarWinds, si bien no puede relacionarse aún a ningún tipo de injerencia o acción concreta, del gobierno ruso, para vulnerar a los Estados unidos, el simple hecho de realizar dicha acción de ciber explotación y espionaje a agencias gubernamentales del gobierno de esta nación, implica el intento de utilizar el ciberespacio para alcanzar una ventaja estrátegica por parte de Rusia.

En el marco de este debate, Contreras (2021), Saavedra (2021) y Parraguez (2021) indicaron que es altamente trascendental que las naciones consideren a los sistemas electorales parte de su infraestructura critica nacional, y que, en los hechos, los Estados Unidos ya la tiene considerada en esta clasficiación junto a otros quince sectores estrátegicos para su seguridad

nacional (Parraguez, Stockton, y Houle, 2021). En este contexto, en el análisis de Glavinich (2021) destacó el hecho de que la manipulación de la información en procesos electorales puede afectar la estabilidad del Estado-Nación, a razón que la manera en la que influye permite cambiar las voluntades del electorado, a través de la polarización. Para esto, se citó el caso de la Primavera Árabe, en que una dinámica a través de platafromas como las redes sociales afecto la estabilidad y gobernabilidad de países como Egipto y Tunez. Asimismo, si bien la dinámica puede vincularse sólo al esquema de la polarización política, Parraguez (2021) indicó que parte las 15,000 instituciones y actores que e fueron víctimas del ataque de SolarWinds, también eran actores que relación directa con el sistema electoral de Estados Unidos.

Tabla 39. Comentarios estratégicos del eje de discusión de ciberespacio y procesos políticos.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Aristides Contreras	• Los procesos electorales y sus respectivas instituciones deben formar parte de las infraestructuras críticas. Esto a razón de que en las elecciones hay una fuerte problemática con respecto a la manipulación de la información en los procesos electorales, en la que es susceptible de ser afectada la población.
2	Boris Saavedra	▪ El poder del internet no debe menospreciarse en materia de infraestructura crítica. Esto es más notorio en los países que cuentan con los recursos para desarrollarse en este rubro. ▪ Cada nación debe desarrollarse en sus propios dominios de infraestructura y en el ciberespacio a fin de poder competir con otros países. ▪ En un futuro Naciones Unidas tendrá que vincularse de mayor forma a los temas de ciberespacio. Incluso, será necesario crear una carta de las Naciones Unidas que contenga las relaciones del ciberespacio.
3	Brenno Pauli	▪ Si Rusia hubiera entrado al sistema electoral de EE. UU. y cambiado el registro de las votaciones, eso se podría considerar como un ataque a la soberanía de EE. UU. Del mismo modo, una intromisión a los sistemas del país puede alcanzar esa meta. ▪ En el caso de Rusia durante las elecciones del 2016 cuando un grupo de hackers intentaron atacar el Comité Democrático Internacional, este si pudo representar un problema de estabilidad interna para los Estados Unidos y daño a la soberanía nacional.

No.	Nombre del entrevistado	Comentarios estrátegicos:
4	Carolina Sancho	▪ Los sistemas electorales deben ser parte de la infraestructura crítica de un país por el tipo de información de los ciudadanos que se maneja. Misma que puede ser utilizada no solo por los partidos políticos para sus campañas, sino también por empresas privadas e incluso por grupos delictivos o terroristas.
5	Edgardo Glavinich	▪ El hackear un sistema electoral tendría que ser considerado como un acto de guerra. Sin embargo, el influir en la conciencia de los ciudadanos no. La clave para saber si es una agresión real es conocer si tiene repercusiones en lo físico.
6	Gianncarlo Delgado	▪ En lo que se refiere a las jornadas electorales digitales, las naciones deben pasar primero por proceso de transformación digital completos y transversales a fin de asegurar las votaciones. Lo cual requiere un nivel de madurez elevado en temas de digitalización y transformación digital. ▪ Parte de la madurez digital implica el poder implementar controles necesarios de ciberseguridad a fin de poder tener elecciones transparentes.

Fuente: Elaboración propia.

Conclusiones generales de la investigación

La presente investigación partió de la hipótesis de que el ciberespacio es una nueva arena de la política internacional en la que es posible vulnerar la soberanía, seguridad nacional y política exterior de los Estados-Nación, a través de la manipulación de información. En este sentido, la selección del caso de *Russiangate* sirvió como un objetivo para esta labor. Una vez concluida la investigación, se indica que la hipótesis de este trabajo se ha verificado, a razón nuestro estudio de caso nos revela que la Federación Rusa, operó al menos tres estrategias en el marco de las elecciones presidenciales de 2016 y el incidente SolarWinds, para utilizar este nuevo dominio en aras de alcanzar una ventaja estrátegica contra Rusia, los cuales fueron:

1) La extracción y filtración de información del Comité Nacional Democráta, así como de la correspondencia de la candidata Hillary Clinton y su jefe de campaña John Podesta, en el marco de la elección presidencial de 2016.
2) La estructuración y ejecución de operaciones a través del ciberespacio, en el marco de la elección presidencial de 2016, con el fin de influir en la opinión pública y ciudadananía, para difundir desinformación y promover los radicalismos políticos, a través de redes sociales y eventos (*rallies*), que impactaron en la intención de voto del proceso electoral.
3) La capacidad de intervenir los sistemas informáticos de las empresas más importantes del país e instituciones del más alto nivel del gobierno de los Estados Unidos. A través de una ciberoperación que vulneró a la empresa *SolarWinds,* lo que implicó un ciber ataque con fines de ciber explotación.

En ese sentido, se expresa que, a través del ciberespacio, la Federación Rusa ha desarrollado un nivel trascendental de ciber poder, que le permite utilizar el dominio con la finalidad de alcanzar una ventaja estrátregica en la política internacional desde este campo.

Con lo cual se indica que hay una fuerte distancia desde el capítulo 1, en el que partimos del caso de análisis del ciber incidente de Estonia, en 2007, que para los estudiosos de la ciberseguridad implicó el primer gran referente de la vulneración a la soberanía de un Estado-Nación, para presentar las dinámicas de ofensa y defensa que poseen los países que detentan ciber poder. Sin embargo, en los inicios de la realización de este trabajo, se bucaba analizar las formas en que era posible ejecutar dicha vulneración a la integridad nacional. Del mismo modo, que calibrar el nivel de ofensa y denfensa de un Estado-Nación en este nuevo dominio.

Para esto, realizamos un análisis que se remontó a la creación del internet, en 1969, con el proyecto ARPANET, que surgió como una red de información entre universidades y el Departamento de la Defensa, de los Estados Unidos, ante situaciones de crisis. Hasta transformarse en dominio clave en la comprensión de eventos como el *Cablegate* de *Wikileaks* (2011), el uso de redes sociales para promover las protestas sociales que derivaron en la caída de Hosni Mubarak y Ben Ali, en el marco de la *Primavera Árabe* (2011), o la vulneración a un proyecto de desarrollo tecnológico nacional, como se dio con el caso del gusano de *Stuxnex* (2010), con la afectación a la central nuclear de Natanz, Irán.

En este contexto, se indicó que, por sus características, el ciberespacio representaba un régimen híbrido de componentes físicos y virtuales que coexisten en el mundo real. Esta noción era clave para entender como el internet se había transformado en una nueva arena de la política internacional, con capacidad de influencia en los conflictos y dinámicas globales.

De esta forma, planteamos la categoría de *hechos ciberfísicos*, que indicaba una nueva unidad de análisis para delimitar eventos, casos o unidades de estudio en que las dinámicas o procesos sociales que vinculan al internet y el espacio físico tienen un impacto en la soberanía del Estado-Nación y, en consecuencia, vulneran la integridad de su seguridad nacional o política exterior. De esta forma, diferenciamos la parte física del ciberespacio, integrada por Infraestructura de Telecomunicaciones (IT), como los *SITE*s, satélites, cables de fibra óptica, redes telefónicas y tecnología móvil de telecomunicación y TIC´s, e Infraestructuras Críticas Nacionales. De su parte virtual, compuesta por la superficie web, que representan la arena virtual a través de la cuál es posible ejecutar acciones para alcanzar una ventaja estrátegica en este dominio.

Con relación a lo anterior, definimos al ciberespacio como una arena de interacción compuesta por una parte virtual, integrada por una infraestructura web (protocolos de internet y softwares), y una parte física, (infraestructura de telecomunicaciones, critica y hardware), en que se suscitan dinámicas, fenómenos o hechos sociales en diferentes canales o esferas (política, económica, cultural, prensa, etc.), que poseen un potencial de transferencia o impacto de estos eventos al mundo material ,con repercusiones al contexto o integridad del Estado-Nación, gobierno o sociedad.

Posteriormente, procedimos a conceptualizar el término de ciber poder, al que presentamos como *"la capacidad de ejecutar y realizar operaciones en el ciberespacio con la finalidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en este dominio"*. Así como presentar una comprensión del término del ciberpoder desde diferentes perspectivas teóricas como la Teoría de la Guerra, el neorrealismo, la Teoría de la Comunicación y de la Complejidad. Del mismo modo, cerramos el capítulo 1 indicando las taxonomías de Kello (2013) y Klimburg (2012), para servirnos de una taxonomía que nos sirviera para analizar eventos de ciberseguridad en el marco de las relaciones internacionales, a la par de presentar los actores con margen de acción reconocidos en esta nueva arena global.

Para el capítulo 2 de investigación, comenzamos discutiendo el concepto de soberanía nacional, desde el enfoque estado-centrico, en el marco de las controversias surgidad a razón se que se define de que dicha noción no es aplicable en su comprensión dentro del ciberespacio. Para esto, nos sirvieron los debates post-westphalianos para indicar, que si bien, el ciberespacio es un campo de confrontación de las naciones, que no ajusta a los preceptos clásicos del Estado-Nación (territorio, población e invsittuciones de gobierno) las dinámicas y fenómenos suscitados en este campo si están adscritos a una soberanía nacional y tienen efectos materiales en el espacio físico de diversas naciones.

Asimismo, está discusión nos llevó a presentar el proceso de securitización del intenet, para entender el papel que juega la ciberseguridad en la doctrina y estragia de seguridad nacional de los Estados-Nación. Para esto, nos sirvió el análisis de Palfrey, que nos presentó las cuatro fases de la regulación del internet: 1) la *fase de acceso abierto* (1960 a 2000), 2) la *fase del acceso negado* (2000- 2005), 3) la *fase de acceso controlado* (2005 a 2010), y 4) la *fase de*

la contienda (2005 a nuestros días). Es precisamente en este última que los ciberataques, alcanzan un grado de magnitud tan amplio y grande, con fuertes efectos para la seguridad nacional, que las naciones deciden incluir al ciberespacio como un dominio de protección clave de la seguridad nacional. Y se da el desarrollo clave de legislaciones y estrategias nacionales de ciberseguridad, para el surgimiento de convenios y acuerdos internacionales para promover la gobernanza del internet, contra ciber delitos y ciber ataques. Como para presentar estándares internacionales para el desarrollo de ciber capacidades de los Estados-Nación como lo son el GCI (2021) y el NCSI (2018), que presentan una serie de estándares y referencia para nivel el margen de acción que tienen las naciones

En este punto, se volvió clave entender el tipo de consecuencias que podían tener los ciberataques en la esfera de la seguridad nacional, para esto fue necesario analizar que dimensiones detentaban las Estrategias Nacionales de Ciberseguridad de las naciones de la OTAN, las más aventajadas en esta materia. Frente a lo cuál se encontró que las principales dimensiones que definen a una ENCS bien estructurada, frente al contexto global de ciber amenazas son los siguientes:

I. El ciberespacio es un componente del poder nacional.
II. La presencia del multilateralismo y cooperación.
III. El ciberespacio es un instrumento de proyección internacional.
IV. La ciberseguridad tiene una dimensión civil, militar y estatal.
V. Vinculación actores estatales-actores no estatales o privados.
VI. Se comprende y diferencia la parte física y virtual del ciberespacio.
VII. Se reconoce la trascendencia comercial y económica del ciberespacio.

Con base a esta delimitación se analizó el estado actual de algunas Estrategias Nacionales de Ciberseguridad (ENCS) de naciones de América Latina, Asía y Afríca, disponibles en el CCD COE (2021). Y se contrastó está información con los siete pilares que presentan las ENCS de las naciones de la OTAN.

Por último, para cerrar el capítulo 2, presentamos los niveles de amenaza que podían provenir del ciberespacio, en una sugerencia de clasificaciónes basada en cuatro categorías: 1) *Ciber crimen, 2) Hacktivismo, 3) Ciber espionaje* y *4) Ciber guerra.* Frente al cual presentamos los conceptos de *Ciber disuasión,* al que definimos como las capacidades de reacción y defensa

para que los adversarios eviten ejecutar acciones en contra de un Estado-Nación, derivado del nivel de represalias que pueden ser mayores a los beneficios a obtener. Y el de *Ciber resiliencia*, que corresponde a una capacidad adaptativa para enfrentar riesgos y amenazas, que tiene como fin la mejora y constante actualización de las capacidades de defensa, en contra de amenazas constantes y evolución. Por último, discutimos algunos referentes internacionales del sector privado para contener ciber incidentes como el PRE-ATT&CK™, el *Cyber Threat Framework*, el *Risk Standards Initiative*, el STIX™, el NIST *Framework for Improving Critical Infrastructure Cyber security*, el CBEST *Intelligence-Led Cyber Threat Modelling*, y el COBIT 5 *and Risk IT*.

Para el capítulo 3 de este trabajo, como se habían abordado los nexos entre la soberanía y seguridad nacional, así como de la estructuración de una política de defensa por parte de los Estados-Nación, en el marco de una ENCS, se procedió a analizar los vínculos entre la soberanía y la política exterior. Y del mismo modo, rastrear los nexos con la capacidad de acción y ofensa en la política exterior. Para esto hicimos un análisis en torno a la comprensión del concepto de interés nacional, y como los diferentes países lo podían operar desde diferentes perspectivas teóricas como el paradigma realista, la visión liberalita, la Teoría de la Guerra, y el Constructivimos. Para presentar un esquema teórico que sirva a futuras investigaciones en ciberseguridad, con enfoque de política internacional, para analizar el uso de los Estados-Nación para perseguir sus intereses particuales y realizar operaciones ofensivas en el ciberespacio.

Después, pasamos a analizar los entornos de ciberseguridad y desarrollo de cibercapacidades, en las diferentes regiones del mundo como los países de la OTAN, el resto de los países de Europa, Asía, América Latina, Medio Oriente, África y Oceanía. Esto con bases a métricas como el GCI y el NCSI, que nos demostraron desde una visión liberalistas, cercana al multilateralismo y la cooperación internacional, los esfuerzos de diferentes países por acatar compromisos internacionales en aras de construir un régimen o la gobernanza del ciberespacio.

Una vez terminado este ejercicio, se analizó el conjunto de naciones que son consideradas líderes en la construcción de ciber poder, con base al NCPI (2021). Esta métrica es de importancia a razón que establece quienes son consideradas las cinco superpotencias del

ciberespacio, integrado por los países de de Estados Unidos, China, Reino Unido, Rusia e Israel. A la par de presentarnos la diferencia entre las dos subdivisiones del NCPI (2021), basados en el *Índice de intención cibernética (IIC),* vinculado al conjunto de países que da alta prioridad al ciberespacio para su consolidación de poder nacional, y el *Índice de Capacidades Cibernética (ICC),* centrado en presentar al conjunto de naciones que tienen capacidades efectivas de ciber poder para alcanzar sus intereses particulares en el ciberespacio.

Por último, presentamos un análisis de las cinco dimensiones que contempla el NCPI (2021): i. Vigilancia, ii Control, iii. Ofensivo, iv. Inteligencia, v. Comercial, vi Normas y vii. Defensa, con énfasis especial a los países que son potencias de este dominio. Cerramos el capítulo 3, analizando una esfera que escapa a la comprensión del NCPI (2022), presentando el panorama de las Amenazas Persistentes Avanzadas o *Advanced Persistent Threat,* una serie de ciber comandos definidos por la agencia de Fire Eye, formados y bajo el resguardo de China, Rusia, Irán, Corea del Norte y Vietnam, que tienen una alta presencia mediática por ejecutar ciberoperaciones en aras de alcanzar objetivos particulares de estos países a través del dominio del ciberespacio.

Una vez concluido este análisis, procedimos a utilizar todos los elementos de los tres primeros capítulos de la investigación, para aplicar este esquema teórico y analítico en el estudio de caso del *Russiangate* y *SolarWinds.* Para esto, en el capítulo 4 de la investigación utilizamos una estrategia de análisis divida en cuatro diferentes apartados que fueron:

1) Un análisis de fuentes abiertas a través de medios de prensa, mediante el cual se presentará una narrativa y contextualización de lo que fue el Russiagate. Este apartado, sirvió para ratrear desde los medios de prensa, como se observaba la información que surgió en torno a las tres tramas analizadas vinculadas a este estudio que fueron la trama *Russiangate, Investigación del Fiscal Especial e Impeachment de Trump* y *SolarWinds.* Desde el periodo de campaña de 2016 que confronto a Hillary Clinton y Donald Trump, pasando por la creación de la Fiscalía Especial para la investigación de la interferencia rusa en las elecciones presidenciales de 2016 y la publicación del Informe Mueller. Para terminar con el polémico fin del gobierno de Trump y el descubrimiento del ciberataque de *SolarWinds* en los primeros meses de la administración del presidente Joe Biden. Con esto

se hizo una reconstrucción de los evetnos enmarcados de la pólemica d ela intromisión de Rusia en las elecciones de 2016 y el hacekó a más 15,000 agencias del gobierno de los Estados Unidos de América.

2) *Un análisis del contenido del Informe sobre la investigación de la interferencia rusa en las elecciones presidenciales de 2016,* centrado en analizar los dos volúmenes de este documento. El primero vinculado a las ciberoperaciones rusas en el marco del proceso electoral de 2016 y la transición del equipo de campaña de Trump, hasta tomar la presidencia. Y el segundo, vinculado a los episodios de osbtrucción de justicia del presidente, para evitar que la investigación de la Fiscalía Especial se llevará a cabo, y culminó en diez episodios de obstrucción de justicia. Lo obtenido a través de este ejercicio sirvió para presentar un panorama amplio de información adicional y complementario a la investigación de fuentes abiertas, de cómo operaba el esquema de ciber operaciones de agentes del gobierno ruso, para causar un impacto en la intención de votos y polarizar a la sociedad estadounidense a través de una estrategia persistente y coordinada de influencia de APTs rusas en el marco de la elección presidencial de 2016.

3) *Un análisis de las cibercapacidades de los Estados Unidos y Rusia, a través de las métricas del NCSI (2019), GCI (2018), y el NCPI (2020) para valorar la evidencia presentada por el análisis de fuentes abiertas y el análisis al Informe Mueller*, que nos permitió valorar con dichas metodologías la viabilidad del éxito de una ciberoperación rusa en las elecciones presidenciales de 2016. En este apartado se analizaron las capacidades de ofensa y defensa de ambas naciones, así como su nivel de cibercapacidades para realizar una operación a través del ciberespacio que vulnere la seguridad nacional y soberanía. Del mismo modo, se presentó la estructura de ciber operaciones de Rusia, y se llegó a la conclusión de la viabilidad de ejecutar esferas de afectación por parte de esta nación a los Estados Unidos, que fueron: 1) La extracción y filtración de información del Comité Nacional Democráta, así como de la correspondencia de la candidata Hillary Clinton y su jefe de campaña John Podesta, en el marco de la elección presidencial de 2016. 2) La estructuración y ejecución de operaciones a través del ciberespacio, en el marco de la elección presidencial de 2016, con el fin de influir en la opinión pública y ciudadananía, para difundir desinformación y promover los radicalismos políticos, a través de redes sociales y eventos (rallies), que

impactaron en la intención de voto del proceso electoral. Y 3) La capacidad de intervenir los sistemas informáticos de las empresas más importantes del país e instituciones del más alto nivel del gobierno de los Estados Unidos. A través de una ciberoperación que vulneró a la empresa SolarWinds, lo que implicó un ciber ataque con fines de ciber explotación.

Por último, está 4) *La realización de un total de diez entrevistas con especialistas en ciberseguridad de las Américas, y la realización de un análisis de teoría fundamentada de los comentarios estratégicos obtenidos en cada conversatorio, con el fin de realizar un análisis sobre la viabilidad de la intromisión de Rusia en las elecciones de Estados Unidos de 2016.* Con base a determinar si está puede ser considerado una violación a la soberanía nacional y la consolidación del dominio del ciberespacio para realizar esta acción. Los comentarios fueron ricos en identificar aportes a la comprensión a la ciberseguridad con enfoque en seguridad nacional en las siguientes esferas:

I. Amenazas e impactos que puedan afectar la Seguridad Nacional desde el ciberespacio
II. Ciberpoder y Ciber resiliencia
III. Soberanía y ciberespacio
IV. Filtraciones a la información
V. Ciberespacio y procesos políticos

Por último, se presentó que, con base a los diez comentarios de los académicos, se logró establecer que la forma en qué opera Rusia, con las estrategias identificadas, para vulnerar a los Estados Unidos, en efecto si preseron una vulneración a la soberanía de esta nación con base a los siguientes ejes temáticos y comenterios estrátegicos:

1. Se considera que el ciberespacio es un nuevo campo de confrontación entre los Estados-Nación, en el que se buscan utilizar al dominio por parte de actores estatales, actores no estatales y actores estatales no organizados. De esta forma, el ciberespacio es un nuevo campo mediante el cual se puede vulnerar la seguridad nacional y soberanía de un Estado-Nación.

2. Del mismo modo, se indica que, entre los países analizados, para el caso de Estados Unidos y Rusia, ambos poseen capacidades probadas de ofensa y defensa, en el

ámbito de realización de ciberoperaciones, con lo cual son consideradas potencias del ciberespacio.

3. Si bien la soberanía es un tema sujeto a debate en el ciberespacio. Se acepta que hay un componente físico del dominio que puede tener impactos y efectos en el espacio material. De esta forma, los países consideran que los efectos en la estabilidad de los Estados-Nación puede verse comprometida por esta interconexión y tener impactos políticos, económicos o sociales que afecten a los Estados-Nación.

4. Las extracciones y filtraciones de información son considerados un componente de alta capacidad de vulneración del Estado-Nación. De esta forma, los casos señalados con el hackeo al comité democráta son considerados eventos que sí afectaron la elección presidencial de Estados Unidos en 2016. Por otra parte, la manipulación mediática y polarización, también se acepta puede tener efectos que dañen la estabilidad política del país, como pasó en el marco del Russiangate durante el gobierno de Trump. Finalmente, el caso de SolarWinds, implica, que más allá de la filtración de información, Rusia tiene el potencial para vulnerar a Estados Unidos y crear acciones de inteligencia que le den ventajas estrátegicas, a través de la ejecución de ciberoperaciones en este dominio.

5. Los procesos políticos son eventos en los cuales se ejecuta uno de los preceptos clave que definen la naturaleza de las democracias. La búsqueda de una injerencia para afectar los resultados ya sea para afectar los resultados, polarizar o causar inestabilidad política, implican una muy fuerte agresión a la soberanía de los Estados-Nación. Del mismo modo, las dinámicas de desinformación y de las redes sociales y el internet, en estos procesos, ha develado que el ciberespacio puede impactar en el marco de la realización de un proceso electoral. De esta forma, se identifica que para el estudio de caso seleccionado, la injerencia de actores rusos se dio al menos a través de tres vías: 1) extracción de información del Comité Nacional Democráta y de la correspondencia de Podesta y Clinton, así como su correspondiente difusión, 2) ejecución de ciberoperaciones sistemáticas y bien estructuradas para polarizar el contexto electoral a través de redes sociales, 3) penetración en sistemas de seguridad

informática de instuticiones públicas y privadas de importancia para el contexto político de los Estados Unidos.

Finalmente, también en la tabla 40 se presentan los comentarios estrátegicos obtenidos de las conclusiones de las entrevistas realizadas.

Tabla 40. Comentarios estratégicos de las conclusiones de las entrevistas.

No.	Nombre del entrevistado	Comentarios estrátegicos:
1	Mariano Bartolomé	▪ El tema de la soberanía en el ciberespacio es muy complejo dado que no existen limitaciones como las hay en el mundo físico. No obstante, el componente físico del ciberespacio si está sujeto a la soberanía nacional del lugar donde se encuentre. ▪ Las filtraciones y extracciones información presentan un gran problema de seguridad nacional y una posible vulneración a la seguridad nacional.
2	Ricardo Magno Texeria	▪ Hay una falta de coordinación entre los stakeholders a la hora de realizar acciones de ciberseguridad, y que es necesario alcanzar cooperación entre dichos actores a fin de proteger al Estado. ▪ El ciberpoder está relacionado con: capacidad de defensa en el ciberespacio, capacidad de ataque en el ciberespacio y capacidad de resiliencia tras un ciberataque.
3	María Luisa Parraguez	▪ No solo es responsabilidad de los Estados la protección del ciberespacio, sino también de los cibernautas, ya que es necesario que tengan ciber higiene al utilizar sus sistemas. ▪ El ciberespacio ha crecido gracias al ingenio y creatividad humana, brindando así una gran cantidad de opciones para realizar actividades, y es una responsabilidad conjunta su protección.
4	Aristides Contreras	▪ El ciberespacio se ha ido uniendo con los temas jurídicos, legales, de comportamiento humano y necesidades políticas. Es vital crear políticas de Estado digitales que trascienden a las políticas gubernamentales en temas de ciberseguridad.
5	Gianncarlo Delgado	▪ La soberanía nacional puede ser vulnerada mediante el ciberespacio, siendo los ataques a las infraestructuras críticas y la filtración de

No.	Nombre del entrevistado	Comentarios estrátegicos:
		información las mayores transgresiones y evidencia de esto.
6	Edgardo Glavinich	▪ La infraestructura crítica debería ser una prioridad en el desarrollo de Estrategias de Seguridad Nacional, sobre todo por el alto grado de interconexión que existe entre este tipo de infraestructura en diversos países. En la actualidad, el sector privado, grupos de crimen organizado y terrorismo, han sabido dominar y aprovecharse de las ventajas del ciberespacio, situación que no sucede del todo con los gobiernos. ▪ La soberanía física de un Estado puede ser vulnerada desde el ciberespacio. Sin embargo, no se puede ejercer soberanía en este dominio ya que no se pueden crear fronteras. Una posible alternativa es la creación de capas a fin de generar gobernanza global en el ciberespacio.
7	Carolina Sancho	▪ Ningún Estado está eximido a sufrir amenazas que puedan afectar su seguridad nacional desde el ciberespacio. Además, las vulneraciones pueden afectar de manera horizontal a diversos países de forma simultánea. Gran cantidad de los gobiernos del mundo no están listos para los procesos electorales electrónicos dado que no se puede garantizar la integridad de los votos. ▪ Los nuevos términos como lo son ciberguerra o ciberpoder, en realidad están implicados en los términos tradicionales de poder y guerra, siendo únicamente dimensiones de estos que sirven para alcanzar objetivos políticos.
8	Boris Saavedra	▪ El desarrollo de estrategias nacionales de ciberseguridad no debe estar basada únicamente en la tecnología actual, se debe de contemplar "los siguientes pasos", hacer especial énfasis en las tecnologías emergentes como lo son el 5G, la inteligencia artificial o la computación cuántica. ▪ El poder actualmente no se remite únicamente a lo militar, político o económico; ahora, es vital contemplar la esfera de la información, misma que se desarrolla en el ciberespacio y está altamente relacionada a temas de ciberpoder.
9	Brenno Pauli	▪ Al realizar un análisis de los ciberataques y ciberamenazas es vital considerar cuáles son los objetivos finales que se pretendían dañar o conseguir

No.	Nombre del entrevistado	Comentarios estrátegicos:
		con dichas operaciones. Situación que permite determinar si la soberanía de un Estado fue diezmada. ▪ La soberanía y el ciberespacio es un tema complejo. Dado que se tiene que estudiar en dos niveles. Con respecto a la parte física los Estados si pueden ejercer su derecho a soberanía; situación que no ocurre en el espectro electromagéntico. Uno de los elementos principales del ciberpoder es su transversalidad.

Fuente Elaboración propia.

Con relación a todo lo anterior, indicamos que deseamos que el presente trabajo se transforme en un marco de análisis útil, para la comprensión y análisis de incidentes de seguridad cibernética, en los que se comprometa la seguridad nacional y la política exterior. Del mismo modo, en aquellas futuras investigaciones que busquén analizar los vínculos de la soberanía con el ciberespacio, y como esta nueva arena de confrontación entre las naciones, se ha transformado en nuevo campo de influencia de la política internacional.

Referencias bibliográficas

(AAGD) Australian Attorney-General's Department (2009). Cyber Security Strategy. Disponible en: https://bit.ly/35cpJey

ABC News Pecorin, A., (2018), Where special counsel Robert Mueller's investigation stands right now. ABC news. https://abcnews.go.com/Politics/special-counsel-robert-muellers-investigation-stands-now/story?id=56722923

Aguilar-Antonio, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (25), 24-40.

Aguilar-Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. Revista de Estudios en Seguridad Internacional, 6(2), 17-43.

Aguilar-Antonio, J. M. (2020). Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. Revista legislativa de estudios sociales y de opinión pública, 13(29), 83-120.

Aguilar-Antonio, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios internacionales (Santiago), 53(198), 169-197.

Ahrens, J. (2017) Trump ante el nombramiento de un fiscal especial: "Es la mayor caza de brujas en la historia de América", El País, disponible en: https://elpais.com/internacional/2017/05/17/estados_unidos/1495053659_525427.html

Altinay, A. (2004). The myth of the military-nation. In The Myth of the Military-Nation (pp. 13-32). Palgrave Macmillan, New York.

AON (2019). "2019 Cyber Security Risk Report: What´s Now and What´s Next", February 19: https://www.aon.com/cyber-solutions/thinking/2019-cyber-security-risk-report-whats-now-and-whats-next/

Aouragh, M. (2012). Framing the Internet in the Arab Revolutions: Myth Meets Modernity. Cinema Journal, 52(1), 148-156.

Aron, J. (2012). How LulzSec kept itself safe during its summer of 'lulz'. New Scientist, 213(2855), 31.).

Bachrach, J. (2011). Wikihistory: Did the Leaks Inspire the Arab Spring? World Affairs, 174(2), 35-44.

Bachrach, P., & Baratz, M. S. (1963). Decisions and nondecisions: An analytical framework. American political science review, 57(3), 632-642.

Baezner, M. (2019). *Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*. ETH Zurich.

Bahrisch, O. y Kim, J. (2011). Hegemonic Power and Technology Advancement. In International Conference on Grid and Distributed Computing (pp. 562-572). Springer, Berlin, Heidelberg.

Baezner, M. (2018). *Use of Cybertools in Regional Tensions in Southeast Asia* (No. 11). ETH Zurich.

Bank of England (2016). CBEST Intelligence-Led Testing, An Introduction to CyberThreat Modelling, disponible en: https://bit.ly/2LgUjMC

Barcena- Coqui, M. (2000). La reconceptualización de la seguridad: el debate contemporáneo. Revista Mexicana de Política Exterior, 59, 9-31.

Barnum, S. 2014. "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). Disponible en: https://bit.ly/33lvWDP

Barrón, J. (2017). Propuesta de un método geopolítico para el estudio de sistema masivo de medios de comunicación desde la socio cibernética crítica. En: Apuntes teórico-metodológicos para el análisis de la espacialidad: aproximaciones a la dominación y la violencia. Herrera, D., Gónzález, F. y Saracho F. (eds). Monosilabo –UNAM, pp. 63-74.

Bartolomé, M. (2021). Entrevista, realizada el 01 de septiembre de 2021

Bartolomé, M. (2006). La seguridad internacional en el siglo XXI: más allá de Westfalia y Clausewitz. Academia Nacional de Estudios Políticos y Estratégicos, Ministerio de Defensa Nacional, Chile.

Bartolomé, M. C. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. URVIO Revista Latinoamericana de Estudios de Seguridad, (25), 8-23.

Bartolomé, M. C. (2013). Una visión de América Latina desde la perspectiva de la agenda de la Seguridad Internacional contemporánea. Relaciones Internacionales.

Barzashka, I. (2013). Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. *The RUSI Journal*, *158*(2), 48-56.

Bassets, M. (2016). La verdadera victoria de Bernie Sanders en EE UU. El País, disponible en: https://elpais.com/internacional/2016/01/27/estados_unidos/1453871402_560644.html

BBC News (2007). Tallinn tense after deadly riots. BBC News, disponible en: http://news.bbc.co.uk/2/hi/europe/6602171.stm

BBC (2016). Bernie Sanders, el socialista que quiere ser presidente de EE.UU. BBC, disponible en: https://www.bbc.com/mundo/noticias/2015/05/150502_eeuu_presidencia_candidato_socialista_bernie_sanders_wbm

BBC (2016b). Rusia "intervino en las elecciones para promover la victoria de Donald Trump", dicen agencias de inteligencia de EE.UU. 10/12/2016, disponible en: https://www.bbc.com/mundo/noticias-internacional-38274334

BBC Mundo (2016c) Acusar a Trump no era una opción: el fiscal especial Robert Mueller habla por primera vez sobre la investigación de la trama rusa. disponible en: https://www.bbc.com/mundo/noticias-internacional-48451374

BBC MUNDO (2016d). Estados Unidos: James Comey, el polémico director del FBI que puso en aprietos a Hillary Clinton e investigaba los supuestos vínculos de la campaña de Trump con Rusia, disponible en: https://www.bbc.com/mundo/noticias-internacional-37823989

BBC MUNDO (2017a). Estados Unidos: James Comey, el polémico director del FBI que puso en aprietos a Hillary Clinton e investigaba los supuestos vínculos de la campaña de Trump con Rusia, disponible en: https://www.bbc.com/mundo/noticias-internacional-37823989

BBC Mundo (2017b) ¿Qué significa que un gran jurado se sume a la investigación sobre la presunta intervención de Rusia en las elecciones de Estados Unidos? disponible en, https://www.bbc.com/mundo/noticias-internacional-40822439

BBC News (2017c) Trump-Russia inquiry: President 'probed for obstruction of justice'. BBC News. Disponible en https://www.bbc.com/news/world-us-canada-40283036

BBC News (2017d). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. [En Línea] Disponible en: https://www.bbc.com/mundo/noticias-39800133

BBC Mundo (2018) El departamento de Justicia de Estados Unidos acusa a 13 ciudadanos rusos de interferir en las presidenciales de 2016.

BBC News (2019a) Trump no fue exonerado por el informe de Muller: el testimonio del exfiscal especial ante el Congreso, BBC News, disponible en: https://www.bbc.com/mundo/noticias-internacional-49105088

BBC News (2019b) Trump impeachment: How Ukraine story unfolded, disponible en: https://www.bbc.com/news/world-us-canada-50323605

Beck, Ulrich (1992) Risk Society: Towards a New Modernity. London: Sage

Bejtlich, R. (2013). China's" advanced persistent threat" to American computer networks. Hampton Roads International Security Quarterly, 16.

Benítez, R. (1986). El pensamiento militar de Clausewitz. Revista Mexicana de Ciencias Políticas y Sociales, 126, 97-123.

Benítez, R. (2005). Seguridad hemisférica: debates y desafíos (Vol. 4). UNAM.

Bertrand, N. y Wolf, E. (2020). Nuclear weapons agency breached amid massive cyber onslaught, Político, disponible en: https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855

Betts, K. (2013). The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can-and Can't-Do Now. Foreign Aff., 92, 87.

Betz, B. (2021). SolarWinds breach launched from within the United States, Seeking Alpha, disponible en: https://seekingalpha.com/news/3663003-solarwinds-breach-launched-from-within-the-united-states

Bhatt, P., Yano, E. T., & Gustavsson, P. (2014l). Towards a framework to detect multi-stage advanced persistent threats attacks. In *2014 IEEE 8th international symposium on service oriented system engineering* (pp. 390-395). IEEE.

BID/OEA (2017). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Banco Interamericano de Desarrollo y Organización de los Estados Americanos, disponible en: https://bit.ly/2qTwdR9

Bodeau, D., McCollum, C., & Fox, D. (2018). Cyber Threat Modeling: Survey, Assessment, and Representative Framework. HSSEDI, The Mitre Corporation.

Brate, A. (2002). Technomanifestos. Texere, LLC.

Bruer, W., y Perez, E. (2016). Officials: Hackers breach election systems in Illinois, Arizona. CNN, 30/08/2016, disponible en: https://edition.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/

Bing,C. (2020). Suspected Russian hackers spied on U.S. Treasury emails – sources. Reuters, disponible en: https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive-idUSKBN28N0PG

Bing, C., Stubbs, J., Satter, R. y Menn, R. (2021). Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources, Reuters, disponible en: https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

Borger, J. (2017) First charges filed in Robert Mueller Russia inquiry – reports. The Guardian. The Guardian. Disponible en: https://www.theguardian.com/us-news/2017/oct/28/robert-mueller-russia-inquiry-first-charges

Bloomberg (2020). At least 200 victims identified in suspected russian hacking. Bloomberg, disponible en: https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking

Brenner, N. (1998). Global Cities, Glocal States: Global City Formation and State Territorial Restructuring in Contemporary Europe. Review of International Political Economy, 5(1), 1-37.

Buchanan, B. y Sulmeyer, M. (2016). Russia and cyber operations: Challenges and opportunities for the next US administration. Carnegie Endowment for International Peace, 3.

Burchill, S. (2005). The national interest in international relations theory. Springer.

Buzan, B., Wever O. y De Wilde, J. (1998), Security: A new framework k for analysis. Boulder: Lynne Rienner.

Cano, S. (2016). La impopularidad de Hillary Clinton sube casi al mismo nivel de Donald Trump. Univisión, disponible en: https://www.univision.com/noticias/elecciones-2016/la-impopularidad-de-hillary-clinton-sube-casi-al-mismo-nivel-de-donald-trump

Cassidy, J. (2016). How Donald Trump Became President-Elect. The New Yorker, 09/11/2016, disponible en: https://www.newyorker.com/news/john-cassidy/how-donald-trump-became-president-elect

CCD COE Tallin (2021). "Strategy and Governance", Cooperative Cyber Defence Centre of Excellence, disponible en: https://ccdcoe.org/library/strategy-and-governance/

(CDPS) Canadian Department for Public Safety (2010). Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada. Disponible en: https://bit.ly/35sr29B

Chalfant, M. y Maggie M. (2020). Biden vows to make cybersecurity 'imperative' following massive hack. The Hill, disponible en: https://thehill.com/policy/cybersecurity/530706-biden-vows-to-make-cybersecurity-imperative-following-massive-hack

Chanona, A. (2015). Indicadores de Seguridad Humana. América del Norte, Unión Europea y Mercosur. UNAM.

Chase, M., & Chan, A. (2016). China's Strategic-Deterrence Concepts. In China's Evolving Approach to "Integrated Strategic Deterrence" (pp. 9-18). RAND Corporation.

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security (pp. 63-72). Springer, Berlin, Heidelberg.

Choucri, N., Madrick, S. Ferwerda, J. (2013). *Institutional Foundations for Cyber Security: Current Responses and New Challenges.* MIT. Massachusetts, EUA, 27 pág.

Chozick, A, Healy, P., y Alcindor, Y. (2016) Bernie Sanders respalda a Hillary Clinton y fortalece la unidad de los demócratas. 12/07/2016, disponible en: https://www.nytimes.com/es/2016/07/12/bernie-sanders-respalda-a-hillary-clinton-y-fortalece-la-unidad-de-los-democratas/

Cillizza, C. (2019) 10 conclusiones clave del testimonio de Robert Mueller ante la Cámara, CNN en Español, disponible en: https://cnnespanol.cnn.com/2019/07/24/7-conclusiones-clave-del-testimonio-de-robert-mueller-ante-la-comision-judicial-de-la-camara/

CISA (2020a). Joint statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI), Cybersecurity and Infrastructure Security Agency, disponible en: https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

CISA (2020b). Emergency Directive 21-01. Cybersecurity and Infrastructure Security Agency, disponible en: https://cyber.dhs.gov/ed/21-01/#supplemental-guidance

Cohen, S. (2019). Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests. *Cyber, Intelligence, and Security*, *3*(1).

Cohen, S. (2019). Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests. *Cyber, Intelligence, and Security*, *3*(1).

Collinson, S. (2015). Cómo Donald Trump se apoderó del Partido Repúblicano. CNN, 15/12/2015, disponible: https://cnnespanol.cnn.com/2015/12/14/como-se-apodero-donald-trump-del-partido-republicano/

Connell, M. y Vogler, S. (2017). Russia's approach to cyber warfare (1rev). Center for Naval Analyses Arlington United States.

(CONPES, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. Consejo Nacional de Política Económica y Social de la República de Colombia. Disponible en: https://bit.ly/33HXsLK

Contreras, A. (2021). Entrevista, realizada el 10 de julio de 2021

Costigan, S., & Lindstrom, G. (2016). Policy and the Internet of Things. Connections, 15(2), 9-18.

Cowley, A. (2011). The evolution on international system: surrender sovereignty or fight to the death. School of Advanced Air and Space Studies, Air University, 2011.

Craig, A. J., y Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. Realism in Practice, 85.

Curtis, S. (2011). Global cities and the transformation of the International System. Review of International Studies, 37(4), 1923-1947.

Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Recuperado el 12 de enero de 2020 de: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Carroll, M. (2000). Inventing the Internet. Publishing Research Quarterly, 16(2), 93-93.

Chertoff, M. (2014). The Strategic Significance of the Internet Commons. Strategic Studies Quarterly, 8(2), 10-16.

Dahl, R. A. (1961). The behavioral approach in political science: Epitaph for a monument to a successful protest. American Political Science Review, 55(4), 763-772.

Daly, M. K. (2009). Advanced persistent threat. Usenix, Nov, 4(4), 2013-2016.

Davies, G. (2016). *Sovereignty and Collaboration: Affordable Strategies in Times of Austerity*. Air Force Research Institute Maxwell Air Force Base United States.

Dean, D., DiGrande, S., Field, D., Lundmark, A., O'Day, J., Pineda, J., & Zwillenberg, P. (2012). The internet economy in the G-20. Boston Consulting Group.

Deibert, R., and Rohozinski, R. (2010). "Beyond Denial: Introducing Next Generation Information Access Controls." In: Access Controlled: The Shaping of Power, Rights, and Rule in

Cyberspace. Eds. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge: MIT Press, 2010.

Delgado, G. (2021). Entrevista, realizada el 28 de septiembre de 2021

Digital Attack Map (2019). Digital Attack Map. Disponible en: https://bit.ly/2qPHqCe

Demchak, D. (2012) Cybered Conflict, Cyber Power, and Security Resilience as Strategy, in: Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, ed. Derek S. Reveron (2012) (Washington, DC: Georgetown University Press), pp. 121–136.

(DMSJ) Dutch Ministry of Security and Justice (2011) The National Cyber Security Strategy, (NCSS). Strength through Cooperation. Disponible en: https://bit.ly/2QAKxIC

Deng, Y. (1998). The Chinese conception of national interests in international relations. The China Quarterly, 154, 308-329.

Detlefsen, W. R. (2015). Cyber Attacks, Attribution, and Deterrence: Three Case Studies. US Army Command and General Staff College Fort Leavenworth United States.

Deutsche Welle. (2017) Australian diplomat's tip led to Trump Russia probe: US paper. Deutch Welle. Disponible en: https://www.dw.com/en/australian-diplomats-tip-led-to-trump-russia-probe-us-paper/a-41982452

DNI -Director of National Intelligence- (2016). Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, disponible en: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1635-joint-dhs-and-odni-election-security-statement

DNI (2016b). Intelligence Community Statement on Review of Foreign Influence on U.S. Elections, disponible en: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1621-intelligence-community-statement-on-review-of-foreign-influence-on-u-s-elections

DNI (2016c). Intelligence Community Statement on Review of Forgein Influence on U.S. Elections, disponible en: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1621-intelligence-community-statement-on-review-of-foreign-influence-on-u-s-elections

DNI (2016d). Statement on Request for Additional Information on Russian Interference in the 2016 Presidential Election, disponible en: https://www.dni.gov/index.php/newsroom/press-

releases/press-releases-2016/item/1619-statement-on-requests-for-additional-information-on-russian-interference-in-the-2016-presidential-election

DNI (2016e), Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity, disponible en: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1616-joint-dhs-odni-fbi-statement-on-russian-malicious-cyber-activity

(DSN) Departamento de Seguridad Nacional (2019). Estrategia Nacional de Ciberseguridad. Disponible en: https://bit.ly/2XreCMi

Dobbins, J., Solomon, R. H., Chase, M. S., Henry, R., Larrabee, F. S., Lempert, R. J., ... & Shatz, H. J. (2015). Choices for America in a Turbulent World: Strategic Rethink. Rand Corporation.

DSA (2003). Declaración de Seguridad de las Américas. Organización de los Estados Americanos (OEA), disponible en: https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf

Eatwell, R. y Goodwin, M. (2018). National populism: The revolt against liberal democracy. Penguin Reino Unido.

Eesti Päevaleth (2007). Pronkssõdur viidi minema. Eesti Päevaleth Disponible en: http://epl.delfi.ee/news/eesti/pronkssodur-viidi-minema?id=51084856

Eisenhut, D. (2010). Sovereignty, National Security and International Treaty Law The Standard of Review of International Courts and Tribunals with regard to'Security Exceptions'. Archiv des Völkerrechts, 48(4), 431-466.

El País (2007). Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE. El País. Disponible en: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

El Universal. (2020a). Casa Blanca buscó restringir información sobre injerencia rusa: funcionario. El Universal, disponible en: Casa Blanca buscó restringir información sobre injerencia rusa: funcionario (eluniversal.com.mx)

Entous, A. & Nakashima, E. (2016). Secret CIA assessment says Russia was trying to help Trump win the White House. Washington Post, disponible en: https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html

(ENCS Costa Rica, 2017). Estrategia Nacional de Ciberseguridad de Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones, disponible en: https://bit.ly/2Y7UoaK

ENCS México (2017). Estrategia Nacional de Ciberseguridad. Presidencia de la República, disponible en: https://bit.ly/2Lj9Ew9

(EOTPW) Executive Office of The President Washington (2017). National Security Strategy of the United States of America. Disponible: https://bit.ly/32W0qMo

Eriksson, J., Giacomello, G., Salhi, H., Cavelty, M., Singh, J., & Franklin, M. (2009). Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. International Studies Review, 11(1), 205-230.

Falk, R. (2002). Revisiting Westphalia, Discovering Post-Westphalia. The Journal of Ethics, 6(4), 311-352.

Falkner, R. (2012). Global environmentalism and the greening of international society. International Affairs (Royal Institute of International Affairs 1944-), 88(3), 503-522.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

Farrell, H., & Finnemore, M. (2013). The End of Hypocrisy: American Foreign Policy in the Age of Leaks. Foreign Affairs, 92(6), 22-26.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Ferrero, A. (2019). El "Russiagate" ha muerto, larga vida al "Russiagate" El País, disponible en: https://elpais.com/internacional/2019/04/04/actualidad/1554378836_708421.html

Fajardo, L. (2016). ¿Habría derrotado Bernie Sanders a Donald Trump en las elecciones en EE.UU.? BBC, 11/10/2016, disponible en: https://www.bbc.com/mundo/noticias-internacional-37941680

France 24 France 24. (2018) Primer miembro de la campaña electoral de Donald Trump condenado por la llamada trama rusa. France 24. https://www.france24.com/es/20180908-primer-asesor-trump-condenado-russiagate

Frank, T. (2016). Forget the FBI cache; the Podesta emails show how America is run. The Guardian, disponible en: https://www.theguardian.com/commentisfree/2016/oct/31/the-podesta-emails-show-who-runs-america-and-how-they-do-it

Frankel, J. (1984). Prophecy and politics: socialism, nationalism, and the Russian Jews, 1862-1917. Cambridge University Press.

Faus,J. (2017) El yerno de Trump, interrogado por el fiscal de la trama rusa. El País.

Faus, J. (2018) Mueller imputa a 12 agentes de inteligencia rusos por el pirateo a la campaña de Clinton. El País.

Fazekas, D. (2016). Hillary Clinton's 55,000 Pages of Emails: A Whole Lot of Paper. ABCE News, 05/07/2016, disponible en: https://abcnews.go.com/Politics/hillary-clintons-55000-pages-emails-lot-paper/story?id=32663275

(FFIEC)The Federal Financial Institutions Examination Council (2016). Information Security Handbook on Risk Assessment, disponible en: https://bit.ly/2s4dmTy

FG Germany (2016). White Paper on German Security Policy and the future of the Bundeswehr. Federal Government of Germany, disponible en: https://bit.ly/2Otj8qN

Finnemore, M. (2010). National interests in international society. Cornell University Press.

FireEye (2020). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye, disponible en: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

FireEye (2021). Anatomy of Advanced Persistent Threats, FireEye, disponible en: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

Foreign Policy (2017). 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? [Foregin Policy. Disponible en: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Forbes (2018) Fiscal independiente Robert Muller está fuera de control: Trump, disponible en: https://www.forbes.com.mx/fiscal-independiente-robert-mueller-esta-fuera-de-control-trump/

Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist. AFL rev., 64, 1.

Freedom House (2017). Freedom of the Net. Disponible en: https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf

Frye, E. (2002). The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World. The Business Lawyer, 58(1), 349-382.

Fu, Y., Li, H., Wu, X., & Wang, J. (2015). Detecting APT attacks: a survey from the perspective of big data analysis. *Journal on Communications*, *36*(11), 1-14.

Gallagher, R. (2021) Russian Hackers continue with attacks despite Biden Warning, Bloomberg, disponible en: https://www.bloomberg.com/news/articles/2021-07-30/russian-hackers-continue-with-attacks-despite-biden-warning

Gambino, L, y Pamkhania, M. (2016) How we got here: a complete timeline of 2016's historic US election, disponible en: https://www.theguardian.com/us-news/2016/nov/07/us-election-2016-complete-timeline-clinton-trump-president

Gambino, L. (2017). Rosenstein stands by memo on firing James Comey: 'I wrote it. I believe it'. The Guardian. 19 de mayo. Disponible en: https://www.theguardian.com/us-news/2017/may/19/comey-deeply-uncomfortable-trump-attempts-relationship

Gamer, Thomas, and Christoph P. Mayer. "Large-scale evaluation ofdistributed attack detection." OMNeT++ 2009: Proceedings of the 2nd International Workshop on OMNeT++(hosted by SIMUTools 2009).

Gans, C. (2001). Historical Rights: The Evaluation of Nationalist Claims to Sovereignty. Political Theory, 29(1), 58-79.

García, R. (2006). Sistemas complejos: conceptos, métodos y fundamentación epistemológica de la investigación multidisciplinaria. Barcelona, Gedisa, 2006.

GBA & ITRC (2018). The Impact of Cybersecurity Incidents on Financial Institutions. Identity Theft Resource Center Generali Global Assistance. Disponible en: https://bit.ly/373fHOR

GCI (2014). Global Cybersecurity Index. International Telecommunication Union, disponible en: https://bit.ly/34rPZ4C

GCI (2017). Global Cybersecurity Index. International Telecommunication Union, disponible en: https://bit.ly/34rPZ4C

GCI (2019). Global Cybersecurity Index. International Telecommunication Union, disponible en: https://bit.ly/34rPZ4C

GCI (2021). Global Cybersecurity Index. International Telecommunication Union, disponible en: https://bit.ly/34rPZ4C

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: an overview. *Int J Adv Comput Netw Secur*, *4*(4), 5054

Ghanem, H. (2016). Roots of the Arab Spring. In The Arab Spring Five Years Later: Toward Greater Inclusiveness (pp. 39-64). Washington, D.C.: Brookings Institution Press.

Ghori, K. (2011a) The Arab Spring: How Will It Blossom?. Pakistan Horizon, 2011, vol. 64, no 3, p. 13-24.

Ghori, K. (2011b). The Global Challenge of WikiLeaks. Pakistan Horizon, 64(1), 5-15. Retrieved from http://www.jstor.org/stable/24711138

Gilpin, R. (2010). War and change in world politics. Cambridge University Press.

Glanville, L. (2013). The Myth of "Traditional" Sovereignty. International Studies Quarterly, 57(1), 79-90.

Glavinich, E. (2021). Entrevista, realizada el 25 de mayo de 2021

Gray, C. S & Sloan, G.. (Eds.). (1999). Geopolitics, Geography and Strategy. Frank Cass.

Greenberg, A. (2016). Trump ignoring US intelligence creates risks beyond Russian hacking, WIRED. Disponible en: https://www.wired.com/2016/12/trump-cia-national-intelligence-briefings/

Grotenhuis, R. (2016). Nation-building: Sovereignty and citizenship. In Nation-Building as Necessary Effort in Fragile States (pp. 59-72). Amsterdam: Amsterdam University Press.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice?. Senate (United States) Washington DC Committee on Armed Services.

Guimón, P. (2021). Los argumentos del segundo 'impeachment' a Trump. El País, disponible en: https://elpais.com/internacional/elecciones-usa/2021-01-13/los-argumentos-del-segundo-impeachment-a-trump.html

Greenberg, A. (2016) Trump ignoring US intelligence creates risks beyond Russian hacking, disponible en: https://www.wired.com/2016/12/trump-cia-national-intelligence-briefings/

Hansen, L., y Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155-1175.

Haas, P. y Haas, E. (2002). Pragmatic constructivism and the study of international institutions. Millennium, 31(3), 573-601.

Hackmageddon (2020). "2019 Cyber Attacks Statistics", disponible en: https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/

Haffa Jr, P. (2018). The Future of Conventional Deterrence: Strategies for Great Power Competition. Strategic Studies Quarterly, 12(4), 94-115.

Hafner-Fink, M., Malnar, B., & Uhan, S. (2013). The National Contexts of Post-national Citizenship. Sociologický Časopis / Czech Sociological Review, 49(6), 867-901.

Haimes, Y. Y. (2006). On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis: An International Journal, 26(2), 293-296.

Hakala, J. y Melnychuk, J. (2021). Russia's Strategy in Cyberspace (2021) CCD COE Tallin, disponible en: https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210

Hall, I. (2006). The international thought of Martin Wight. Springer.

Harwit, E., & Clark, D. (2001). Shaping the internet in china. Evolution of Political Control over Network Infrastructure and Content. Asian Survey, 41(3), 377-408. doi:10.1525/as.2001.41.3.377

Hathaway, M., & Klimburg, A. (2012). Preliminary considerations: on national cyber security. National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Herb, J & Jarret, L. (2019) Special counsel Robert Mueller ends investigation, CCN Politics, disponible en: https://edition.cnn.com/2019/03/22/politics/robert-mueller-report/index.html

Hennessey, S., y Wittes, B. (2017). Rober Mueller's show of strength: A quick and disty analysis. Brookings. disponible en: https://www.brookings.edu/blog/fixgov/2017/10/30/robert-muellers-show-of-strength-a-quick-and-dirty-analysis/

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses.

HM Government (2016). National Cyber Security Strategy 2016-2021. Disponible: https://bit.ly/35iQpu8

Hobbes, T. (2013). Del ciudadano y Leviatán. Tecnos.

Hoerder, D. (2010). Recent Methodological and Conceptual Approaches to Migration: Comparing the Globe or the North Atlantic World? Journal of American Ethnic History, 29(2), 79-84.

Hosenball, M. y Layne, N. (2018) Exclusive: Special Counsel subpoenas another Stone aide in Russia probe - sources. Reuters. Disponible en: https://www.reuters.com/article/us-usa-trump-mueller-subpoena-exclusive/exclusive-special-counsel-subpoenas-another-stone-aide-in-russia-probe-sources-idUSKCN1IJ2MV

Hughes, R. (2010). A treaty for cyberspace. International Affairs, 86(2), 523-541.

Hurrell, A. (2006). Hegemony, liberalism and global order: what space for would-be great powers?. International affairs, 82(1), 1-19.

Hunt, A. (2017). Trump fired Comey. Why not Mueller too?. Chicago Tribune Disponible en: https://www.chicagotribune.com/opinion/commentary/ct-donald-trump-robert-mueller-20170613-story.html

Hurwitz, R. (2012). Depleted Trust in the Cyber Commons. Strategic Studies Quarterly, 6(3), 20-45.

Iasiello, E. J. (2017a). Russia's Improved Information Operations: From Georgia to Crimea. Parameters, 47(2).

Iasiello, E. (2017b). China's Cyber Initiatives Counter International Pressure. Journal of Strategic Security, 10(1), 1-16.

ICA -Intelligence Community Assessment- (2017). Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, disponible en: https://www.dni.gov/files/documents/ICA_2017_01.pdf

ICT (2017). Facts and Figures 2005, 2010, 2014. Telecommunication Development Bureau, International Telecommunication Union (ITU). Disponible en: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf .

Ikenberry, G. J. (2011). Liberal leviathan. Princeton University Press.

Issikoff, M. (2016). FBI says foreign hackers penetrated state election systems. Yahoo News, 29/08/2016, disponible en: https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html

ISACA (2009). The Risk IT Framework Excerpt, disponible en: https://bit.ly/37YhEMN

ISACA (2014). "Risk Scenarios: Using COBIT 5 for Risk," September 2014, disponible en: https://bit.ly/33L8QGC

ISO/IEC (2012), Information technology – Security techniques – Guidelines for cybersecurity.

Islas, O. (2004). Marshall McLuhan, 40 años después. Chasqui. Revista Latinoamericana de Comunicación, (86).

ITU (2011) Measuring the Information Society. Disponible en: http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf.

IWS (2019). Internet Wordl Stats. Disponible en: https://bit.ly/2KVOgwD

Iltalehti (2007). Viron diplomaattien perheet evakuoitu Moskovasta. Disponible en: https://www.iltalehti.fi/uutiset/200705026057323_uu.shtml

Jacobus, C. (2017). Trump team collusion with Russia? Ukraine connection may hold key, disponible en: https://www.usatoday.com/story/opinion/2017/11/03/rubber-meets-road-russia-collusion-investigation-leads-more-questions-cheri-jacobus-column/822894001/

Jasper, S. (2020). Russian Cyber Operations: Coding the Boundaries of Conflict, Georgetown University Press.

Jayanthi, M. (2017). Strategic Planning for Information Security-DID Mechanism to befriend the Cyber Criminals to Assure Cyber Freedom. In Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on (pp. 142-147). IEEE.

Jervis, R. (2003). Understanding the Bush Doctrine. Political Science Quarterly, 118(3), 365-388.

Jibilian, I. y Canales, K. (2021). The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. Insider. Disponible: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=MX&IR=T

Johnson, C. (2009). Socio-Technical Approaches to Risk Assessment in National Critical Infrastructures. Risk Management, 11(3/4), 155-158.

Johnson, J. (2021). Internet penetration in Africa, by country. Statista. Disponible en: https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

Kapersky (2019). *Cyberthreat Real-Time Map*, disponible en: https://bit.ly/2XQbn17

Kass, H. (2020). Rare CISA Security Directive: Power Down Solarwinds Orion, MSSP Alert, disponible en: https://www.msspalert.com/cybersecurity-news/cisa-emergency-directive-solarwinds-orion/

Kao, D. Y. (2015, July). Performing an APT investigation: Using people-process-technology-strategy model in digital triage forensics. In *2015 IEEE 39th Annual Computer Software and Applications Conference* (Vol. 3, pp. 47-52). IEEE.

Kapersky (2020). "The Kapersky Lab Global IT Risk Report", February: https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf

Kapersky Lab (2020). Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado el 12 de enero de 2020: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Center for Excellence (CCDCOE), 28).

Keeling, D. (2004). Latin American Development and the Globalization Imperative: New Directions, Familiar Crises. Journal of Latin American Geography, 3(1), 1-21.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7-40.

Kemp, S. (2018). Digital in 2018 essential insights into internet social media, mobile, and ecommerce around the world. We Are Social. Disponible en: https://wearesocial.com/blog/2018/01/global-digital-report-2018

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Taylor & Francis

Keohane, R. y Dunn, J. (2002). International liberalism reconsidered. Power and Governance in a Partially Globalized World, 39.

Kramer, A. (2018) He Says He's an Innocent Victim. Robert Mueller Says He's a Spy. The New York Times. Disponible en: https://www.nytimes.com/2018/04/06/world/europe/robert-mueller-kilimnik-ukraine-russia-manafort.html

Krasner, Stephen D. (2010) The Durability of Organized Hypocrisy. In Sovereignty in Fragments: The Past, Present and Future of a Contested Concept, edited by Hent Kalmo and Quentin Skinner. Cambridge: Cambridge University Press

Krasner, S. (2001). Abiding Sovereignty. International Political Science Review / Revue Internationale De Science Politique, 22(3), 229-251.

KrebsOnSecurity (2020). Malicious Domain in SolarWinds Hack Turned into 'Killswitch', KrebsOnSecurity, disponible en: https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/

Kim, C. (2019) Full transcript of Robert Mueller's remarks. VOX, disponible en: https://www.vox.com/2019/5/29/18644237/robert-mueller-remarks-transcript

Klimburg, A. (2013). National cyber security framework manual (NATO CCD COE publication, 2012).

Klimburg, A., & Healey, J. (2012). Strategic Goals & Stakeholders. National Cyber Security Framework Manual, NATO CCD COE Publication, Talinn.

Kittichaisaree, K. (2017). Introduction: Perspectives of Various Stakeholders and Challenges for International Law. In Public International Law of Cyberspace (pp. 1-22). Springer, Cham.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 30.

Kover, J. y O. Johnson, (2020). SolarWinds MSP To Revoke Digital Certificates For Tools, Issue New Ones As Breach Fallout Continues, CRN, disponible en: https://www.crn.com/news/managed-services/solarwinds-msp-to-revoke-digital-certificates-for-tools-issue-new-ones-as-breach-fallout-continues

Kubálková, V. (2016). Foreign policy in a constructed world. Routledge.

Kundnani, H. (2017). What is the liberal international order? German Marshall Fund of the United States.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

Langner, R. (2015). To Kill a Centrifuge-A Technical Analysis of What Stuxnet's Creators Tried to Achieve. 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

LBND Brasil (2012). Libro Blanco de Defensa Nacional, disponible en: https://bit.ly/2PaYlHH

Le Monde Diplomatique (2019) "Russiagate", la débacle. Le Monde diplomatique, disponible en: « Russiagate », la débâcle (Le Monde diplomatique, 26 mars 2019) (monde-diplomatique.fr)

Lee, S. O. (2018). A New Warfront: North Korea's Cyber Threats. *Chicago Policy Review (Online)*.

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26-59.

Lenz-Raymann, K. (2014). Securitization Theory: Legitimacy in Security Politics. In Securitization of Islam: A Vicious Circle: Counter-Terrorism and Freedom of Religion in Central Asia (pp. 243-256).

Lewis, J. (2009). Sovereignty and the Role of Government in Cyberspace. Brown J. World Aff., 16, 55.

Lewis, J. A. (2014). National perceptions of cyber threats. Strategic Analysis, 38(4), 566-576.

Li, F., Lai, A., & Ddl, D. (2011, October). Evidence of advanced persistent threat: A case study of malware for political espionage. In *2011 6th International Conference on Malicious and Unwanted Software* (pp. 102-109). IEEE.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. Rand Corporation.

Limnéll, J. (2015). The exploitation of cyber domain as part of warfare: Russo-Ukrainian war. International Journal of Cyber-Security and Digital Forensics, 4(4), 521-533.

Lindstrom, G., & Luiijf, E. (2012). 2. Political aims & policy methods. Studies (Cambridge: Cambridge University Press, 2009), 136, 37.

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7-47.

Luhby, T. (2016). Estas son las razones de la derrota de Hillary Clinton. CNN. 09/10/2016, disponible en: https://cnnespanol.cnn.com/2016/11/09/estas-son-las-razones-de-la-derrota-de-hillary-clinton/

Luhmann, N. (1996). Introducción a la teoría de sistemas. Reís, 85(99), 315-367.

MacFarlane, N., & Sabanadze, N. (2013). Sovereignty and self-determination: Where are we? International Journal, 68(4), 609-627.

Mace, G., Thérien, J., & Gagné, S. (2012). Canada and the security of the Americas: Between old threats and new challenges. International Journal, 67(3), 603-622. Marchetti, R. (2009). Mapping Alternative Models of Global Politics. International Studies Review, 11(1), 133-156.

Maclean, J. (1988). Marxism and international relations: a strange case of mutual neglect. Millennium, 17(2), 295-319.

Magno-Texeira, R. (2021). Entrevista, realizada el 15 de julio de 2021

Maiquez, M. (2016) Donald Trump: una máquina populista de ofender en la recta final hacia la Casa Blanca. 20 Minutos, 04/11/2019, disponible en: https://www.20minutos.es/noticia/2767882/0/donald-trump-candidato-republicano-presidencia-eeuu/#xtor=AD-15&xts=467263

Mangan, D., y Calia, M. (2018) Special counsel Mueller: Russians conducted 'information warfare' against US during election to help Donald Trump win. CNBC News. Disponible en: https://www.cnbc.com/2018/02/16/russians-indicted-in-special-counsel-robert-muellers-probe.html

Marcin, T. (2019). James Comey on Hillary Clinton's emails: 'zero chance' she would be prosecuted based on the facts. Nesweek, disponible en: https://www.newsweek.com/james-comey-hillary-clinton-emails-zero-chance-prosecuted-1319270

Mardones, R. (2005). Doctrina de Seguridad Nacional: impacto y recomposición de la relación cívico-militar.

Martins, M. (2009). International Law as Glocal Law. Proceedings of the Annual Meeting (American Society of International Law), 103, 475-476.

Mars, A. (2017). La cadena rusa RT se registra como agente del Kremlin en Estados Unidos. El País. 13 de noviembre de 2017, disponible en: https://elpais.com/internacional/2017/11/13/estados_unidos/1510592734_479821.html

Mars, A. (2018). El exjefe del FBI obró mal en el caso de los correos de Clinton pero no fue partidista, según el departamento de Justicia. El País, 14/07/2018, disponible en: https://elpais.com/internacional/2018/06/14/actualidad/1528996202_698888.html

Mars, A. (2021). Empieza el segundo 'impeachment' a Trump: estas son las claves. El País, disponible: https://elpais.com/internacional/2021-02-08/empieza-el-segundo-impeachment-a-trump-estas-son-las-claves.html

Mascaro, L & Jalonick, M (2019a). Democrats impeachment charges say Trump betrayed the nation, AP NEWS.

Mascaro, L. & Jalonick, M. (2019b). Trump impeached on charges of abuse of power, obstruction, AP NEWS.

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). Stuxnet under the microscope. ESET LLC (September 2010).

Mayer, M., de Scalzi, N, Martino, L, Chiarugi, I (2013). International Politics in the Digital Age: Power Diffusion or Power Concentration? SISP CONFERENCE, University of Florence 12-14 September.

McCarthy, T., Swaine, J. & Jacobs, B. (2017) Former FBI head Robert Mueller to oversee Trump-Russia investigation. The Guardian. Disponible en: https://www.theguardian.com/us-news/2017/may/17/trump-russia-investigation-special-counsel-robert-mueller-fbi

McMillan, R. (2021). Hackers Lurked in SolarWinds Email System for at Least 9 Months, CEO Says, The New York Times, disponible en: https://www.wsj.com/articles/hackers-lurked-in-solarwinds-email-system-for-at-least-9-months-ceo-says-11612317963

McNeill, D. (2001). Embodying a Europe of the Cities: Geographies of Mayoral Leadership. Area, 33(4), 353-359.

McLuhan, M., & Powers, B. R. (2020). La aldea global: transformaciones en la vida y los medios de comunicación mundiales en el siglo XXI. Editorial Gedisa.

(MEAC) Ministry of Economic Affairs and Communications (2019). Cybersecurity Strategy: Republic of Estonia. Disponible en: https://bit.ly/37kwe0T

Medcalf, R. (2011). Diplomacia, transparencia y opinión pública. Política Exterior, 25(141), 114-121.

Mearsheimer, J. J. (1985). Conventional deterrence. Cornell University Press.

Mearsheimer, J. J. (2001). The tragedy of great power politics. WW Norton & Company.

(MFA) Minister of Foreign Affairs (2018). Working Worldwide for the Security of the Netherlands. Disponible en: https://bit.ly/2QxqLxK

Miller, L. (2018). Global order: values and power in international politics. Routledge.

Miller, M. (2021a). US intel agencies blame Russia for massive SolarWinds hack, The Hill, disponible en: https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack

Miller, M. (2021b). Senate Intelligence panel to hold hearing on SolarWinds breach next week. The Hill, disponible en: https://thehill.com/policy/cybersecurity/539444-senate-intelligence-panel-to-hold-hearing-on-solarwinds-breach-next-week

MITRE (2016). "PRE-ATT&CK – Model to Improve Cyber Threat Detection Before Adversaries Compromise Your Network (PR 16-3852)" and "PRE-ATT&CK Briefing (PR 16-4128)," The MITRE Corporation, McLean, VA, November 30, 2016. https://attack.mitre.org/

Morath, E. y Chaney, S. (2021). SolarWinds Hack Leaves Market-Sensitive Labor Data Intact, Scalia Says. The New York Times, disponible en: https://www.wsj.com/articles/solarwinds-hack-leaves-market-sensitive-labor-data-intact-scalia-says-11610627053?mod=tech_lead_pos4

Morawska, E. (2001). Structuring Migration: The Case of Polish Income-Seeking Travelers to the West. Theory and Society, 30(1), 47-80.

Morgan, S. (2017). Cybercrime Report. Cybersecurity Ventures. Arvutivõrgus: https://cybersecurityventures.com/2015wp/wpcontent/uploads/2017/10/2017Cybercrime-Report.pdf

Morgenthau, H. J. (2008). Politics Among Nations: The Struggle For Power and Peace Seventh Edition, revised. New York: McGraw Hill.

Moseley, A. (2011). Just war theory. The Encyclopedia of Peace Psychology.

Moses, J. (2013). Sovereignty as irresponsibility? A Realist critique of the Responsibility to Protect. Review of International Studies, 39(1), 113-135.

(MSJ) Ministry of Security and Justice (2017). The National Cyber Security Strategy (NCSS). Disponible en: https://bit.ly/2QBJE2y

(MTMAC) Ministry of Transport Maritime Affaris and Communications (2016). National Cyber Security Strategy 2016-2019. Disponible en: https://bit.ly/37fCZ45

Mueller, R. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. U.S. Department of Justice, disponible en: https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf

Murphy, S. (2012). Was our interview with Anonymous hacker an FBI set-up?.

Nakashima, N. (2016). U.S. government officially accuses Russia of hacking campaign to interfere with elections. The Washington Post, 07/10/2016, disponible en: https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.6516636a3888b

Navari, C. (2018). The National Interest and the 'Great Debate'. In Hans J. Morgenthau and the American Experience (pp. 75-93). Palgrave Macmillan, Cham.

Nazeri, H. (1996). Imagined Cyber Communities, Iranians and the Internet. Middle East Studies Association Bulletin, 30(2), 158-164.

(NCD) National Cyber Directorate (2017). Israel National Cyber Security Strategy in Brief. Disponible en: https://bit.ly/2pDIKHS

NCSCA Pakistan (2014). National Cyber Security Council Act. Disponible en: https://bit.ly/2DHvNQt

NCS Afganistan (2017). National Cyber Security Strategy of Afghanistan. Islamic Republic of Afghanistan Ministry of Communications and IT. Disponible en: https://bit.ly/2DDTMQF

NCS Chile (2017). Política Nacional De Ciberseguridad. Gobierno de Chile, disponible en: https://bit.ly/2rQ70Hc

NSS Egypt (2017). National Cybersecurity Strategy 2017-2021. Cybersecurity Council, disponible en: https://bit.ly/361mcQz

NCSI (2018). National Cyber Security Index. E-Governance Academy, disponible en: https://bit.ly/2XS1eAR

Newmeyer, P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), 9-19.

Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. Cal. L. Rev., 101, 1079.

NIST (2012). Computer Security Incident Handling Guide. NIST Special Publication, disponible en: https://bit.ly/2Yb3jIf

Nitti, R. (2017) Robert Mueller employs powerful weapong in Trump-Russia investigation: The IRS. Forbes. Disponible en: https://www.forbes.com/sites/anthonynitti/2017/09/01/robert-mueller-employs-powerful-weapon-in-trump-russia-investigation-the-irs/?sh=76053abf75ac

Nugroho, G. (2008). Constructivism and international relations theories. Global & Strategis, 2(1), 85-98.

Nye, Joshep. 2010. “Cyber power.” Cambridge: Harvard University Press.

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Commission on Internet Governance.

OCDE (2013). Strategic Crisis Management. Disponible en: https://bit.ly/35THoYX

ODNI (2017). “The Cyber Threat Framework.” Disponible en: https://bit.ly/35Dcfsp

OMG (2014). “UML Operational Threat & Risk Model Request for Proposal.” Disponible en: https://bit.ly/2Dn7ZBi

OSCE. (2009). The OSCE Concept of Comprehensive and Cooperative Security: An Overview of Major Milestones. Organization for Security and Co-operation in Europe.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In Proceedings of the 7th European Conference on Information Warfare (p. 163).

Ozturk, I. (2013). Energy Dependency and Energy Security: The Role of Energy Efficiency and Renewable Energy Sources. The Pakistan Development Review, 52(4), 309-330. Retrieved from http://www.jstor.org/stable/24397894

Palfrey, J. (2010). Four Phases of Internet Regulation. Social Research, 77(3), 981-996.

Palma, S. (2021). Entrevista, realizada el 14 de septiembre de 2021

PBS: PBS. (2018). Mueller's Russia probe by the numbers. PBS. https://www.pbs.org/newshour/politics/muellers-russia-probe-by-the-numbers

Pereda, C. (2016). El vídeo machista de Donald Trump quiebra la campaña republicana. El País, disponible en: https://elpais.com/internacional/2016/10/08/estados_unidos/1475946885_014850.html

Panettieri, J. (2020a). State Sponsored Hackers Steal Fire Eye Red Team Security Testing Tools, MSSP Alert, disponible en: https://www.msspalert.com/cybersecurity-breaches-and-attacks/hackers-steal-fireeye-red-team-security-testing-tools/

Panettieri, J. (2020b). Solarwinds orion vulnerability investigation. , MSSP Alert, disponible en: https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation/

Panettieri, J. (2021). Russia hacked DHS email, MSSP Alert, disponible en: https://www.msspalert.com/cybersecurity-markets/americas/russia-hacked-dhs-emails/

Parraguez, M. (2021). Entrevista, realizada el 01 de agosto de 2021.

Pardo, P. (2021). La Cámara de Representantes aprueba el segundo 'impeachment' a Donald Trump con el apoyo de diez republicanos. El Mundo, disponible en: https://www.elmundo.es/internacional/2021/01/13/5ffec35efc6c835e5e8b4664.html

Parraguez, L., Stockton, P y Houle, G. (2021). Cybersecurity and Critical Infrastructure Resilience in North America. Wilson Center & Harvad Kennedy School. Disponible en: https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Cyber%20Security%20and%20Critical%20Infrastructure%20in%20North%20America.pdf

Pauli-Medeiros, B. y Goldoni, L. (2020). The Fundamental Conceptual Trinity of Cyberspace. Contexto Internacional, 42, 31-54.

Pauli-Medeiros, B. (2021). Entrevista, realizada el 12 de julio de 2021

Peck, J. & Tickell, A. (1994) 'Searching for a new institutional fix: the after-Fordist crisis and the global-local disorder', in Ash Amin (ed.) Post- Fordism: A Reader, Cambridge, Mass.: Blackwell, pp. 280-315.

Peters, J. (2005). A "Bridge over Chaos": "De Jure Belli", "Paradise Lost", Terror, Sovereignty, Globalism, and the Modern Law of Nations. Comparative Literature, 57(4), 273-293.

Pendergrass, S. (2012). Hackers gone wild: the 2011 spring break of lulzsec. Issues in Information Systems, 13(1), 133-143.

Pessiri, P. (2019). “2018: A Year of Cyber Attacks” Hackmageddon, 15 de enero de 2019. https://bit.ly/2Da7k7d

Petallides, C. J. (2012). Cyber terrorism and IR Theory: realism, liberalism, and constructivism in the new security threat. Inquiries Journal, 4(03).

Piore, A. (2019). Russia Is Using Cold War Strategy to Undermine the Faith of Americans in the 2020 Election—Will It Work? NewsWeek, 07/23/2019, disponible en: https://www.newsweek.com/2019/08/02/elections-2020-will-take-place-cyber-battleground-that-puts-us-disadvantage-says-expert-1450351.html

Polantz, K. (2018) Rick Gates continues to help Mueller investigation, lawyer says. CNN Politics. https://edition.cnn.com/2018/10/11/politics/gates-robert-mueller/index.html

Poulsen, K., McMillan, R. y Volz, D. (2020). SolarWinds Hack Victims: From Tech Companies to a Hospital and University. The New York Times, disponible en: https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?mod=tech_lead_pos1

Preda, C (2017) ¿Qué poderes y funciones tiene el fiscal especial que investiga a Donald Trump?, El País, disponible en: https://elpais.com/internacional/2017/05/18/estados_unidos/1495130718_546693.html

(PG España) Presidencia del Gobierno (2013). Estrategia de Ciberseguridad Nacional. Disponible en: https://bit.ly/344VXbv

Quackenbush, S. (2011). Deterrence theory: Where do we stand? *Review of International Studies*, *37*(2), 741-762.

Ramakrishna, S. (2021). New Findings From Our Investigation of SUNBURST. Orange Matter, disponible en: https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Regnum News (2007). Estonian prime minister: Drunken looters are buried under the Bronze Soldier Monument. [En Línea] disponible en: https://web.archive.org/web/20120224090707/http://www.regnum.ru/english/817953.html

Reuters (2017). Republicans seek special counsel's removal from Russia probe. Reuters. Disponible en: https://www.reuters.com/article/us-usa-trump-russia-congress/u-s-republicans-seek-special-counsels-removal-from-russia-probe-idUSKBN1D31W8

Reuters (2020). U.S. Treasury has not seen any damage from widespread hack-CNBC. Reutersm disponible en: https://www.reuters.com/article/us-usa-cyber-breach-treasury/u-s-treasury-has-not-seen-any-damage-from-widespread-hack-cnbc-idUSKBN28V1X0

Reuters (2021). U.S. House committees to hold Feb 26 hearing on 'SolarWinds' hack, Reuters, disponible en: https://www.reuters.com/article/us-usa-cyber-solarwinds/u-s-house-committees-to-hold-feb-26-hearing-on-solarwinds-hack-idUSKBN2AM233

Rice, C. (2000). Promoting the national interest. Foreign Aff., 79, 45.

Rodriguez, J., y Jin, B. (2018) The Mueller indictments so far: lies, trolls and hacks. Politico. https://www.politico.com/interactives/2018/interactive_mueller-indictments-russia-cohen-manafort/

Rivas, P., & Rodríguez, M. (2010). Autoritarismo, totalitarismo y doctrina de seguridad nacional. Espacios Públicos, 13(29), 99-118.

Robinson, T. W., & Shambaugh, D. L. (Eds.). (1995). Chinese foreign policy: theory and practice. Oxford University Press.

Roth, A & Borger, J (2021). Biden hits Russia with new sanctions in response to election meddling, The Guardian, disponible en: https://www.theguardian.com/world/2021/apr/15/joe-biden-russia-sanctions-election-interference-hacking

Russett, B. M., Oneal, J. R., & Cox, M. (2000). Clash of civilizations, or realism and liberalism déjà vu? Some evidence. Journal of Peace Research, 37(5), 583-608.

Saavedra, B. (2021). Entrevista, realizada el 15 de agosto de 2021.

Samaan, J. L. (2010). Cyber command: The rift in US military cyber-strategy. The RUSI Journal, 155(6), 16-21.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. URVIO. Revista Latinoamericana de Estudios de Seguridad, (20), 8-15.

Sancho, C. (2021). Entrevista, realizada el 01 de julio de 2021

Sassen, S. (2000). The Need to Distinguish Denationalized and Postnational. Indiana Journal of Global Legal Studies, 7(2), 575-584

Sahuquillo, M. (2020). Anatomía del gran ciberataque que ha comprometido el corazón de la Administración de EE UU, *El País*, disponible en: https://elpais.com/internacional/2020-12-27/anatomia-del-gran-hackeo-que-ha-comprometido-el-corazon-de-la-administracion-de-eeuu.html

Schia, N., & Gjesvik, L. (2017). China's cyber sovereignty. Norwegian Institute of International Affairs, www. jstor. org/stable/resrep07952.

Schmidt, S. (2011). To Order the Minds of Scholars: The Discourse of the Peace of Westphalia in International Relations Literature. International Studies Quarterly, 55(3), 601-623.

Schmidt, A. (2013). The estonian cyberattacks. The fierce domain–conflicts in cyberspace, (1986-2012).

Schmidt, M. (2015). Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules. The New York Times, 02/03/2015, disponible en: https://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html?_r=0

Schmidth, M. (2017) Comey memo says Trump asked him to end Flynn investigation. The New York Times.

Scheuerman, W. E. (2009). Hans Morgenthau: realism and beyond.

Sicherheitstacho (2019). Overview of Current Cyber Attacks. Deutsche Telekom, disponible en: https://bit.ly/2OeLLGH

Siddiqui, S (2019) Mueller´s testimony on Trump and Russia: The biggest takeaways, The Guardian, disponible en: https://www.theguardian.com/us-news/2019/jul/24/robert-mueller-testimony-key-takeaways-exoneration-indictment

Serianu (2020). Africa Cybersecurity Report. Disponible en: https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

Shaban, H. (2018). Twitter suspends Guccifer and DCLeaks after Mueller links them to Russian hacking operation. The Washington Post. 16/07/2018, disponible en: https://www.washingtonpost.com/technology/2018/07/16/twitter-suspends-guccifer-dcleaks-after-mueller-links-them-russian-hacking-operation/?utm_term=.3f7cd2b1b487

Sheldon, J. (2012). "Deciphering Cyberpower: Strategic Purpose in Peace and War." Strategic Studies Quarterly, vol. 5, no. 2, 2011, pp. 95–112.

Shevel, O. (2009). The Politics of Citizenship Policy in New States. Comparative Politics, 41(3), 273-291.

Sidaway, J. (2006). On the Nature of the Beast: Re-Charting Political Geographies of the European Union. Geografiska Annaler. Series B, Human Geography, 88(1), 1-14.

Singer, P. y Friedman, A. (2014) Ciber Security and Ciber War. Oxford. Reino Unido. Oxford University Press, 321 pág.

Sklenka, S. D. (2007). Strategy, National Interests, and means to an end. Army War Coll Strategic Studies Inst Carlisle Barracks Pa.

Smith, A. (2015). La riqueza de las naciones (Vol. 2188). NoBooks Editorial.

SolarWinds (2020). SolarWinds Corporation (SWI) - FORM 8-K | Current report, SolarWinds, disponible en: https://seekingalpha.com/filing/5276758

Sørensen, G. (2009). Big and Important Things' in IR: Structural Realism and the Neglect of Changes in Statehood. International Relations, 23(2), 223-239.

Sotomayor, M. (2016). FBI Director Has High Expectations for New Cyber Security Agents. NBC News, 20/08/2016, disponible en: https://www.nbcnews.com/news/us-news/fbi-director-has-high-expectations-applicants-n640316

Space (pp. 17-42). Santa Monica, CA; Washington, DC; Pittsburgh, PA; New Orleans, LA; Jackson, MS, Boston, MA; Doha, QA; Cambridge, UK; Brussels, BE: Rand Corporation.

Sputnik (2007). Estonian government cuts up WWII memorial. Sputnik Disponible en: https://sputniknews.com/world/2007042764546318/

Stahn, C. (2007). Responsibility to protect: Political rhetoric or emerging legal norm?. American Journal of International Law, 101(1), 99-120. Stacy, H. (2003). Relational Sovereignty. Stanford Law Review, 55(5), 2029-2059.

Starr, S. H. (2009). Toward a preliminary theory of cyberpower. Cyberpower and national security, 43-88.

Stern, P. (2011). Design principles for global commons: Natural resources and emerging technologies. International Journal of the Commons, 5(2), 213-232.

Stracqualursi, V. (2016). Key Moments of the 2016 Election. ABC News, disponible en: https://abcnews.go.com/Politics/key-moments-2016-election/story?id=43289663

Stubs, J. (2021). SolarWinds hackers linked to known Russian spying tools, investigators say, Reuters, disponible en: https://www.reuters.com/business/media-telecom/solarwinds-hackers-linked-known-russian-spying-tools-investigators-say-2021-01-11/

Submarine Cable Maps (2018). Hauwei Submarine Cable Maps. Disponible en: https://www.submarinecablemap.com/#/

SudOuest. (2019). Russiagate, affaire ukrainienne: ces deux scandales d'Etat qui visent Donald Trump. SudOuest, disponible en: https://www.sudouest.fr/international/russiagate-affaire-ukrainienne-ces-deux-scandales-d-etat-qui-visent-donald-trump-2459292.php

Symantec (2016) Cybercrime & cyber security trends in Africa. Disponible en: https://docs.broadcom.com/doc/cyber-security-trends-report-africa-interactive-en

Sunderman, A. (2021). White House names SolarWinds response leader amid criticism, Associated Press, disponible: https://apnews.com/article/technology-politics-national-security-hacking-software-88156917ce76d9bef227dd55ee1995de

Tabansky, L. (2011). Basic concepts in cyber warfare. Military and Strategic Affairs, 3(1), 75-92.

Take, I. (2012). Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS. Regulation & Governance, 6(4), 499-523.

Tamanes, J. (2019). Russiangate: los medios fracasan como contrapeso a Trump. Política Exterior, disponible en: https://www.politicaexterior.com/russiagate-los-medios-fracasan-contrapeso-trump/

Tang, M., & Huhe, N. (2014). Alternative framing: The effect of the Internet on political support in authoritarian China. International Political Science Review / Revue Internationale De Science Politique, 35(5), 559-576.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network security, 2011(8), 16-19.

Tarzi, S. (2014). The folly of a grand strategy of coercive global primacy: a fresh perspective on the post-9/11 bush doctrine. International Journal on World Peace, 31(3), 27-52.

Taylor, P. J. (1996). Embedded statism and the social sciences: opening up to new spaces. Environment and Planning A, 28, 1917-1928.

Taylor, D., y Morris, S. (2018). Who has Mueller charged in the Trump-Russia Inquiry and who might be next?. The Guardian, disponible en: https://www.theguardian.com/us-news/ng-interactive/2018/dec/05/robert-mueller-who-charged-list-trump-russia-inquiry-latest-indictments-flynn-manafort-cohen-what-happens-next

The Guardian (2020) Trump impeachment: president acquitted on both articles, disponible: https://www.theguardian.com/us-news/2020/feb/05/donald-trump-acquitted-senate-impeachment-trial

The New Daily. (2020). Ex FBI lawyer charged with doctoring Russiagate "evidence" against Trump advisor. The New Daily, disponible en: https://thenewdaily.com.au/news/world/us-news/trump-news/2020/08/15/fbi-lawer-charged-russiagate/amp/

The New York Times. (2020a). Prosecutors Recommend Roger Stone Receive Up to 9 Years in Prison. The NY Times, disponible en: https://www.nytimes.com/2020/02/10/us/roger-stone-prison-sentence.html?searchResultPosition=175

The New York Times (2020b). FireEye and SolarWind Russia Hack, New York Times, disponible en: https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html

The New York Post. (2020c). The FBI's "Russiagate" search-and-destroy mission against Team Trump. NY Post, disponible en: The FBI's 'Russiagate' search-and-destroy mission against Team Trump (nypost.com)

The Washington Post: Helderman, R., Hamburger, T., Barret, D., Zapotosky, M., & Esteban, C. (2018) What its Mueller looking at? The Washington Post. Disponible en: https://www.washingtonpost.com/graphics/2018/politics/mueller-russia-probe/

The Washington Post (2021). Biden Russia sanctions Solarwinds Hacks, The Washington Post, disponible en: https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html?source=content_type%3Areact%7Cfirst_level_url%3Anews%7Csection%3Amain_content%7Cbutton%3Abody_link

TIME (2007). Estonians Under Siege in Moscow. TIME. Disponible en: http://content.time.com/time/world/article/0,8599,1616943,00.html

Tkacheva, O., Schwartz, L., Libicki, M., Taylor, J., Martini, J., & Baxter, C. (2013). The Internet and Political Process in Different Regimes. In Internet Freedom and Political

Tomasky, M. (2015). Trump. The New York Review of Book, disponible en: https://www.nybooks.com/articles/2015/09/24/trump/

Triandafillov, V. (2013). The nature of the operations of modern armies. Routledge.

Tucker, E. (2020). Senator: Treasury Dept. email accounts compromised in hack. Associated Press, disponible en: https://apnews.com/article/technology-politics-ron-wyden-russia-hacking-572ac201e8f365cf6ec218b478742aa0

Tucker, E. (2021). Hackers targeted SolarWinds earlier than previously known. Associated Press, disponible en: https://apnews.com/article/hacking-business-technology-government-and-politics-b221968496ed498457ab56aae7970c90

Tulchin, J., Benítez, R., & Diamint, C. (Eds.). (2006). El rompecabezas: conformando la seguridad hemisférica en el siglo XXI. Prometeo.

UK Cabinet Office (2011). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. Disponible en: https://bit.ly/2py0Vyt

UNDP (1994). Human Development Report 1994. New Dimensions of Human Security. Oxford and New York: Oxford University Press

US Cyber Command (2022). US Cybber Command Structure, disponible en: https://www.cybercom.mil/Components/

US Deparment State (2020). "Major Non-NATO Ally Status", 30 January: https://www.state.gov/major-non-nato-ally-status/

Varacalli, T. F. (2016). National interest and moral responsibility in the political thought of Admiral Alfred Thayer Mahan. Naval War College Review, 69(2), 108-128.

Van Creveld, M. (1991). The transformation of war: the most radical reinterpretation of armed conflict since Clausewitz.

Van Creveld, M. (2002). The transformation of war revisited. Small Wars and Insurgencies, 13(2), 3-15.

Van Dyke, V. (1962). Values and interests. The American Political Science Review, 56(3), 567-576.

Van de Haar, E. (2009). Classical liberalism and international relations theory: Hume, Smith, Mises, and Hayek. Springer.

Van Vugt, C.(2015). The National Security Doctrine of the United States: A Comparison of the Truman and George W. Bush Foreign Policy Doctrines.

Van Wijk, J., & Bolhuis, M. (2017). Awareness Trainings and Detecting Jihadists among Asylum Seekers: A Case Study from The Netherlands. Perspectives on Terrorism, 11(4), 39-49.

Vilardo, C. F. (2021). Las sociedades a través del tiempo según los medios. El legado de Marshall McLuhan: de la civilización preimprenta a la percepción multisensorial.

Vitkovskaya, J., Granados, S., Uhrmacher, K. & Williams, A. (2017). Who was charged in the Mueller Probe, and why. The Washington Post. Disponible en:

https://www.washingtonpost.com/graphics/2017/national/robert-mueller-special-counsel-indictments-timeline/

Volz y McMillan (2020). Suspected Russian Hack Said to Have Gone Undetected for Months, Wall Street Journal, disponible en: https://www.wsj.com/articles/suspected-russian-hack-said-to-have-gone-undetected-for-months-11607974376?mod=tech_lead_pos3

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Waltz, K. (2004). Neorealism: Confusions and criticisms. Journal of Politics and Society, 15(1), 2-6

Waltz, K. N. (2010). Theory of international politics. Waveland Press.

Wang, P., & Johnson, C. (2018). Cybersecurity Incident Handling: A Case Study Of The Equifax Data Breach. Issues in Information Systems, 19(3).

Warf, B. (2015). The Hermit Kingdom in cyberspace: unveiling the North Korean internet. Information, Communication & Society, 18(1), 109-120.

Waver, O. (2012). Thinking international relations differently (pp. 92-114). A. B. Tickner, & D. L. Blaney (Eds.). London: Routledge.

Weber, E. (2007). Globalization, "Glocal" Development, and Teachers' Work: A Research Agenda. Review of Educational Research, 77(3), 279-309.

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. *Minn. J. Int'l L.*, *22*, 347

Wendt, A. E. (1987). The agent-structure problem in international relations theory. International organization, 41(3), 335-370.

Wight, M. (2002). Power politics. A&C Black.

Winseck, D. (2017). The Geopolitical Economy of the Global Internet Infrastructure. Journal of Information Policy, 7, 228-267.

White, E. (2020). Senators want answers regarding SolarWinds cyber attack, Federal News Networks, disponible en: https://federalnewsnetwork.com/federal-newscast/2020/12/senators-want-answers-regarding-solarwinds-cyber-attack/

Williams, D. (2012). The World Bank and social transformation in international politics: liberalism, governance and sovereignty. Routledge.

Wimmstedt, S. (2020). The “G” Race: Sino-US tensions over 5G, International Relations in Cyberspace and the relevance of Realism.

Wolfe, J (2019) How Trump's impeachment trial would differ from a criminal one

Ximénez, P. (2016). Correos de Clinton filtrados revelan supuestas contradicciones en su campaña. El País, disponible en: https://elpais.com/internacional/2016/10/11/actualidad/1476215767_085445.html

Yanakiev, Y. (2019). The Process Of Evaluation Of National Interests As The Basis For Security Policy-Making And Strategy Development. 36 vol. XIX.

Yang, J. (2013). Post-Lulzsec Cybersecurity. Insight and Inquiry, 6(1), 46-64.

Yang, J. Y., Kim, S. J., & Oh, I. S. (2016, August). Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities. In *International Workshop on Information Security Applications* (pp. 102-111). Springer, Cham.

Yergin, D. (2006). Ensuring Energy Security. Foreign Affairs,85(2), 69-82. doi:10.2307/20031912

Yingfa, S. y Hongna, M. (2014). Implications for E-Media, the Press, Government, and Politics in China. In De Landtsheer C., Farnen R., German D., Dekker H., Sünker H., Song Y., et al. (Eds.), E-Political Socialization, the Press and Politics: The Media and Government in the USA, Europe and China (pp. 341-362). Frankfurt am Main: Peter Lang AG.

Yizhou, W. (2002). Rethinking National Interests [J]. Social Sciences In China, 2.

Zittrain, J., & Palfrey, J. G. (2007). Access denied: the practice and policy of global Internet filtering. Oxford Internet Institute.

Zurcher, A. (2017). Trump-Russia Inquiry: Why Attacks on Robert Mueller are mounting. BBC NEWS disponible en: https://www.bbc.com/news/world-us-canada-42372603

Anexo 1. Guía de entrevista semiestructurada.

Estimado Expert@,

El fin de esta entrevista es recopilar información que apoye a la investigación de tesis del Mtro. Juan Manuel Aguilar Antonio, alumno del doctorado en Relaciones Internacionales de la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México (UNAM), con título **"Ciberseguridad en enfoque teórico y analítico para la seguridad nacional y la política exterior."**

Se propone que la dinámica sea la siguiente:

- La entrevista se realizará vía Zoom en una fecha pactada con anticipación entre Usted y el doctorante.
- El objetivo es recuperar sus comentarios de forma verbal sobre los temas que se tocan en las guías de entrevistas adjuntas.
- La entrevista completa tendrá una duración de máximo 90 minutos.
- En virtud de que esta entrevista es únicamente con propósitos académicos y se procesará de manera ética.
- En caso de no existir inconveniente, esta entrevista será grabada para facilitar su posterior análisis.

Preguntas

1. La soberanía es un tema que está a debate en el dominio del ciberespacio, ¿considera que existe la soberanía en el ciberespacio?
2. ¿Considera que la soberanía de un Estado-Nación puede ser vulnerada desde el ciberespacio? Cite algún ejemplo con base a su argumento.
3. ¿Considera que la manipulación de información e influencia de las personas en procesos políticos a través de internet consiste en una afectación a la estabilidad del Estado-Nación?
4. En años recientes los sistemas electorales están sujetos en su operación a sistemas informáticos. Esto representa una gran responsabilidad por parte de los Estados-Nación, ¿considera que los sistemas electorales deben ser parte de la infraestructura crítica de un país?
5. Si un país hackeara el sistema electoral de México o manipulara a su electorado vía operaciones en el ciberespacio, ¿considera esto afecta la soberanía del Estado-Nación?

6. Un hackeo o ciber ataque a un sistema electoral de México, ¿considera sería una agresión a la soberanía nacional de México como Estado-Nación?