UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE ECONOMÍA Y RELACIONES INTERNACIONALES

PROGRAMA DE DOCTORADO EN ESTUDIOS DEL DESARROLLO GLOBAL

TESIS:

"EL EFECTO DE LA CIBERSEGURIDAD SOBRE LAS FORMAS DE PARTICIPACIÓN ESTATAL EN EL CIBERESPACIO"

PARA OBTENER EL GRADO DE:
DOCTOR EN ESTUDIOS DEL DESARROLLO GLOBAL

PRESENTA:
GERMÁN ALEJANDRO PATIÑO OROZCO

DIRECTOR DE TESIS:
DR. SANTOS LÓPEZ LEYVA

Tijuana, Baja California, octubre del 2019

Para Carmen, Germán, Paola, Karen, Erick y Sandra.
Gracias por enseñarme la más grande lección de vida,
que el amor y el cariño pueden trascender el tiempo y el espacio.

Agradecimientos

En primer lugar, agradezco a mi madre y mi padre por su apoyo incondicional, constante y por las innumerables enseñanzas de vida que me han brindado. Agradezco a mis hermanas Paola, Karen y mi hermano Erick quienes son una fuente constante de inspiración, cariño y alegría, especialmente durante los momentos más complejos de este proceso. También agradezco a Sandra Gómez Muñoz quien ha sido aliada, confidente y parte fundamental en esta fase de mi vida.

Asimismo, agradezco al CONACYT y a la Universidad Autónoma de Baja California por ayudarme con su apoyo material e institucional para cumplir con mi educación profesional. Agradezco en particular a mi asesor, el Dr. Santos López Leyva por su retroalimentación puntual, eficaz y asertiva. Además, agradezco a mis sinodales, por su tiempo y esfuerzo, Dr. Daniel Efrén Morales Ruvalcaba, Dr. José de Jesús López Almejo, Dr. Rafael Velázquez Flores y Dr. Luis Alfredo Ávila López, porque con sus observaciones y comentarios permitieron que este trabajo se consolidara y ejecutara de mejor manera. No obstante, cualquier omisión o falla es única y exclusivamente mi responsabilidad.

Agradezco en especial al Dr. Jesús López por su amistad, su apoyo, lecciones de vida y múltiples consejos profesionales y personales. También agradezco al Dr. Daniel Morales por su ayuda invaluable durante mi estancia de investigación en la Universidad Sun Yat-sen en la República Popular de China. Gracias por tu generosidad, amistad, sus observaciones y recomendaciones en lo profesional y personal.

De la misma manera, agradezco a todas y cada una de las personas que me acompañaron en diversos momentos de este proceso, nombrarle a cada uno sería imposible, pero todos han contribuido de manera directa e indirecta en este proceso profesional y personal. Por último, agradezco a esas personas que han sido parte fundamental de mi vida, pero que por razones naturales se han adelantado en el camino, no obstante, han dejado una huella profunda de mi vida, y por ello seguiré agradecido.

Introducción

En la segunda década del siglo XXI, la utilización del ciberespacio ha alcanzado un punto que abarca un amplio espectro de actividades políticas, económicas, sociales, culturales, estratégicas y de seguridad. En razón de esto, ha permitido el desarrollo y despegue de acciones como el crecimiento de empresas electrónicas, medios sociales digitales, nuevas formas de organización social, laboral y personal e interconectar prácticamente cualquier objeto, esto en gran medida, permitido por el mejoramiento de las magnitudes de almacenamiento, distribución y capacidad de transmisión de la información.

Sin embargo, así como el espacio digital ha posibilitado grandes cambios positivos también ha traído aparejadas transformaciones pavorosas. Por ejemplo, el crecimiento de intrusiones informáticas, fraude electrónico, robo de identidad, lavado de dinero, registro falso de nombres de dominio, espionaje, robo de secretos comerciales desarrollo de mecanismos de vigilancia más sofisticados que socavan la privacidad, uso de dispositivos de identificación biométrica en forma indiscriminada, perfeccionamiento de *software* malicioso persistente, mecanismos de filtrados de información que minan la libertad de deliberación, desarrollo de códigos informáticos con fines militares ofensivos, nuevas formas de modificar las acciones o elecciones políticas en otras jurisdicciones a través del perfilamiento de alternativas de acción disponibles, entre otros.

De allí se ha desprendido una cantidad de debates sobre las características particulares del ciberespacio como un lugar de oportunidades y de riesgos, ya que una amplia gama de agentes lo utilizan con diferentes propósitos y distintas intenciones. En suma, la amplitud del ciberespacio permite una extensión de acciones de distinta índole que puede ser sumamente extensa y variada. Por ello, la discusión y el debate se han vuelto sumamente complejos, pues lo que sucede en el ciberespacio permea en cada una de las acciones de la agencia humana. Esto se ha extensivo al momento de observar los datos que componen el ciberespacio.

Por ende, es clave conocer el panorama general de los problemas del ciberespacio, en particular, de la ciberseguridad. Cabe resaltar que cualquier cifra o

estadística presentada sobre desarrollo tecnológico debe evaluarse con cautela, pues está el riesgo de que al momento de presentarla pueda estar quedando obsoleta. Además, las metodologías de medición de datos presentan una heterogeneidad amplia. Aunque, se está consciente de esta incertidumbre, no es necesario rechazar *a priori* datos que pueden perfilar un panorama general sobre un fenómeno incipiente que, además, florece de manera vertiginosa.

Ciertamente, el significado que ha tenido la interconectividad para la productividad y para el desarrollo de intercambios comerciales y financieros es ampliamente reconocido. Precisamente, avances tecnológicos como el comercio electrónico, los pagos y transferencias electrónicas, el almacenamiento en nube, el análisis de grandes datos (*Big Data*), la Internet de las Cosas y el aprendizaje automático son factores fundamentales para el crecimiento del comercial global, pero también han llevado a aumentar la superficie de incidencia de agresiones, transgresiones o actividades nefarias cibernéticas. (Ponemon Institute, 2017).

En este sentido, algunas firmas especializadas en ciberseguridad como CISCO y Cybersecurity Ventures han observado que la actividad criminal cibernética puede convertirse en una de las problemáticas más grandes de la humanidad en las siguientes dos décadas (CISCO/Cybersecurity Ventures, 2019). Con base en esto, calculan que su rápido crecimiento en tamaño y sofisticación puede representar un costo acumulado global de más de $6 billones de dólares en pérdidas para el 2021 (CISCO/Cybersecurity Ventures, 2019). A partir de ello, en 2017, a nivel mundial el crimen cibernético representó un gasto de más del 23% a las empresas en relación con el 2016 (Accenture & Polemon Institutte, 2017). Como consecuencia, de 2016 a 2017, el incremento en soluciones de ciberseguridad empresarial aumentó en un 22 por ciento (Accenture & Polemon Institutte, 2017). En este contexto, las industrias más lastimadas en los últimos años son la de salud, manufactura, servicios financieros, transporte y gobierno. Sin embargo, algunos estudios prospectivos recalcan que de 2019 a 2022 serán la industria minorista, energética, de medios de comunicación, entretenimiento y educación las que sufran más afectaciones por alguna acción cibernética agresiva (CISCO/Cybersecurity Ventures, 2019).

Bajo estas circunstancias, las compañías que más invierten en cuestiones de soluciones de ciberseguridad se encuentran en el sector financiero (Accenture & Polemon Institutte, 2017). Sin embargo, la industria de la salud es la que recibe más transgresiones cibernéticas (Morgan, 2017). Con respecto a estas evidencias, se puede vislumbrar tanto una problemática que puede trastocar el desarrollo económico global y un fuerte interés de las firmas de ciberseguridad de enmarcar el fenómeno como un riesgo que solamente ellas pueden resolver. Cabe resaltar que, durante el año 2017, el costo promedio para solucionar un ataque cibernético fue de $2.4 millones de dólares. (Accenture & Polemon Institutte, 2017), y el tiempo promedio de solución fue de 50 días (Accenture & Polemon Institutte, 2017). No obstante, un porcentaje considerable de empresas a nivel mundial considera que los riesgos de seguridad informática han ido creciendo (Ponemon Institute, 2017).

En efecto, el mercado de ciberseguridad aumentó su valor de mercado en aproximadamente 35 veces durante el período 2004-2017, es decir, de contar con una estimación global de $3.5 mil millones de dólares en 2004, la cotización del mercado de ciberseguridad aumentó hasta $120 mil millones de dólares para 2017 (CISCO/Cybersecurity Ventures, 2019). Sin embargo, la dificultad se produce al momento de sopesar estas cifras y tratar de precisar en qué dimensión se encuentra la problemática que aqueja el funcionamiento económico del ciberespacio.

Por otro lado, en cuanto al aspecto social del ciberespacio, el más perceptible para la mayoría de personas, se relaciona fuertemente con la manera de crear, almacenar, modificar, intercambiar y aprovechar el contenido de datos y con su crecimiento exponencial. Algunas de sus manifestaciones más perceptibles son las siguientes: por ejemplo, para marzo de 2019, en un minuto se generaban 3.8 millones búsquedas en Google, se escribían 87,500 de tuits, se llevaban a cabo más de 1 millón de actualizaciones de Facebook, se desplazaban por el contenido de Instagram 347,222 personas, se visualizaron el equivalente a 694,444 horas de contenido en Netflix, se visualizaban 4.5 millones de horas de video en YouTube, se enviaron más 59.7 millones de mensajes instantáneos y se descargan 390 mil aplicaciones y se crearon más de 188 millones de correos electrónicos (Desjardins, 2019). Por una parte, cabe subrayar que es una amplia fracción del uso social

digital, pero no es la totalidad, puesto que, esta perspectiva deja de lado el uso social del ciberespacio en otras latitudes geográficas que cuentan con aplicaciones afines a las mencionadas. De igual manera, significa y expresa la gran relevancia que el entorno cibernético ejerce y despliega sobre la sociedad actual.

Por otra parte, en relación con las implicaciones para la protección del contenido y los datos que transitan en estos usos sociales, esto se traduce en una superficie amplia de vectores de vulnerabilidad y riesgo. En otras palabras, esto se vincula con nuevas amenazas que surgen día con día y con las prácticas individuales para mantener la confidencialidad, integridad y disponibilidad de los datos. Por ejemplo, un 21 por ciento de todos los archivos globales no cuentan con algún tipo de protección (Varonis Data Lab, 2018). Al mismo tiempo, durante 2017 1 de cada 13 búsquedas conducían a un programa o página contaminada (*malware*) (Symantec, 2018). Para ello, el correo electrónico fue el vehículo más utilizado para realizar algún tipo de estafa electrónica (Symantec, 2018). Asimismo, las variantes de código malicioso para dispositivos móviles aumentaron en un 54 por ciento en 2017 para diferentes sistemas operativos (Symantec, 2018).[1] Además, en ese mismo año, cada día fueron bloqueadas alrededor de 24 mil aplicaciones para dispositivos móviles con algún tipo de código malicioso (Sobers, 2019).

En razón de esto, se estima que problemáticas relacionadas son el secuestro de datos, con el desarrollo de vulnerabilidades sistemáticas llamadas 'día cero' o los ataques distribuidos de denegación de servicio seguirán en crecimiento.[2] Generalmente estas actividades se presentan ya sea en países con un gran número de interconexiones informáticas o que cuenten con capacidades poco eficientes para hacer frente a estas vulnerabilidades. Por ejemplo, en 2017, la nación que sufrió más transgresiones cibernéticas maliciosas fue India, seguida de Estados

[1] Solamente, en 2017 hubo un incremento de código malicioso del 80% para equipos desarrollados por la empresa Mac.

[2] Se prevé que las explotaciones día cero alcancen la cifra de una por día para 2021, en comparación con una por semana en 2015. Menos de la mitad de las empresas en todo el mundo están suficientemente preparadas para un ataque de ciberseguridad de esta clase (CISCO/Cybersecurity Ventures, 2019).

Unidos (Ponemon Institute, 2017). Por otra parte, en 2017 se presentaron más de 130 intromisiones de larga escala en los Estados Unidos, lo que representó un crecimiento del 27% en relación con el año anterior (Accenture & Polemon Institutte, 2017). A su vez, Estados Unidos es el país que más ha invertido en respuestas cibernéticas pos-incidente (Ponemon Institute, 2017). Igualmente, los Estados Unidos encabezan la lista con 18.2% de la recepción de ataques *ransomware*. (Symantec, 2018). Por su parte, en 2017, el 20 por ciento de la actividad maliciosa en el ciberespacio provino de China, 11 por ciento se originó en Estados Unidos y 6 por ciento en Rusia (Symantec, 2018).

Justificación de la investigación

Del vacío epistémico detectado, proviene la pertinencia y la factibilidad de realizar esta investigación. Bajo este contexto, es evidente la necesidad de estudiar el concepto de ciberseguridad (*seguridad cibernética*) a la luz de Relaciones Internacionales, primero para contribuir a la integración de las nuevas realidades cibernéticas en la disciplina, y segundo para analizar la representación de sus efectos sobre la agenda de los estudios de seguridad internacional.

En efecto, el tema de la ciberseguridad internacional es multidimensional, transdisciplinario e incipiente, y por ello difícil de definir con precisión en una forma holística y metódica. Además, es escasamente analizado desde la perspectiva de Relaciones Internacionales como se aprecia en la literatura revisada y, por ello, no deja de plantear dificultades el hecho de querer presentar una visión sistemática en torno a una literatura dispersa al respecto y que, además, ilustre cuáles son sus implicaciones sobre la reconfiguración de un orden internacional complejo, imbricado y confuso que ha sido la característica desde la posguerra fría.

Elucidar ese cambio implica analizar y comprender las acciones y prácticas más significativas de la recomposición en la relación de los agentes estatales con el espacio digital (ciberespacio). Estas acciones están encuadradas por justificaciones de *seguridad* y por ciertas medidas emergencia y, como resultado de ese proceso, se observa un incremento en el número de elementos del complejo de

seguridad y defensa, la asignación de mayores recursos para el control, dominio y aseguramiento del espacio, así como más mecanismos regulatorios que servirán como evidencia empírica para sustentar la afirmación que apuntala este trabajo de investigación.

Preguntas de Investigación e hipótesis

En relación con lo antes expuesto, la siguiente interrogante funciona como guía de la investigación, ¿cuáles son los efectos de la ciberseguridad sobre las formas de participación estatal en el ciberespacio? ¿qué ha cambiado en las prácticas estatales en este ámbito cibernético? Como hipótesis central de este trabajo se sostiene que la ciberseguridad tiene un efecto directo sobre el comportamiento gubernamental en el ciberespacio, puesto que estos actores han reestructurado su comportamiento dentro de este terreno, transitando del desentendimiento o poca actividad, a una participación intensa, que se refleja en un proceso de "securitización" y una disputa hegemónica en el dominio digital.

Debido a que las actividades cibernéticas tienen una magnitud, alcance y variedad tan dilatada conduce a la restructuración del comportamiento de los actores estatales en aras de estar capacitados para afrontar un fenómeno contingente, multidimensional y multidisciplinar.

Con base en esta hipótesis se pretende alcanzar los objetivos de esta pesquisa doctoral que son examinar el impacto del fenómeno de la ciberseguridad sobre las actividades estatales en el ciberespacio, examinar las estrategias de participación gubernamental en la configuración de la arquitectura de seguridad cibernética global y observar sus efectos sobre una competencia internacional estatal en el rubro de las tecnologías de la información. En este trabajo se reconoce que la seguridad cibernética, llamada *ciberseguridad*, es un área que involucra la participación de múltiples actores sociales y políticos, no obstante, se pretende analizar particularmente el papel estatal en el ciberespacio y sus efectos sobre el funcionamiento de éste.

Con base en esto, la amplia gama de percepciones que los principales actores internacionales tengan puede causar una profunda transformación en la estructuración del entorno internacional, así como también sobre la normatividad internacional, en este caso en el entendimiento de una concepción fija sobre la seguridad cibernética y su asociación con un entorno cibernético internacional determinado. A través de ilustrar el proceso de construcción del debate sobre la ciberseguridad se puede inferir que las prerrogativas estatales son el resultado de una constante interacción e intercambio entre actores domésticos e internacionales.

Una vez planteado el problema, se muestra el orden temático de la investigación. Esta tesis doctoral se divide en cinco capítulos. El primer capítulo aborda la dimensión y alcance de un ordenamiento cibernético de carácter global. Dentro de éste se encuentra la pregunta rectora y la hipótesis central de esta investigación. Para dar respuesta a esta interrogante, en primera instancia se trazaron brevemente las líneas generales de un debate sobre las implicaciones del desarrollo tecnológico y la revisión del estado de la cuestión. En seguida, se delimitaron el área de acción y las características del marco en el que se mueven los actores estatales en las dinámicas de configuración de ciberseguridad global.

En el segundo capítulo se analizan perspectivas teóricas que delinean las bases conceptuales del trabajo de investigación, como la problematización en la definición de seguridad, la relevancia de incluir su variante cibernética para el debate epistemológico en el área de la subdisciplina de estudios de Seguridad Internacional y la manera en la que un objeto de estudio dúctil enriquece la deliberación de las ideas. Además, se recurre a la perspectiva constructivista de Relaciones Internacionales para apuntalar el andamiaje teórico-conceptual en relación con la percepción de la amenaza, conocer el proceso de constitución entre el agente y la estructura, así como ejemplificar la dinámica de cambio en las prácticas de los actores.

En el tercer capítulo, se presenta la evolución de la administración del ciberespacio en su ámbito de seguridad, los mecanismos que la rigen y las perspectivas en competencia en relación con su gobernabilidad. Además, se perfilan las alternativas que diferentes agentes pretenden establecer sobre el

espacio digital, el impacto que tienen sobre las actividades cibernéticas de seguridad y las divergencias que generan al momento de administrar y gestionar este entorno.

Para el capítulo cuatro se analiza el efecto del tema de la ciberseguridad como eje toral en las políticas internas y externas chinas y su impacto sobre su conducta internacional cibernética. En este capítulo se presenta el caso de la República Popular de China, el cual permite la contrastación con el de Estados Unidos de América, sobre las disposiciones institucionales, recursos y acciones realizadas en materia de ciberseguridad. En este sentido, se revisan algunos trabajos que preceden a éste, para situarse en la discusión, además, se plantea la organización, estructura, y las iniciativas específicas para hacer frente al desarrollo de vulnerabilidades a los sistemas informáticos.

En el capítulo 5 se analiza el efecto del tema de la ciberseguridad como eje toral en las políticas internas y externas estadounidense. En esta segunda parte del ejercicio de comparación, se presenta un esquema similar al capítulo anterior, lo que permite observar más claramente los puntos de convergencia y divergencia entre esquemas gubernamentales de participación en el ámbito de ciberseguridad. Finalmente, la última parte de esta tesis doctoral, muestra cuáles son las divergencias y convergencias de los modelos de ciberseguridad sino-estadounidenses, cómo son percibidos por otras entidades gubernamentales y no gubernamentales, qué impulsa a ambos Estados a mostrar un enfoque basado en la competencia, cómo se traduce ese afán competitivo más allá de la competencia interestatal y qué implicaciones puede tener esta dinámica para la configuración de la ciberseguridad a nivel global. Por último, se presentan los principales hallazgos, las limitantes del objeto de estudio y perfila algunas líneas de investigación futuras.

Metodología: estructura de investigación y enfoque teórico

La teoría tradicional de Relaciones Internacionales está anclada y se refiere a las interacciones primordialmente en lugares físicos. Todas las formas de espacio en las relaciones internacionales brindan oportunidades para expandir el *poder* y la *influencia* en la política mundial. Lo que está en disputa en las diferentes teorías de

Relaciones Internacionales no es si el poder está presente en la política internacional o no, sino cómo se le interpreta, cómo se le concibe y qué lo explica (Santa Cruz, 2000, pág. 168). Por ello, Nazli Chocri (2012, pág. 5) define el ciberespacio como dominios de interacción que: *1)* crean fuentes potenciales de poder; *2)* proporcionan lo necesario para la expansión de la influencia y el empoderamiento; *3)* habilitan nuevos servicios, recursos, mercados y conocimientos y; *4)* dan cuenta de potenciales agregados cuando son reforzados y sostenidos por avances tecnológicos. Cuando las actividades de un actor amenazan la soberanía, la estabilidad o la *seguridad* de otros actores, "el espacio se convierte en una variable crítica en las relaciones internacionales" (Choucri, 2012, pág. 5).[3]

Dentro de la percepción estatal sobre la contingencia de la ciberseguridad, cabría preguntarse, ¿es realmente una percepción de amenaza o, efectivamente, se trata de una amenaza real? En ese sentido, ¿por qué amenazan la soberanía, la estabilidad o la seguridad nacional?, o incluso, es pertinente cuestionar si la narrativa surge de la amenaza o la amenaza genera una narrativa propia y por ende acciones determinadas. En atención a la problemática expuesta, los aspectos fundamentales giran en torno a las características del campo de juego, es decir, quién puede jugar, cómo y por qué lo hace de cierta manera.

Es común que en el momento de emprender un trabajo de investigación surjan diversos obstáculos. En este caso, debido al estrecho lazo que ha existido entre los planteamientos de seguridad con el sector militar y de defensa, así como un alto sentido de sensibilidad sobre determinado tipo de información relacionado con ésta, es complejo el reto de emprender un trabajo sobre cuestiones de seguridad sin que se genere "recelo, sospecha y rechazo para acceder a cierto tipo de datos de carácter sensible" (Mesa, 2009). No obstante, el debate sobre los estudios de *seguridad*, en este caso en el plano internacional es rico y extenso, donde abunda una literatura de perspectivas diversas lo que ayuda a fortalecer la viabilidad sobre el emprendimiento de este estudio. Para ello, este trabajo de investigación se edifica en una recolección lo más extensa posible de fuentes

[3] Tradicionalmente, la noción del espacio estuvo íntimamente relacionada con la territorialidad. Claramente, esta conexión para algunos se está desvaneciendo (Sassen, 2006).

abiertas que pretenden ser aquí estructuradas de forma metódica, con el objetivo de hacer un análisis holístico que ayude a soportar la valoración de la hipótesis de trabajo y de las conclusiones finales. Para este efecto, se busca revisar las perspectivas que tengan diversos actores sobre el tema para la fortalecer la riqueza explicativa del argumento.

El presente trabajo se inscribe en la idea de que no hay recetas metodológicas que sean universalmente aceptadas por las diferentes comunidades epistémicas dentro de la política internacional. Esto no significa que se pretenda desdeñar una estrategia metodológica para guiar esta investigación, puesto que es un activo valioso para el análisis académico y para la implementación de toma de decisiones de manera ordenada y holística (López, 2015). En este caso se ha seleccionado un fenómeno incipiente como lo es la ciberseguridad, pero que tiene efectos observables sobre un sistema internacional cibernético, pero sus causalidades son explicadas escasamente o son incompletas (Van Evera, 1997, pág. 22).

Tampoco se busca establecer un conocimiento con pretensiones predictivas o ley universal análogo a las ciencias naturales. La diferencia entre los objetos naturales y sociales no significa que el estudio científico de los últimos no sea posible, sino que el proceso mediante el cual se lleva a cabo la investigación es diferente (Santa Cruz, 2013, pág. 39). [4] Los fenómenos sociales son producto de una ontología básica que, aun cuando no sea observable en sí misma, tiene efectos observables. No se trata, pues, de predecir u obtener generalizaciones con carácter de ley (Shapiro & Wendt, 1992), sino, de reconocer, los poderes causales en el ámbito social son siempre contingentes, es decir, pueden suceder o no suceder (Santa Cruz, 2013, pág. 40)

Si bien una posición epistemológica provee criterios metodológicos, es más amplia que la metodología misma (la cual trata simplemente de los métodos que se aplican para obtener y procesar las evidencias de un trabajo) (Santa Cruz, 2013,

[4] De manera similar, Max Weber sostenía que las leyes generales son importantes en las ciencias naturales, pero no en las sociales (Weber, 2009).

pág. 42) (Fearon & Wendt, 2002, pág. 65). El objetivo es comprender las partes y la totalidad en su mutua composición. Para la presente investigación se utiliza un estudio comparativo, a través del análisis de contenido, implementando el método de diferencia, el cual explora un número reducido de variables a detalle para saber si los sucesos desplegados se comportan y actúan conforme la teoría predice (Van Evera, 1997, pág. 37). Esto ayuda a encontrar y conocer cuáles son las causas en variaciones de la variable de estudio.

Por ello, se han seleccionado como variables de estudio dos estructuras estales, la República Popular de China y los Estados Unidos, no obstante, esto se realiza a través de la desagregación de los distintos agentes que participan dentro de estos dos amplios bloques para entender cómo determinados temas son "securitizados" para favorecer los intereses de ciertos actores o sectores. La selección de esta variable radica en el papel relevante que ambos actores juegan sobre la recomposición del orden internacional (cinético y cibernético), especialmente en el rubro de la *seguridad*, y por sus prácticas (paradigmáticas y contrapuestas) de intervención e injerencia en un espacio que era ajeno al dominio gubernamental.

Con base en esto, habrá más elementos para determinar con mayor precisión cuáles son las razones de la variabilidad en el entorno internacional cibernético en relación con las prácticas de seguridad emprendidas por los actores gubernamentales, que oscilan entre las percepciones chinas y estadounidenses al respecto. La pertinencia radica en la importancia y el tamaño de las entidades que ejecutan dicha configuración sobre el debate de la seguridad cibernética, sus características territoriales, demográficas, de poder, y por supuesto, las implicaciones de sus acciones a nivel sistémico en el terreno digital.

Capítulo 1. El sistema internacional cibernético: elementos para su análisis

Introducción

La sociedad internacional está cambiando en las últimas décadas y una de las razones principales se relaciona directamente con las transformaciones de algunas cuestiones de carácter estructural. Al finalizar el periodo histórico denominado como Guerra Fría se inició una época compleja de cambio, reconfiguración y restructuración que marca la intensificación de acondicionamientos globales en lo político, económico, social y cultural. El abanico de situaciones que aquejan una solución global conjunta o el desarrollo de nuevos planteamientos conceptuales y teóricos es amplio.

Ciertas características se relacionan con la interrelación del entorno digital (ciberespacio), el espacio cinético y el ecológico, que están redefiniendo la teoría y la práctica de las relaciones internacionales contemporáneas (Mitrany, 1948) (Choucri, 2012, pág. 3). Con la emergencia de una llamada "sociedad de Internet" (sociedad red, de acuerdo con el sociólogo Manuel Castells) y una creciente interconectividad en un mundo cada vez más globalizado, se han generado dos visiones sobre los efectos de las interacciones sociales, políticas y económicas en este entorno. Por una parte, algunos arguyen que la sociedad debe preocuparse por la vulnerabilidad que estas interconexiones traen consigo (Clarke & Knake, 2010; Kello, 2013; Libicki M. C., 2007). Para estos autores, esto incluye repensar el concepto de *seguridad* en diversos niveles (global, nacional, grupal e individual) y en diversas dimensiones (político, militar, económico, ambiental, de género, cibernético) en aras de buscar estrategias y respuestas frente a amenazas que pudieran aparecer en cada uno de estos planos.

Por otra parte, algunos autores mencionan que las interacciones sociales a nivel global, facilitadas por la floreciente y creciente innovación tecnológica, tendrán

un efecto emancipador sobre la humanidad (Castells, 2009; Zittrain, 2008; Khanna, 2016); puesto que desafían la comprensión tradicional de poder e influencia, las relaciones internacionales y la política de poder, la seguridad nacional, las fronteras y las demarcaciones tradicionales, así como una serie de conceptos y sus realidades correspondientes. Entender dichas dinámicas es importante pues permite observar las transformaciones asociadas a los elementos que están (re)configurando el entorno de *seguridad internacional* hacia una fragmentación de éste, una crisis de legitimidad y hacia una reconfiguración de las estructuras de poder a nivel global.

Entre la primera y la segunda década del siglo XXI, en teoría, las cuestiones relacionadas con el ciberespacio y sus usos han construido una narrativa que los considera la quintaesencia del marco de análisis de la seguridad internacional. Las cualidades del ciberespacio son tanto una fuente de desarrollo y progreso, así como de vulnerabilidad y, como una herramienta de control y de ataque, que representan una amenaza potencial para la *seguridad* y una perturbación del orden internacional tradicional (Choucri, 2012, pág. 3). Desde ese punto de vista, la arena del ciberespacio es la principal zona de disputa política internacional, donde se puede observar que el enfoque dominante es el desarrollo de un proceso de construcción de la amenaza cimentado en el miedo (Valeriano & Maness; Klimburg, 2017; Dunn Cavelty, 2008b). Para algunos, ese miedo está asociado fuertemente con las acciones del 11 de septiembre de 2001, pero, se ha disipado, y en cierta forma ha sido reemplazado con “el miedo de un posible conflicto cibernético, e incluso de una guerra cibernética” (Valeriano & Maness, 2015, pág. 2).

Con base en lo anterior, el objetivo general de la presente investigación es analizar los efectos de la ciberseguridad sobre las formas de participación estatal en el ciberespacio. Esta es un área que los Estados habían desdeñado, así como los efectos que tienen sobre la conformación de ciertas prácticas sobre los mecanismos de gobernanza de una estructura cibernética internacional. Para ello, es clave analizar el proceso de interacción social dónde se construyen dichas amenazas, cómo y quién las construye y, para qué propósito. En este trabajo de investigación se estudia la dinámica de negociación entre diversos grupos de

interés, actores sociales y sus diferentes perspectivas sobre el tema de seguridad cibernética de carácter internacional, en particular, el papel de las acciones gubernamentales en relación con el espacio digital y su funcionamiento.

1.1 El debate sobre la ciberseguridad internacional

Cualquier tecnología puede ser estudiada desde una variedad de perspectivas: *1)* por medio de las costumbres que origina; *2)* las relaciones sociales que ayuda a fomentar; *3)* el desarrollo de ciertas prácticas; y *4)* los valores que fomenta. Asimismo, estudiar la tecnología en contextos culturales permite entender en qué medida, la especie humana está condicionada por la estructura sistémica en la que se desenvuelve y cómo, a su vez, esta (la agencia) influye en la estructura mediante su interacción social en función de la multiplicidad de intereses determinados por enlaces crecientes de intereses e identidades colectivas (Escobar, 1994).

La reestructuración de relaciones con base en la tecnología funciona como un agente de producción social y cultural (Escobar, 1994). El origen y la operación de estos enlaces permiten observar la continuidad y la transformación de los valores dominantes de racionalidad, instrumentalidad, ganancia y violencia que están circunscritos, regularmente, por intereses económicos y político-militares (Escobar, 1994). Los avances en la tecnología, respaldados por la innovación científica, han permitido el acceso a nuevas formas de espacio. La innovación tecnológica también ha mejorado nuestra capacidad de delinear el conocimiento sobre las propiedades y características de ámbitos de actividad en otros territorios previamente inaccesibles. No obstante, estas tecnologías pueden también ser objeto de abuso para producir condiciones desestabilizadoras, como el desarrollo de armas de destrucción en masa, instrumentos de dominación, control y explotación, sobre todo a medida que se vuelven más económicas y la capacidad de obtenerlas y manipularlas se generaliza (Choucri, 2012, pág. 6).

Dentro de este cuadro se puede enmarcar el estudio del espacio digital. Creado a través de la innovación tecnológica, el espacio digital permite a los usuarios participar en actividades dentro de campos electrónicos cuyos dominios espaciales trascienden las restricciones territoriales, gubernamentales, sociales y

económicas tradicionales (Choucri, 2012, pág. 6; Mattelart, 2007) Este espacio ofrece nuevas oportunidades para la competencia, la colaboración, la contención, el conflicto y la cooperación.

Además, los nuevos espacios se han formado mediante el despliegue de la fuerza física combinada con el poder de la competencia, la innovación y el espíritu de aventura. Históricamente, sólo los actores más capaces, los más poderosos y eficaces, militarmente o no, han podido competir efectivamente en la colonización del territorio y la exploración de los nuevos espacios (Krishna-Hensel, 2007). Es por ello que el ciberespacio se ha concebido como el lugar donde está la búsqueda del poder, el prestigio colectivo, el posicionamiento en el panorama internacional, la mejora de la riqueza y la ventaja estratégica en la competencia militar (Choucri, 2012, pág. 6)

Las interacciones internacionales de todo tipo están cambiando debido a la llegada de las tecnologías cibernéticas. El espacio digital es ahora un lugar de competencia entre intereses y grupos de interés diversos, así como también una arena para conflictos y colaboración que marcan la pauta de los reacomodos sociales, económicos, políticos, culturales e identitarios (Choucri, 2012). Sin embargo, la interrelación entre relaciones internacionales e interacciones cibernéticas, se ha abordado escasamente (Eriksson & Giacomello, 2007).

En particular, la seguridad cibernética ha sido un problema relativamente ignorado por la academia, en especial la comunidad epistémica de las Relaciones Internacionales. Llama la atención, en especial, la ausencia de bibliografía que se produce en el área de Relaciones Internacionales. Existen pocos análisis sistemáticos, teóricos o empíricos del problema cibernético desde la disciplina de las Relaciones Internacionales o desde el subcampo de los Estudios de Seguridad (Deibert R. J., 2003; Eriksson & Giacomello, 2006; Hansen & Nissenbaum, Digital disaster: cyber security, and the Copenhagen School, 2009; Valeriano & Maness, Cyber war versus cyber realities: cyber conflict in the international system, 2015; McEvoy, 2010; Klimburg, 2017; Eriksson & Giacomello, 2007). No obstante, destaca la aportación seminal que hicieron John Arquilla y David Ronfeldt (1993) sobre la emergencia de nuevos modos de conflicto, el desarrollo de conceptos como

“ciberguerra” o “guerra en red” (*netwar*) y el impacto de las tecnologías de la información digital sobre el conflicto internacional. Por otra parte, autores como Thomas Rid (2012) cuestiona que la guerra cibernética y los desarrollos digitales tengan un impacto significativo sobre los asuntos polemológicos.

Existe cierto consenso entre los autores acerca de la causa principal que supuestamente explica la situación de escasez analítica del tema. Para algunos autores, esto responde a un importante grado de escepticismo sobre la relevancia del ecosistema cibernético de carácter internacional como un importante componente para explicar el cambio y la transformación a nivel internacional, por ende, la escasa literatura de relevancia (Choucri, 2012; Kello, 2013; Valeriano & Maness, Cyber war versus cyber realities: cyber conflict in the international system, 2015). Para otros autores, el desarrollo poco profuso desde la perspectiva de Relaciones Internacionales se debe a una ‘obsesión’ al interior de la disciplina por brindar esquemas teóricos generales con poca aplicabilidad empírica, dejando de lado cuestiones como el desarrollo tecnológico y su impacto sobre el esquema político, económico y social de carácter global (Eriksson & Giacomello, 2007, pág. 2).

Existe una dicotomía en relación con los supuestos sobre la correspondencia entre el dominio digital y la política. Algunos consideran que esta arena modifica, en absoluto, todas las actividades humanas formando nuevos ecosistemas, por medio de mayor información asequible y un grado superlativo de transparencia política (Castells, 2009; Zittrain, 2008). En ese tenor, algunos recalcan que las herramientas de interacción social digital coadyuvan en la construcción de la esfera pública internacional (Shirky, 2011). No obstante, esta visión desestima los efectos negativos de la Red. Por su parte, otros consideran que el espacio digital modifica pocas situaciones, puesto que gobiernos y agentes privados continúan utilizando su fuerza militar y su influencia económica para asegurar el control y dominio sobre amplios sectores sociales (Deibert R. J., 2013; Escobar, 1994).

En realidad, suceden ambas tendencias simultáneamente (Wu I. S., 2008, pág. 5; Morozov E. , 2011). El desafío es entender cómo las viejas fuentes del poder interactúan con nuevos formatos (Morozov E. , 2011). Unos argumentan que el

debate de las relaciones cibernéticas necesita moverse hacia las bases del estudio de la política internacional (Choucri, 2012; Kello, 2013; Valeriano & Maness, 2015; Lindsay J. R., 2015a; Eriksson & Giacomello, 2007). En efecto, los problemas cibernéticos internacionales no están desmarcados completamente de los procesos de las relaciones internacionales cinéticos, en otras palabras, "las operaciones que ocurren en el dominio cibernético no están desconectadas de otros dominios de la interacción política internacional" (Valeriano & Maness, Cyber war versus cyber realities: cyber conflict in the international system, 2015, pág. 14). Como recalca Brandon Valeriano y Ryan C. Maness "es cierto que el ciberespacio es un dominio con dinámicas propias, pero no está desvinculado totalmente del plano político internacional que es la génesis de los conflictos internacionales" (Valeriano & Maness, 2015, pág. 15).

Antes de continuar con la revisión de los debates teóricos sobre el tema, algunas aclaraciones conceptuales y metodológicas son necesarias para solventar la capacidad explicativa de este estudio. Para realizar el análisis propuesto, se debe describir y explicar en qué consiste el espacio en el cual participan los agentes estudiados, la diversidad de su índole, así como su evolución y la diversificación que permite la reconfiguración de fuerzas y actores. En este proceso se articulan prácticas y políticas distintivas y específicas que ayudan a entender la dimensión y el alcance desplegado por las prácticas estatales de seguridad en el terreno cibernético.

1.1.1 Antecedentes de la conformación del ciberespacio

Las raíces históricas y filosóficas del vocablo "cibernético", a menudo, se considera que aparecieron por primera vez en la obra *La República* del filósofo griego Platón (Klimburg, 2017). Para otros, su identidad semántica para la "edad moderna" se deriva del término *cibernética*, "el estudio de la comunicación y el control" presentado por el matemático Norbert Wiener (1948) en *Cybernetics: Or Control*

and Communication in the Animal and the Machine (Escobar, 1994, pág. 211) (Choucri, 2012, pág. 7); (Valeriano & Maness, 2015, pág. 3) (Deibert R. J., 2013).[5]

En consecuencia, el trabajo de Norbert Weiner influyó el de Karl W. Deutsch (1963) *The Nerves of Government*, que sigue siendo un punto de entrada importante en la ciencia política y la investigación política sobre la interrelación entre comunicación, política y control.[6] Por otra parte, el autor de ciencia ficción William Gibson (1984) es reconocido por ser el primero en acuñar el vocablo *ciberespacio* en su obra *Neuromancer*,[7] proporcionando la primera designación formal que integraba las nociones de cibernética y espacio, y así, dar cabida a la creación de un nuevo campo de interacción (Choucri, 2012, pág. 7). Por otro lado, el sitio tecnológico *Gizmodo* rastreó la vida del prefijo '*ciber*' desde 1950 hasta 2013, y encontró las variaciones que el concepto cibernético ha tenido (Klimburg, 2017, pág. 23).

En torno a ello, han surgido diversas definiciones y concepciones de lo que el *ciberespacio* representa y los elementos que lo componen. Por ejemplo, para autores como Richard Clarke y Robert K. Knake (2010, pág. 70) lo definen como "todas las redes de computadora en el mundo y todo con lo que conectan y controlan". No obstante, limitar lo cibernético (*cyber*) a redes computacionales es un poco estrecho y restringe la integración de nuevas tecnologías cibernéticas dentro del paradigma. Para otros autores, la inclusión del término *microprocesador* puede proveer de mayor precisión a una definición del ciberespacio (Valeriano & Maness,

---

[5] Cuando Norbert Wiener acuñó el término "cibernética" tenía en mente la labor que los jinetes o los "pilotos" de la Grecia antigua realizaban (*kibernetes*), aunque no exista una raíz etimológica griega para dicha expresión, su uso se ha vuelto un prefijo común para identificar las acciones relacionadas con el espacio digital (Escobar, 1994).

[6] Karl Deutsch utilizó elementos de la teoría de las comunicaciones y cibernética, así como de la sociología estructural-funcionalista. La sociología estructural-funcionalista estudia la sociedad como una totalidad formada por partes interdependientes, cada una de las cuales cumple una función en el mantenimiento y la reproducción del sistema. El concepto de sistema, entendido como una red de comunicaciones análoga al sistema nervioso es central en su obra. (Choucri, 2012; Santa Cruz, 2000: 50-51).

[7] Para algunos autores, el nacimiento del término se da en la pequeña historia intitulada "Burning Chrome" y que fue popularizada en su novela *Neuromancer* (Deibert, 2013, pág, 264)

2015, pág. 22). Por otro lado, la definición que Joseph Nye (2011) propone está mucho más cerca del contenido real de lo que es el ciberespacio para la mayoría de quienes utilizan el término en el contexto político. Para Nye (2011), "el dominio cibernético incluye la red de computadoras conectadas a Internet, pero también incluye las redes internas (*intranet*), las tecnologías de telefonía móvil, cables de fibra óptica, comunicación satelital-espacial. Asimismo, el ciberespacio tiene una capa de infraestructura física que está sujeta a leyes económicas, leyes políticas de soberanía, competencia por recursos y por justificar su control y regulación" (Nye J. S., 2011, pág. 19)

Para los propósitos de este trabajo de investigación, se tomará al prefijo "*cibernético*" (*cyber*) simplemente con el sentido de las interacciones digitales, computarizadas, o realizadas a través de microprocesadores, las cuales están directamente relacionadas con el ciberespacio y permiten la comunicación e interacción de diversos agentes. Aunque ciberespacio e internet se han utilizado de manera intercambiable, no son lo mismo. El Internet es la red global de redes de computadoras configuradas para operar de acuerdo con un protocolo de intercomunicación (*TCP/IP protocol*). El ciberespacio es mucho más amplio e incluye el dominio entero de las comunicaciones globales, donde se incluye (pero no se limita) al Internet (Deibert R. J., 2013) (Klimburg, 2017).

Aunque la palabra ciberespacio ha tomado diferentes significados derivados de sus características fundamentales, aquí se utiliza la relacionada con un dominio global dentro de un ambiente de información, cuya característica única y distintiva está dada por "el uso del espectro electrónico y electromagnético para crear, almacenar, modificar, intercambiar y aprovechar información a través de redes e infraestructuras interconectadas por medio de tecnologías de la información y la comunicación" (Kuehl, 2009, pág. 28). Para el ámbito que compone el *ciberespacio* (*cyberspace*), en este trabajo de investigación se toma un parte de la siguiente definición: "el ciberespacio es el sistema en red de microprocesadores, servidores, y computadoras que interactúan en el nivel digital" (Deibert R. J., 2013) (Mattelart, 2007) (Valeriano & Maness, 2015). Sin embargo, a esta conceptualización se puede agregar que no son únicamente las infraestructuras dentro el espectro, o la cantidad

de contenido, sino que incluye todos los dispositivos móviles que utilizan algún punto del espectro electromagnético para la interconectividad, que puede incluir, *wearables* (sensores enlazados a la red) y aparatos que necesitan enlazarse con el peldaño lógico-programático del ciberespacio para funcionar (también llamado el Internet de las Cosas).[8]

De suma importancia para este trabajo son las formas en que los espacios cibernéticos se utilizan para dar forma a las ideas, intercambiar información y aumentar el acceso al conocimiento y modos alternativos de razonamiento. En efecto, como lo dice el artículo de John Palfrey (2010), todas estas visiones describen una forma de la relación entre el uso de la tecnología y los impactos en la actividad social, que van de la mano con su clasificación de las etapas de desarrollo del ciberespacio.

De igual manera, en relación con la introducción del término *ciberseguridad* o seguridad cibernética no existe un contexto tan amplio sobre su primera acepción. De acuerdo con algunos analistas, el concepto fue utilizado por primera vez en 1989 (Newitz, 2013). Para otros especialistas, el asentamiento de la idea de *ciberseguridad* en el terreno político surge en 1995, cuando la revista *Time* publicó en la portada principal el término '*ciberguerra*' (Klimburg, 2017, pág. 23). Quizá esta sea una de las raíces de la asociación de la narrativa de lo cibernético con el miedo y con el conflicto. Incluso, para 1999, un oficial de alto rango del Departamento de Defensa de los Estados Unidos utilizó el concepto '*ciberguerra*' por primera vez ante el Congreso de su país, marcando un enlace entre el conflicto internacional y las herramientas de explotación computacional como el *hackeo* (Klimburg, 2017, pág. 24).[9] No obstante, para una comprensión más clara se necesita trazar, de forma

[8] La cantidad de dispositivos conectados en Internet superará los 50 mil millones para 2020. La cantidad de dispositivos del Internet de las Cosas será tres veces más alta que la población mundial proyectada para 2021, y para 2022 se incorporarán en el mundo 1 billón de sensores enlazados a la Red (CISCO/Cybersecurity Ventures, 2019).

[9] El término *hacking* (acceso sin autorización) fue utilizado por primera vez en 1955 en el MIT. Su origen y su construcción conceptual siguen siendo imprecisos. Por ejemplo, en su primera acepción fue asociado como sinónimo de broma (*prank*). Al final de la década de 1950, comenzó a usarse en relación con el estudio de códigos internos y características para modificar los sistemas telefónicos, fue su asociación con hacer algo 'fuera de la norma'. Sin embargo, en 1960 comienza a utilizarse en relación con el campo informático. Dentro de la comunidad de expertos informáticos hay una

sistémica, una cronología sobre el desarrollo de lo cibernético de carácter internacional, estableciendo un terreno empírico y teórico que sirva para comprender las relaciones internacionales de cooperación y conflicto que surgen en una dimensión emergente, donde las posturas y visiones son tan diversas como el número de actores.

1.1.2 Fases del desarrollo del ciberespacio

De acuerdo con algunos especialistas sobre el desarrollo cibernético y la seguridad internacional, se pueden identificar las siguientes fases del desarrollo del ciberespacio: *1)* la era abierta, que va desde su nacimiento hasta el 2000; *2)* el acceso denegado, de 2000 a 2005; *3)* el acceso controlado, de 2005 a 2010 y; *4)* acceso en disputa, de 2010 a la actualidad (Palfrey, 2010, pág. 981). La primera etapa corresponde a la arquitectura y los cimientos de la red global, donde el propósito central de su desarrollo era que fungiera como una herramienta para el intercambio de comunicación de forma libre en instituciones académicas y gubernamentales de Estados Unidos (Palfrey, 2010). Este funcionamiento comienza a ceder paso a finales de la década de 1980, cuando nace la *World Wide Web* (red informática global), y comienza lo que algunos autores denominan "la comercialización de Internet" (Perrit, 1998; Sassen, 1998).

En la segunda etapa, algunos actores estatales y no estatales consideran que algunas actividades que se comenzaron a desarrollar en Internet necesitan ser reguladas o interceptadas, principalmente, en relación con algunas muestras de libertad de expresión, creando fuertes filtros para el acceso a la información (Palfrey, 2010, pág. 985; Morozov E. , 2011). Dentro de una concepción general, se considera que únicamente algunos gobiernos (calificados como autoritarios o no democráticos) son propensos a utilizar filtros para bloquear el contenido que fluye dentro de sus fronteras a través del ciberespacio; sin embargo, es una actividad realizada también por gobiernos democráticos, en ocasiones apoyados por empresas privadas que manejan una gran cantidad de los flujos informativos en la

distinción entre *hackeo* y *crackeo*. El primero, denota intrusión en un sistema sin fines maliciosos, el segundo, describe actividades nefarias como desplegar virus, modificación o destrucción de datos e interrupción de sistemas (Peterson, 2011, págs. 5-7).

Red (Deibert, Palfrrey, Rohozinski, & Zittrain, 2008) (Deibert & Rohozinsky, 2010) (Vaidhyanathan, 2018).

Estos controles demuestran lo que algunos han tratado enfatizar sobre en qué medida la teoría tradicional de las relaciones internacionales gobierna tanto en el espacio real como el ciberespacio (Goldsmith & Wu, 2006; Palfrey, 2010). Precisamente, la tercera fase se caracteriza como un período durante el cual los Estados han enfatizado la pertinencia de enfoques regulatorios que sirven como variables de control (Palfrey, 2010, pág. 989). Lo destacado de esta etapa es el desarrollo de una serie de mecanismos que pueden utilizarse para limitar el acceso a la información, más sofisticados y rebuscados que en la etapa anterior. (Deibert R. , Palfrey, Rohozinski, & Zittrain, 2010; Morozov E. , 2011). Dentro de esta etapa surgieron requerimientos como el registro de usuarios, licencias de uso y controles legales sobre la forma de utilizar el ciberespacio. A su vez, se observa una combinación entre vigilancia y medios de imposición, aplicación y ejecución legal, que para algunos tiene un efecto negativo sobre la libertad de expresión en línea (Deibert & Rohozinsky, 2010; Morozov E. , 2011).

Por último, en la cuarta etapa, la regulación que se ha impuesto comienza a enfrentar respuestas de los ciudadanos y desafíos del sector privado (Deibert R. , Palfrey, Rohozinski, & Zittrain, 2012). Las compañías de tecnología de la información han comenzado a competir directamente, o indirectamente, entre ellas y contra los gobiernos sobre cómo desempeñar el control e, incluso la censura, en el ciberespacio (Palfrey, 2010, pág. 992) (Vaidhyanathan, 2018). Asimismo, los agentes estatales y los organismos internacionales intergubernamentales se han comenzado a enfrascar en fuertes debates y en acciones que buscan regular el ciberespacio en formas divergentes, lo que ha resultado en una disputa sobre la forma de gobernanza del ciberespacio (DeNardis, 2009) (DeNardis, 2014).

Estas etapas cronológicas que John Palfrey (2010) encuadra conforme a su característica primordial de interrelación entre actores y contexto tratan de describir la utilización, el papel y las prácticas que diversos actores han tenido en el desarrollo del dominio digital, incluidos los agentes estatales. No obstante que su temporalización es muy útil, pareciera que el comienzo de una etapa no rechaza por

completo la existencia de la otra, por lo cual se puede afirmar que siguen coexistiendo y retroalimentándose entre sí.

1.1.3 Organización del ciberespacio

Ciertamente, el ciberespacio es un elemento que genera una reconfiguración de las relaciones internacionales contemporáneas, pero, ¿cómo se organiza el sistema internacional cibernético?, ¿qué aspectos distinguen el sistema internacional cibernético del tradicional? Primeramente, se puede observar el ciberespacio como un sistema contingente compuesto por cuatro categorías: *1)* el primer escalón lo componen los fundamentos físicos e infraestructuras que permiten su funcionamiento; que son los cables de fibra óptica, comunicación satelital, dispositivos digitales, servidores, computadoras, 'el esqueleto del ciberespacio'; *2)* el segundo son los bloques de construcción lógica que soportan la plataforma física y que habilitan los servicios, que son una amalgama de códigos, protocolos, *software* y actualizaciones de estos, que forman las 'neuronas' y se desempeñan como el sistema nervioso del ciberespacio; *3)* la tercer capa es el contenido de información almacenado, transmitido o transformado, y reconfigurado, que incluye documentos, vídeos, imágenes, sonido y mensajes, análogos a los 'músculos' del cuerpo ciberespacial; *4)* y en última instancia se encuentran los actores, entidades y usuarios que emiten y ayudan a movilizar la tercera capa, que cuentan con diversos intereses y participan en este campo con distintos papeles, representan el 'corazón' del sistema (Choucri, 2012, pág. 8) (Klimburg, 2017, págs. 28-29).

En la siguiente figura se puede observar, de forma esquemática, cómo se configuran los distintos sistemas que componen el ciberespacio. Se elige esta figura, pues se considera que la complementariedad y retroalimentación entre los cuatro bloques es indispensable para el buen desempeño de este. Si bien es cierto que, en este trabajo de investigación el énfasis se pone en los dos primeros bloques, no se perderá de vista que la aportación y el ejercicio de los otros dos, pues son imprescindibles para entender la complejidad de las interacciones cibernéticas internacionales.

Figura 1.1 Sistemas que componen el ciberespacio

Fuente: Elaboración propia con datos de (Choucri, 2012; Klimburg, 2017).

Además, el ciberespacio se puede definir bajo cuatro principios: primero, que es replicable, significa que el concepto es expandible y resiliente al mismo tiempo; segundo, consiste en acciones reconocidas, como el escribir mensajes en códigos lingüísticos conocidos en oposición al código binario que la gran mayoría poblacional no entiende (dentro del sistema lógico); tercero, tiende a tener reglas o tecnologías persistentes; y por último está dividido entre el estrato físico y el estrato sintético (la información y el conocimiento) (Valeriano & Maness, 2015, pág. 24).

Todas estas capas, funciones y entidades son relevantes para las relaciones internacionales en su manifestación cibernética. Como una amalgama de redes interoperables, se ha convertido en una parte fundamental de la emergente infraestructura de comunicación e interacción global, donde la capa de contenido de información se está expandiendo a tasas exponenciales, generando y transmitiendo nueva información, y a su vez creando más mecanismos para facilitar el uso y la reutilización de contenido (Choucri, 2012, pág. 8).

1.2 El ciberespacio como lugar de competencia entre intereses

De acuerdo con lo antes mencionado, las interacciones internacionales están cambiando debido a la llegada de las tecnologías cibernéticas, pues el ciberespacio es ahora un lugar de competencia entre intereses y grupos de interés, así como también arena para colaboración y conflictos que marcan la pauta de los reacomodos sociales, económicos, políticos, culturales e identitarios (Choucri, 2012). No obstante, el sistema cibernético cuenta con cualidades distintivas cuyas características difieren de las interacciones del sistema social o el sistema ambiental.

Para algunos autores como David D. Clark (2010) la cualidad distintiva reside en que los sistemas de decisión del ciberespacio están involucrando una tremenda gama de actores y entidades en la operación de éste. Aunado a esto, la discusión se ha centrado en sí esta característica peculiar está transformándose o transitando hacia esquemas de gobernabilidad tradicionales y qué efectos puede tener sobre el funcionamiento general del dominio ciberespacial. En el nivel más general, incluye a los agentes de la industria de internet e informática, aquellos involucrados en aplicaciones y desarrollo de software, proveedores de contenido, gobiernos, organizaciones internacionales, gerentes de espacios en la red, organizaciones no gubernamentales y, lo más importante, una gran amalgama de grupos e individuos a lo largo del orbe.

Por un lado, en el ciberespacio se realiza una toma de decisiones menos estratificada, que combina diversas formas de organización y de gestión, a través de un procedimiento consensual, a diferencia del proceso de gobernabilidad internacional tradicional. Por otro lado, las interacciones internacionales físicas tradicionales son rígidas y cambian de forma menos vertiginosa, por el contrario, en el terreno ciberespacial se suceden transformaciones de manera acelerada y con flexibilidad. En el siguiente cuadro, se puede ejemplificar, de manera sencilla algunas de las diferencias entre el sistema internacional tradicional y el cibernético.

Tabla 1.1 Sistema Internacional Cibernético

Sistema	**Sistema Internacional**	**Sistema Internacional Cibernético**
Actores	• Estados-nación • Organismos internacionales intergubernamentales • Organizaciones no gubernamentales • Agencias regionales • Actores de la sociedad civil organizada	• ICANN (Corporación de Internet para la Asignación de Números y Nombres, *Internet Corporation for Assigned Names and Numbers*) • Grupo de Trabajo sobre la Gobernanza de Internet de las Naciones Unidas (*Internet UN Working Group on Internet Governance*) • Cumbre Mundial de las Naciones Unidas sobre la Sociedad de la Información (*UN World Summit on the Information Society*) • Estados-nación
Arena/Contexto	Cinético	Cibernético
Dinámicas/Interacciones	Rígidas, cambian de forma lenta, diversas	Flexibles, cambian de forma

		vertiginosa, diversas
Gobernabilidad	Estratificada, regularmente la toma de decisiones se da en forma vertical	Flexible, irregularmente estratificada, combina formas verticales y horizontales de toma de decisión

Fuente: Elaboración propia con datos de (Valeriano & Maness, 2015; Choucri, 2012).

Es cierto que en el ciberespacio los actores son diversos, con diferentes grados de poder y capacidades, organización e infraestructura, lo cual hace al análisis mayormente desafiante. Esto acentúa más la necesidad de mover el debate de las relaciones cibernéticas hacia las bases del estudio de la política internacional (Valeriano & Maness, 2015). Para algunos expertos, los problemas cibernéticos internacionales no están desprovistos de los procesos de las relaciones internacionales cinéticas o pueden brindar claves para su estudio sistemático, holístico y heurístico (Dunn Cavelty, 2008b).

Justamente, hay elementos identificables que constituyen al entorno cinético y cibernético internacional como temporalidad, espacialidad, alcance de las interacciones, formas de participación, atribución de las acciones y mecanismos de rendición de cuentas (Choucri, 2012), no obstante, sus composiciones son distintas. Por ejemplo, en cuanto a la temporalidad, en el ambiente cinético las interacciones que pueden modificar algún principio de ordenamiento son de media duración, por el contrario, en el espacio cibernético pueden ser casi-instantáneas. De igual manera, las acciones y el alcance en el sistema internacional tradicional se ajustan primordialmente a demarcaciones territoriales rigurosamente definidas, a la inversa, en el ciberespacio la trascendencia territorial se da con mayor facilidad, aunque en ocasiones esta fluidez puede verse obstruida. Después, en el caso de la atribución de las acciones se presenta una diferencia clara, puesto que en el sistema internacional se busca que las acciones realizadas sean conocidas y reconocidas por otros, no obstante, en el entorno internacional cibernético se pretende mantener oculta la identidad de las acciones. Por último, relacionado con el punto anterior, los

mecanismos de rendición de cuentas del sistema internacional cinético tienen atribuciones claras y precedentes para ejercer adecuadamente su ejercicio, mientras que, en el caso contrario, no hay acuerdos sobre cómo implementar normatividades y reglamentaciones de comportamiento adecuado. En el siguiente cuadro se presenta una propuesta de análisis para entender la conformación del Sistema Internacional Cibernético.

Tabla. 1.2 Elementos del Sistema Internacional Cibernético

Elementos	**Sistema Internacional Cinético (tradicional)**	**Sistema Internacional Cibernético**
Temporalidad	Proceso de media duración.	Instantáneo/quasi-instantáneo
Espacialidad	Sujeto a soberanías territoriales	Trasciende limitaciones geográficas
Alcance	Rigidez entre jurisdicciones	Movilidad entre jurisdicciones
Participación	Altas barreras para la participación política directa	Menores barreras para el activismo y la participación política
Atribución	Se busca la visibilidad en la autoridad de las acciones	Se busca mantener oculta la identidad de las acciones
Rendición de cuentas	Atribuciones de acción definidas con mayor claridad	Elude mecanismos de responsabilidad tradicional

Fuente: Elaboración propia con datos de (Choucri, 2012)

1.3 El ciberespacio bajo la teoría de Relaciones Internacionales

Aquí se presentan algunas consideraciones elementales de la teoría de las Relaciones Internacionales que pueden servir de puente y de hilo conductor para comprender de qué forma la metodología y creación conceptual puede ayudar a perfilar de manera más precisa el fenómeno de la ciberseguridad y el papel que juega en la construcción narrativa de los Estados sobre su participación dentro del ciberespacio.

Por un lado, el realismo es un enfoque dentro de Relaciones Internacionales que ha tenido fuerza explicativa y una alta atracción dentro de la comunidad

académica durante un largo período de tiempo, principalmente durante la Guerra Fría. Sus supuestos básicos son: 1) el Estado es la unidad primaria de análisis; 2) el Estado actúa de forma racional para satisfacer sus intereses nacionales; 3) el poder y la seguridad son los valores centrales del Estado (Waltz, 1979; Morgenthau, 1948). En todas las vertientes del realismo, su cosmovisión es esencialmente pesimista (Sterling-Folker, 2013). En otras palabras, para el enfoque realista de Relaciones Internacionales, la anarquía (ausencia de un gobierno central) caracteriza el sistema internacional, lo cual obliga a los actores a comportarse en función de su interés que es la supervivencia (Waltz, 1979). Para los realistas, las causas del conflicto surgen de la competencia entre Estados que buscan sobrevivir a través de incrementar su seguridad. Por ende, las condiciones anárquicas conducen a un "dilema de seguridad", un proceso en el cual una acción está correspondida con una reacción (Jervis, 1979; Glaser C. L., 2004). Como consecuencia, el poder es medido principalmente en términos de capacidades militares y asociado con la búsqueda de seguridad (Morgenthau, 1948; Gilpin R. , 1986).

La emergencia de eventos relacionados con la ciberseguridad presenta una oportunidad para el resurgimiento de la perspectiva realista de Relaciones Internacionales como herramienta útil para analizar cuestiones como: la competencia de seguridad en el ámbito digital; las estrategias cibernéticas de defensa y ataque y su posible escalamiento a conflictos cinéticos de gran envergadura; el establecimiento de leyes nacionales férreas de vigilancia y control en el ciberespacio; la competencia por el desarrollo de arsenales digitales por actores estatales y no estatales; la apropiación espacial en el terreno digital e, incluso, del uso e implementación de la disuasión en el ciberespacio (Craig & Valeriano, 2018; Edde, 2018; Crosset & Dupont, 2018; Ebert & Maurer, 2014; Reardon & Nazli, 2012; Friis & Ringsmose).

Por consiguiente, conforme lo mencionan algunos teóricos, los enfoques realistas no ven la necesidad de corregir o actualizar sus supuestos teóricos para entender el significado de la seguridad en la era digital. El Estado sigue siendo visto como el actor más importante, y la definición de seguridad se sigue manteniendo

estática, la cual niega que los actores no estatales pueden ejercer algún grado de poder militar (Eriksson & Giacomello, 2006, pág. 229). Generalmente, procesos como la transnacionalización, la interdependencia y la globalización, se han estudiado como epifenómenos, los cuales pueden afectar las políticas y estructuras domésticas de los Estados, pero que no socavan la anarquía del sistema político internacional, por ende, no afectan la primacía de éste como unidad política suprema del sistema (Walt S. , 1994) (Eriksson & Giacomello, 2006, pág. 229).

Por otro lado, el liberalismo es una perspectiva muy amplia en cuanto las temáticas que aborda, en la cual se incluyen, entre otros, el idealismo wilsoniano y la teoría neoliberal (Moravcsik, A., 1998) (Moravcsik, 1999) (Walker, 1993); la teoría de la paz democrática (Russett & Antholis, 1993); la teoría de la interdependencia (Keohane & Nye, 1977), teorías de segunda imagen (Gourevitch, 1978), enfoques sobre la ejecución políticas domésticas y el papel de instituciones internacionales, la construcción de regímenes internacionales y la institucionalización internacional (Allison & Zelikow, 1999) (Risse-Kappen, T., 1995) (Snyder, 1991). Los principales supuestos teóricos del liberalismo en la disciplina de Relaciones Internacionales pueden resumirse en lo siguiente: *1)* un énfasis en la pluralidad de actores internacionales; *2)* la importancia de factores domésticos en el comportamiento de los Estados en el entorno internacional; *3)* el papel de las instituciones internacionales en establecer normas de comportamiento para los actores; y *4)* la expansión de la agenda de estudios internacionales (Eriksson & Giacomello, 2006; Sterling-Folker, 2013).

Si bien es cierto que, los liberales están de acuerdo con los realistas en que los Estados son actores centrales en la política internacional, los primeros consideran que estos no son los únicos que pueden jugar papeles significativos en las interacciones internacionales (Keohane R. , 1984). Por su parte, la lectura que los liberales dan a la política internacional contemporánea es que la soberanía del Estado-nación constantemente está siendo permeada y fragmentada por el desarrollo de interacciones transnacionales fluidas de actores no estatales (Keohane & Nye, 1977; Khanna, 2016) (Eriksson & Giacomello, 2006). Los autores y estudiosos de este enfoque plantean que, aunque para un solo actor es

complicado desafiar el poder económico, político y militar de un Estado, la creciente red de relaciones transnacionales complejas afecta a los Estados soberanos a tal grado que la *soberanía* se convierte más en un símbolo de integridad territorial que en un activo político sustentable (Keohane & Nye, 1977) (Camilleri & Falk, 1992) (Rosenau, 1990). Asimismo, el liberalismo recalca que los actores no estatales con capacidad transnacional y económica importan tanto como la seguridad y los Estados (Keohane R. , 1984).

En general, el liberalismo, tiende a reiterar los resultados positivos de la interdependencia y la interconectividad (Eriksson & Giacomello, 2006, pág. 230) (Nye J. S., 2004b). El énfasis se pone sobre las posibilidades de superar los conflictos a través de medios pacíficos, en particular, por medio del establecimiento de normas y la construcción de instituciones a nivel internacional (Finnemore & Sikkink, 1998). No obstante, lo que mayormente enfatiza el liberalismo es que en la medida que las sociedades creen mayores lazos de interconexión entre sí, éstas interactúan en mayor como canales de comunicación y entendimiento, lo cual reduce las posibilidades de escenarios bélicos entre ellas. A su vez, algunos liberales han apoyado la ampliación de la concepción de seguridad para incluir aspectos económicos, sociales y ecológicos en la definición (Keohane & Nye, 1998). No obstante, paradójicamente, los liberales parecen evaluar el desafío de la revolución de la información tangencialmente (Eriksson & Giacomello, 2006, pág. 231).

De este modo, a través de la revisión de la literatura liberal sobre construcción de regímenes e institucionalización con respecto a la era digital, internet y elementos cibernéticos se puede constatar la poca fertilidad en el terreno. Respecto a temas no relacionados con la seguridad en el ámbito digital destacan los estudios de Marcus F. Franda (2001) y los trabajos editados por James N. Rosenau y J. P. Singh (2002). A pesar de ello, también existen estudios que bajo este enfoque abordan cuestiones de seguridad en la era digital como los de Lorenzo Valeri (2000) y Giampiero Giacomello (2005). Por su parte, la teoría de la interdependencia compleja ha hecho actualizaciones para adaptarse a los retos planteados por la era digital. (Keohane & Nye, 1998) (Nye J. S., 2004b). Estos autores argumentan que

el “poder suave” se está volviendo más importante en la era digital, principalmente debido a la evolución de múltiples canales de comunicación global que trascienden fácilmente las fronteras soberanas (Keohane & Nye, 1998) (Nye J. S., 2004a).

Por otro lado, para ciertos especialistas, las tecnologías de la información y la comunicación globales no son meramente instrumentos de cooperación, democratización y paz, sino que, a su vez, también pueden ser mecanismos de engaño, propaganda, fraude y terror (Eriksson & Giacomello, 2006; Klimburg, 2017; Morozov E. , 2011). Esto puede tener tanto efectos positivos como negativos: por un lado, la integración, la cooperación y la democratización pueden ser más asequibles, pero también el terrorismo, la delincuencia transnacional y la desestabilización de los Estados pueden crecer rápidamente (Eriksson & Giacomello, 2006, pág. 232; Crosset & Dupont, 2018).

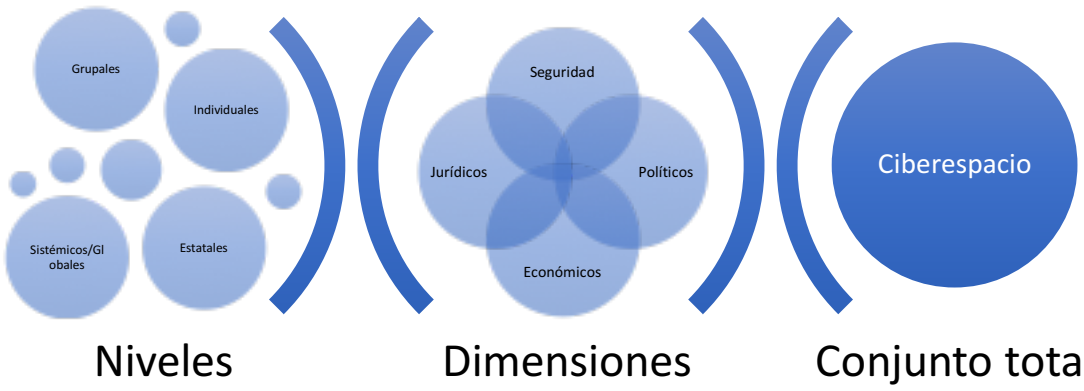
1.4 Disciplinas científicas para el estudio de la ciberseguridad

Una vez revisadas, de manera somera, algunas perspectivas teóricas de Relaciones Internacionales y su visión acerca del desarrollo del paradigma cibernético, es conveniente anotar que la política cibernética cruza un amplio conjunto de áreas temáticas, junto con cambios acordes con el discurso político y con las interacciones, generando efectos mundiales en la articulación y agregación de nuevos intereses, así como nuevos patrones en el escenario internacional, nuevos tipos de respuestas y acuerdos globales (Choucri, 2012, págs. 10-11).

En este aspecto, la política cibernética no es diferente (Valeriano & Maness, 2015, pág. 24). Como destaca el politólogo del Massachusetts Institute of Technology (MIT) Nazli Choucri (2012, pág. 9) “toda política, en la arena cibernética o no, involucra negociación, intercambio y conflicto sobre los mecanismos, instituciones y *normas* necesarios para resolver de forma acreditada las controversias sobre un conjunto de *valores* nucleares particulares”. De esa manera, la pregunta, acerca de quién tiene más poder cibernético (*cyber power*) se relaciona con las cuestiones de capacidades, recursos y prácticas de los actores. De acuerdo con Joseph Nye Jr. (2010, pág. 3) “el poder está supeditado al contexto, y el poder

cibernético está en función de los recursos que caracterizan el dominio del ciberespacio". La siguiente figura busca ejemplificar cómo se ejecutan estos ajustes, en qué niveles se llevan a cabo y cuáles son los efectos, que son multidireccionales, multidimensionales y multinivel.

Figura 1.2 Política internacional y seguridad cibernética



Fuente: elaboración propia

Por otra parte, hay una gran literatura técnica sobre seguridad de redes informáticas, así como una discusión emergente sobre los incentivos económicos y las fallas del mercado que dan forma al problema (Kramer, Starr, Wentz, & (eds.), 2009) (Hansen & Nissenbaum, 2009) (Lindsay J. R., 2015a) (Libicki M. C., 2009) (Owens W. A., Dam, Lin, & (eds.), 2009) (Singer & Friedman, 2014). Desafortunadamente para el análisis teórico, el contexto político internacional a menudo se pierde en el enfoque sobre la tecnología y sobre la utilización de ésta por grupos especializados. Para algunos estudiosos, la temática de la seguridad cibernética y su impacto sobre la seguridad internacional presenta dos problemas principales para su factibilidad como tópico de estudio sistemático y holístico, tanto dentro de Relaciones Internacionales como en el subcampo de los estudios de

seguridad internacional (Kello, 2013). El primero se refiere a la escasez de casos disponibles para proponer, probar y refinar afirmaciones teóricas sobre los fenómenos cibernéticos, y el segundo es la tendencia de los gobiernos a clasificar en exceso la información, lo que ha llevado a una brecha de datos significativa, ya que las maniobras tácticas más importantes en el ciberespacio permanecen envueltas en el secreto, lo que complica la investigación académica de los motivos y los objetivos del ataque cibernético como instrumento de política exterior y de defensa (Kello, 2013, págs. 9-10; Schmidt M. , 2012; Sanger D. , 2012).

Dentro del subcampo de estudios de seguridad de Relaciones Internacionales, en el estado del arte sobre seguridad cibernética, que aún es limitado, la mayoría de análisis presta poca atención a la interrelación de la ciberseguridad con temas políticos, económicos y sociales (Kramer, Starr, Wentz, & (eds.), 2009; Clarke & Knake, 2010; Demchak, 2011) (Reveron & (eds.), 2012) (Libicki M. C., 2007). Del mismo modo, los analistas de políticas de defensa han dirigido más sus esfuerzos hacia el problema de la interrupción a gran escala de la infraestructura crítica en lugar de prestar atención al desarrollo de interacciones cibernéticas más amplias, transversales y de largo plazo (Lindsay J. R., 2015a, pág. 5; Clarke & Knake, 2010; Valeriano & Maness, 2015).

Sin embargo, como recalcan Brandon Valeriano y Ryan C. Maness (2015) en su trabajo, aquí radica la relevancia de las personas dedicadas al estudio de Relaciones Internacionales, puesto que toda acción cibernética tiene una relación directa con la competencia y la rivalidad internacional, ya sea ésta interestatal o no.[10] Por ejemplo, algunos analistas invocan la lógica de Carl von Clausewitz para argumentar que, el peligro cibernético es exuberante porque la tecnología (en este caso los medios cibernéticos) no altera el carácter o los medios de la guerra (Kello, 2013, pág. 10; Rid, 2012). Además, otros afirman que los ataques cibernéticos no son violentos y no crean daños colaterales; por lo tanto, los nuevos fenómenos no deben calificarse como actos de guerra o como cuestiones de seguridad

[10] No obstante que su apunte es una llamada de atención relevante para la comunidad epistémica de la disciplina de Relaciones Internacionales, su enfoque solamente se centra en una cara de las prácticas estatales, el conflicto, dejando de lado el aspecto de colaboración.

internacional (Brito & Watkins, 2011) (Dunn Cavelty, 2008b) (Liff, 2012) (Morozov E. , 2009) (Rid, 2012).[11]

Por otra parte, hay quienes afirman que veremos una proliferación de la guerra cibernética porque la sociedad digital será una extensión lógica del dominio de seguridad (Rattray, 2001; Clarke & Knake, 2010; Kello, 2013), (Nye J. S., 2011). A su vez, otros argumentan que las amenazas cibernéticas y su proliferación son socialmente construidas y que debemos atenuar la elección de la terminología y de las metáforas para su análisis (*cyber war*, *cyber Armageddon*, *cyber 9/11*, entre otros), pues de esta manera crece la inflación de la amenaza (Hansen & Nissenbaum, 2009).

Asimismo, existen otros factores que condicionan la complejidad del estudio o magnifican la brecha entre lo cibernético y la dinámica internacional. Uno es que la nueva tecnología, en ocasiones es tan especializada que puede impedir la entrada a neófitos tecnológicos (Lindsay J. R., 2015b; Kello, 2013). Otra es la imbricación de temáticas de diversa índole como delitos informáticos, señales de inteligencia, "guerra electrónica", robo de identidad, protección de la privacidad, estafa electrónica, lo que hace confuso su abordaje y sistematización teórica (Choucri, 2012) (Nye J. S., 2011) (Lindsay J. R., 2015a, pág. 9).

Dentro del sector académico, hay observadores que afirman que el problema cibernético está plagado de peligros; por ello, cualquiera que intente abordarlo será abrumado por su complejidad (Walt S. M., 2010), una postura que busca evitar todo diálogo con la cuestión cibernética. De igual manera, un enfoque tradicional que enmarca una idea tradicional de la seguridad y el conflicto internacional, subraya que las amenazas que carecen de un carácter abiertamente físico o que no alcanzan el nivel de violencia interestatal son intelectualmente carentes de interés (Kello, 2013, pág. 11) (Buzan & Hansen, 2009).[12]

[11] En general, estas visiones parten de la definición que otorga sobre la guerra el grupo de investigación *Correlates of War* de la Universidad de Michigan, la cual definen como "un conflicto armado conducido por o entre entidades nacionales, en el que al menos uno de ellos es un Estado, en el cual resultan al menos 1,000 muertes en batalla de personal militar" (Valeriano & Maness, 2015).

[12] El estudio de la guerra y de la geopolítica constituyen importantes antecedentes para la preponderancia de este enfoque.

Para otros estudiosos, los efectos violentos de una supuesta "guerra cibernética" no necesitan ser letales para caer en la categoría conceptual tradicional de guerra (Stone, 2012, pág. 107). Una causa es que hasta finales de la Segunda Guerra Mundial, la guerra se estudió como historia militar o como derecho y filosofía del uso de las fuerzas armadas (Buzan & Hansen, 2009). Por su parte, la geopolítica se centró en cómo la posición geográfica, el espacio y las distancias repercuten en la proyección del poder (Herz, 2013) (Kirshner, 2010).

No obstante, existen esfuerzos académicos que realizan compendios sobre las diferentes perspectivas del debate sobre la seguridad cibernética y su relevancia en el entorno de seguridad internacional (Eriksson & Giacomello, 2007) (Kramer, Starr, Wentz, & (eds.), 2009) (Reveron, 2012) (Singer & Friedman, 2014) (Valeriano & Maness, 2015). El debate se puede subdividir en dos grandes perspectivas. Por un lado, una de éstas sostiene que la infraestructura interconectada hace que las potencias industriales avanzadas sean particularmente vulnerables a serias perturbaciones por parte de los Estados más débiles o incluso de actores no estatales, puesto que las herramientas de *hackeo* son cada vez de más fácil acceso (Nye J. S., 2011; Borg, 2005; Brenner, 2011; Clarke & Knake, 2010; Junio, 2013; Kello, 2013; Petterson, 2013; Rattray, 2001).[13]

Del otro lado del debate, distintos analistas argumentan que la industria de la defensa y el *establishment* de la seguridad nacional exageran en gran medida la intensidad de la amenaza cibernética (Dunn Cavelty, 2008b; Lawson S. , 2013; Ohm, 2008; Brito & Watkins, 2011; Morozov E. , 2009; Schneier B. , 2012). Dentro de este marco, otros afirman que las empresas privadas y actores que operan y gestionan un gran número de sistemas informáticos críticos suelen ser reacios a reportar incidentes cibernéticos perjudiciales debido a su potencial sobre costo de reputación y de otro tipo (Kello, 2013, pág. 10). Por último, otros estudiosos tratan de equilibrar la desacreditación de la retórica exagerada con evaluaciones sobre el

[13] Las herramientas de *hackeo* e instrumentos para realizar ataques como robo de identidad, desarrollo de *malware*, *ransomware* y otros propósitos nefarios han estado disponibles en los mercados en línea durante varios años, a costos relativamente baratos, lo que produce barreras de entrada al crimen cibernético sumamente bajas (CISCO/Cybersecurity Ventures, 2019).

potencial de los sustitutos emergentes para la agresión de baja intensidad y los complementos para la guerra de alta intensidad (Betz, 2012) (Gartzke, 2013) (Liff, 2012) (Lindsay, 2013) (Libicki M. C., 2007) (Rid, 2012).

Junto con la problemática de la ciberseguridad cibernética confluyen de manera implícita dos cuestiones teóricas que se engarzan de forma simultánea. Por un lado, la cuestión sobre la categorización semántica del concepto de seguridad, su ampliación conceptual, su múltiple dimensionalidad, sus marcos analíticos y la expansión de sus facetas más allá del ámbito militar y de defensa. Por el otro, se enlaza con el estudio sobre de la transición hegemónica internacional y el futuro político y económico de una potencia ascendente, las respuestas de la antigua potencia y la transformación en el sistema internacional actual.

De un lado de la intersección de esta última cuestion, se encuentran las dilucidaciones sobre las implicaciones que principalmente conlleva el ascenso de la República Popular de China respecto a la reconfiguración del orden internacional, en el cual confluyen una rica y variada gama de explicaciones de distinta índole. En términos generales, un sector académico sostiene que China está cada vez más integrada a las instituciones internacionales y a la economía global Estas, además, subrayan el hecho de que el gobierno chino está comprometido con el crecimiento y la estabilidad internacional para mantener su legitimidad al interior (Shambaugh, 1996; Ross, 1997; Drezner, 2009; Ikenberry, 2009; Steinfeld E. S., 2010; Christensen, 2015; Nathan, 2016).

Por otro lado, dadas las percepciones divergentes que sobre el tema de la seguridad (otros temas se pueden incluir) tienen tanto la República Popular de China como los Estados Unidos de América, sobresale el estudio de su competencia estratégica, cada vez más abierta, por el establecimiento de sus visiones, valores, intereses e identidades sobre una preeminencia hegemónica en función de sus respectivas posturas. Por otra parte, cabe considerar que ambos países han edificado una fuerte relación bilateral de interdependencia en diversos rubros, que comparten el estatuto de potencias en la arena internacional, y también son fuertes competidores en distintos dominios. Siguiendo esta lógica, en este trabajo se asume que la seguridad cibernética funge como una herramienta que, además de apoyar

en la búsqueda de la seguridad para ambos, es una estrategia de competencia por la hegemonía en el ámbito internacional que se ven reflejadas en las prácticas antitéticas sobre el orden global de seguridad.

Dentro de esta margen, algunos académicos y políticos argumentan que el poder económico y militar chino devendrá en una China más irracional, bélica y amenazante de la seguridad regional y global, esto junto con el declive relativo de los Estados Unidos, lo cual aumenta el potencial de agresión oportunista, error de cálculo en una crisis o guerra preventiva (Rachman, 1996) (Krauthamer, 1995) (Layne, 2009) (Jacques M. , 2009) (Friedberg, 2011) (Dobbins, 2012) (Kirshner, The Tragedy of Offensive Realism: Classical Realism and the Rise of China, 2010) (Kupchan, 2012) (Pillsbury, 2015).

En el otro vértice del empalme analítico, se encuentran diversos trabajos que buscan explicar los cambios o transformaciones de la hegemonía internacional, así como también se puede localizar una postura intermedia que pretende comprobar y explicar la existencia y la magnitud de un cambio en el poder hegemónico en el sistema internacional, enfocado particularmente en la disputa entre la República Popular de China y Estados Unidos (Morales, 2018) (Rocha & Morales, 2018) (Gilpin R. , 1981) (Keohane R. , 1984) (Goldstein, 2015) (Kennedy, 1987) (Tammen & (ed.), 2000) (Starrs, 2013) (Johnston, 2013) (Layne, 2009) (Layne, 2006) (Li R. , 2009) (Foot & Walter, 2010) (Schweller & Pu, 2011) (Beckley, 2011) (Shambaugh D. , 2013) (Friedberg, 2011). Por último, las potencias mundiales han comprendido que la protección de la información es un elemento estratégico para la preservación de su dominio y control. Por ello, el análisis del nexo entre estos debates teóricos es imprescindible para comprender el balance entre seguridad del dominio digital, competencia hegemónica y reafirmación o recomposición del *statu quo* internacional y la transformación de las prácticas en esta estructura digital.

Capítulo 2. La ciberseguridad y la teoría de Relaciones Internacionales: sus dimensiones y alcances

Introducción

En el presente capítulo se revisa y delinean las bases teóricas que fungen como guías conceptuales para la observación de las dimensiones, alcances y el papel que juega la *ciberseguridad* en la teoría de Relaciones Internacionales y, en particular, en los estudios de seguridad internacional. Esto permite entender en qué medida este concepto ha influido sobre las acciones estatales en el ciberespacio, dando forma a sus intereses y preferencias. Aquí, el interés académico es la búsqueda de un posicionamiento que tienda puentes de colaboración entre la disciplina de Relaciones Internacionales, el subcampo de estudios de seguridad internacional y el desarrollo tecnológico.

Primero, es importante subrayar que, para teorizar sobre la ciberseguridad se requiere plantear las siguientes interrogantes: ¿qué amenazas y objetos referentes caracterizan la ciberseguridad?; ¿qué distingue a la ciberseguridad de otros sectores de la seguridad?; ¿cuántos ejemplos concretos de securitización cibernética pueden ser analizados?; ¿qué se puede aprender al analizar el discurso de la seguridad cibernética? (Hansen & Nissenbaum, 2009, pág. 1157). En el caso de la ciberseguridad se considera que el enfoque constructivista de Relaciones Internacionales puede tender un puente teórico importante para algunas de las contradicciones persistentes en el debate de la seguridad (especialmente en su variante cibernética) y en su dimensión internacional.

En Relaciones Internacionales, ontológicamente, los Estados han sido las partes constituyentes del sistema internacional, así como un actor preponderante en la política mundial. Sin embargo, por un lado, las realidades globales a principios del siglo XXI están ampliando la concepción sobre los cimientos en los que se sustentan las interacciones internacionales y, por otro lado, éstas incitan a repensar los preceptos claves que han articulado la disciplina, como la *seguridad*.

En relación con lo anterior, todavía no hay consenso sobre los próximos pasos a seguir para incorporar al espacio cibernético en el discurso contemporáneo sobre *soberanía*, estabilidad y *seguridad*, no obstante, esta tesis es un esfuerzo académico en esa dirección (Choucri, 2012, pág. 13). Existen diversas posturas sobre el papel que desempeña la ciberseguridad en la realidad internacional y en la dinámica de la política global. Con el objeto de esclarecer los elementos teóricos de este trabajo de investigación, se hace una síntesis general sobre aquellas posturas con más adeptos sobre la incorporación o la desagregación del concepto *ciberseguridad* en la disciplina de las Relaciones Internacionales y las implicaciones conceptuales de su utilización. Para efectos de este capítulo, la revisión de estas posiciones en su conjunto arroja claridad explicativa sobre la continuidad, el cambio, el contexto y la estructura de interacción entre los actores estatales y el desarrollo tecnológico.

2.1 Procesos de securitización en el ciberespacio[14]

Cuando se debaten incidentes cibernéticos o temores de posibles incidentes, es importante separar la idea de vulnerabilidad de la de amenaza. Por ejemplo, los aspectos determinantes de las amenazas son el actor y la consecuencia. Además, el reconocimiento de un actor nos obliga a pensar estratégicamente sobre las amenazas y comprender que la amenaza puede evolucionar en respuesta a determinadas acciones defensivas (Singer & Friedman, 2014, pág. 38). En otras palabras, como lo asevera la Escuela de Seguridad de Copenhague, “los problemas se convierten en un tema de seguridad no necesariamente porque existe una amenaza existencial real, sino porque el problema se presenta y establece con éxito por agentes clave, como una amenaza” (Buzan, Waever, & de Wilde, 1998).

[14] Este concepto es un anglicismo (*securitization*) cuya traducción significa que un fenómeno de carácter público se convierte en un asunto de seguridad porque se presenta y establece en la agenda política como una amenaza, aunque no exista evidencia que sustente dicha condición. Se usa indistintamente en relación con su acepción en inglés, puesto que o existe un consenso sobre una traducción reconocida oficialmente para el idioma español.

Una de las razones por la que los gobiernos piensan que el ciberespacio es amenazante para la seguridad es que un ataque cibernético puede moverse a gran velocidad, ilimitado por geografía y espacios políticos. Esta desvinculación física también se traduce en que puede estar en múltiples lugares al mismo tiempo, lo que significa que el mismo ataque puede alcanzar múltiples objetivos a la vez (Singer & Friedman, 2014, págs. 68-69). Sin embargo, un ataque cibernético difiere de un ataque físico en el objetivo, en lugar de causar daño material directo, un ataque cibernético siempre se dirige primero a otro dispositivo o máquina y a la información que contiene. Los resultados previstos del ataque pueden dañar algo físico, pero ese daño siempre es el primer resultado de un incidente en el ámbito digital (Singer & Friedman, 2014, pág. 69). Por esa razón, un problema cibernético sólo se convierte en un problema de ciberseguridad si se busca obtener algo de la actividad, ya sea conseguir información privada, socavar el sistema, evitar su uso legítimo o destruirlo.

De acuerdo con diversos criterios de la comunidad de la seguridad de información (InfoSec), para que una acción cibernética pueda ser representada como una problemática de ciberseguridad debe violar los principios de *confidencialidad*, *integridad* y *disponibilidad* (*confidentiality, integrity, availabiltiy*, C-I-A) (Klimburg, 2017) (Singer & Friedman, 2014) Primero, la *confidencialidad* se refiere a mantener los datos privados. La privacidad no es solo un objetivo social o político. En un mundo digital, la información es la esencia del valor, proteger esa información es, por lo tanto, primordial. (Singer & Friedman, 2014, pág. 35). Segundo, la *integridad* significa que el sistema y los datos que contiene no han sido alterados o modificados indebidamente sin autorización. Por último, la d*isponibilidad* significa poder usar el sistema como está previsto (Singer & Friedman, 2014, pág. 35). Además de estas propiedades, debe añadirse la *resiliencia*. Esta es lo que permite a un sistema soportar amenazas de seguridad en lugar de fallar críticamente, se trata de la permanencia operativa en el supuesto de que los ataques e incidentes ocurren de manera continua (Singer & Friedman, 2014, pág. 36).

No obstante, no todas las transgresiones, infracciones, intromisiones o desacatos pueden caer en el mismo rubro de ciberseguridad. Como bien lo recalcan algunos expertos, “la escala y el impacto son absolutamente claves para tratar de sopesar las implicaciones de los ataques cibernéticos” (Singer & Friedman, 2014, pág. 70) (Valeriano & Maness, 2015). Asimismo, P.W. Singer y Allan Friedman subrayan que “sopesar este tipo de ataques depende tanto de la información extraída como de la escala del esfuerzo” (Singer & Friedman, 2014, pág. 71). Por esta razón, la idea de que el conflicto es la base de las interacciones cibernéticas a nivel interestatal es confusa y problemática. Como mencionan algunos autores, “existe el peligro de mal interpretar la amenaza que proviene de individuos cibernéticos no estatales y de las amenazas que proceden de actores cibernéticos afiliados al Estado, pero no directamente empleados por los gobiernos” (Valeriano & Maness, 2015, pág. 4).

Para algunos analistas la arena del “ciberespacio es la principal zona de conflicto internacional” (Clarke & Knake, 2010; Li Z. , 2016; Lewis, 2018), donde se observa que el enfoque dominante es “el desarrollo de un proceso de construcción de la amenaza cimentado en el miedo” (Valeriano & Maness, 2015). No obstante que, el miedo asociado con las acciones del 11 de septiembre de 2001 se ha disipado, para algunos autores, en cierta forma, ha sido reemplazado con el miedo de un posible conflicto cibernético, e incluso de una guerra cibernética (Valeriano & Maness, 2015, pág. 2; Klimburg, 2017).

Ciertamente, con la emergencia de una sociedad digital y una creciente interconectividad en un mundo cada vez más globalizado, algunos especialistas y gobernantes argumentan que la sociedad debe preocuparse por la vulnerabilidad que estas interconexiones traen consigo (Clarke & Knake, 2010; Chappell, 2015). Asimismo, los efectos políticos que han provocado algunos eventos internacionales relacionados con el entorno cibernético han aumentado esa ‘sensación de peligro’.

Por ejemplo, escándalos como el monitoreo indiscriminado que viene realizando la *National Security Agency* de los Estados Unidos (NSA, por sus siglas en inglés) y sus efectos sobre la privacidad personal digital genera incertidumbre sobre el alcance de la vigilancia realizada por gobiernos. De igual manera, las

filtraciones hechas por la organización *Wikileaks* sobre el mal comportamiento y malas prácticas de empresas y Estados alrededor del mundo y las revelaciones sobre los programas de captura de datos indiscriminada realizadas por el ex contratista de la NSA Edward Snowden, producen un sentimiento de vulnerabilidad.

Por otro lado, el desarrollo de armas cibernéticas como *Stuxnet* o el papel de las redes sociales en las movilizaciones sociales como la Primavera Árabe, actividades de espionaje cibernético a gran escala realizadas por gobiernos o por grupos auspiciados por estos, así como mecanismos de filtrado de información que socavan la privacidad personal de las personas o la posible intervención extranjera en elecciones de otras naciones ayuda a incrementar la hipérbole y aumenta la ansiedad sobre la 'amenaza cibernética' (Klimburg, 2017; Valeriano & Maness, 2015).

Por otra parte, la esperanza y la promesa que generaban las tecnologías de comunicación e información se ha fusionado con una especie de "ansiedad cibernética" (Singer & Friedman, 2014, pág. 3). Con el advenimiento de la era digital de comunicaciones cibernéticas, este proceso de construcción del miedo continúa formando los diálogos en las relaciones internacionales, por ello, el ciberespacio se está convirtiendo en una nueva área de disputa en las interacciones internacionales (Valeriano & Maness, 2015, pág. 1).

Del lado gubernamental, ha llevado a la creación de nuevas oficinas gubernamentales y agencias gubernamentales relacionadas con la ciberseguridad y a un aumento presupuestario para poder realizar estas tareas (Klimburg, 2017). Como muestra, un mayor número de naciones están recurriendo cada vez más a estas herramientas, lo que para algunos autores "puede socavar los beneficios económicos y de derechos humanos que han florecido con la conectividad global" (Klimburg, 2017, págs. 301-313). Además, la cuestión es tan grave que "todas estas tendencias convergen en una 'tormenta perfecta' que amenaza los valores tradicionales de Internet, como son la apertura, la colaboración, la innovación y el intercambio libre de ideas" (Bonner, 2011; Wu, 2011).

Por su parte, en el sector empresarial, se desarrolla un floreciente negocio de ciberseguridad. Algunas estimaciones, mencionan que la escala global del

complejo industrial de ciberseguridad oscila entre $80 mil millones y $150 mil millones de dólares anualmente (Schmidt & Cohen, 2013, pág. 110), es por ello que algunas la califican como “una de las industrias con más rápido crecimiento en el mundo” (Singer & Friedman, 2014, pág. 3). Asimismo, las nuevas conexiones y controles operacionales cibernéticos pueden crear condiciones que al momento de interactuar producen debilidades en la dinámica de seguridad que son críticas para la supervivencia (Valeriano & Maness, 2015, pág. 2). No obstante, con el fin de proveer de una narrativa alternativa al del discurso del miedo, este trabajo de investigación pretende presentar evidencia sobre la construcción social de la amenaza cibernética y cuáles son las implicaciones para el escenario de seguridad internacional. El propósito de lo anterior es descubrir si estas construcciones públicas están respaldadas con hechos y evidencia empírica o si realmente son exageraciones discursivas (Valeriano & Maness, 2015, pág. 3).

2.2 La ciberseguridad y las relaciones internacionales

En primer lugar, el paisaje cibernético internacional está cambiando las relaciones de poder, influencia y seguridad entre diversos actores. En términos de las relaciones internacionales actuales no está claramente observado qué significa ni que implica esa modificación. A pesar de que, el ciberespacio ha sido edificado, manejado y operado primordialmente desde el sector privado, los agentes estatales han estado rivalizando ese predominio desde la primera década del siglo XXI. Sobre todo, puede decirse que los actores estatales “son actores que arribaron tarde al terreno, pero que desean recuperar el tiempo perdido” (Deibert, Palfrrey, Rohozinski, & Zittrain, 2008).[15]

De ahí que, algunas opiniones plantean que las realidades cibernéticas “socavan la supremacía del Estado de manera notable” (Kahin & Nesson, 1997; Khanna, 2016). De manera específica, para el profesor de la Universidad de Syracuse Milton L. Mueller (2010, pág. 4), el ciberespacio pone presión sobre el

[15] Sobre el debate de la incursión estatal en el ciberespacio y sobre la búsqueda de preeminencia dentro de esta área, se profundizarán sus elementos en el siguiente capítulo de esta investigación.

Estados de cinco maneras distintas: *1)* globaliza el alcance de la información; *2)* facilita un salto cuántico en la escala de la comunicación; *3)* distribuye el control de información estratégica; *4)* crea nuevas instituciones y; *5)* cambia la naturaleza de los procedimientos gubernamentales.

Desde este punto de vista, el ciberespacio está destruyendo el vínculo entre la ubicación geográfica y el poder de los gobiernos para ejercer control sobre el comportamiento de sus ciudadanos en el espacio digital. Además, bajo este enfoque, se subraya que la legitimidad y los esfuerzos gubernamentales para ejecutar reglas aplicables a fenómenos globales está en entredicho, así como la pérdida de habilidad de la ubicación física para notificar qué conjuntos de reglas se aplican, por quién y de qué manera (Choucri, 2012, pág. 13).

Por el contrario, otra línea de pensamiento sostiene que, a pesar del poder emergente que brinda Internet a la ciudadanía, los fundamentos de poder y autoridad del Estado siguen siendo sólidos, como se revela en distintos esfuerzos exitosos y no exitosos de gobiernos, tanto democráticos como autoritarios, para regular la transmisión de contenido y de información (Goldsmith & Wu, 2006; Deibert R. , Palfrey, Rohozinski, & Zittrain, 2010; Klimburg, 2017). En este tenor, algunos autores argumentan que las personas pueden ser incluso más vulnerables y contar con menos herramientas de acción, no sólo para salvaguardarse de las acciones pendencieras de los Estados, sino también, de los esquemas comerciales de grandes conglomerados digitales sobre el manejo de su información personal con fines de lucro (Schneier B., 2015; Vaidhyanathan, 2018; Pariser, 2011).

Dentro de esta postura, se recalca que el terreno digital no está completamente desvinculado con respecto a la geografía, incluso las normas técnicas específicas que permiten su operación pueden reforzar los fundamentos de los límites de autoridad (Goldsmith & Wu, 2006; Morozov E. , 2011; Klimburg, 2017; Edde, 2018). Sin embargo, otro punto de vista sugiere que el ciberespacio es fundamentalmente (re)generativo en términos tanto tecnológicos como sociales, y ello contribuye a (re)plantear las concepciones de autoridad y el papel del Estado, sobre todo en la provisión de bienes públicos (Zittrain, 2008; Shirky, 2011; Naím, 2014). Este punto de vista sostiene que la red digital empodera a los ciudadanos,

facilita la innovación y permite la construcción de una esfera pública internacional, así como un sinnúmero de posibilidades aún no exploradas (Castells, 2009; Shirky, 2011).

En efecto, todas estas actividades pueden retar las interpretaciones tradicionales de la seguridad, pero, al mismo tiempo, el ciberespacio provee nuevos sitios para el ejercicio del poder estatal y permite la (re)orientación de la autoridad y territorialidad como principios fundamentales para la justificación de decisiones, elecciones y acciones en esta arena (Choucri, 2012) (Hansen & Nissenbaum, 2009) (Valeriano & Maness, 2015).[16] Dentro de esta postura se sostiene que a través de las prácticas como la *securitización* del espacio digital, diversos Estados pretenden legitimar y justificar sus acciones a través de referencias que enfatizan la necesaria protección de valores culturales-nacionales y de la seguridad nacional o seguridad del régimen y que permitan el establecimiento de sitios de apuntalamiento que apoyen y confirmen la necesidad de medidas urgentes y necesarias.

2.2.1 El constructivismo y la ciberseguridad

Ante de profundizar sobre el proceso de securitización y el enmarcado de la amenaza cibernética, así como las acciones que promueven los Estados para dar respuesta a ésta, este apartado busca exponer sucintamente un apalancamiento teórico sobre cómo se modelan las preferencias de los agentes, su influencia sobre sus decisiones y las implicaciones de sus interacciones. Para ese propósito se utiliza la aproximación teórica constructivista de Relaciones Internacionales.

En primer lugar, el constructivismo es una teoría cuya ontología de mutua constitución entre agencia y estructura permite entender que tanto los agentes como las estructuras se constituyen mutuamente en el proceso de interacción social (Klotz & Lynch, 2007, pág. 41). En otras palabras, se puede argumentar que, en el proceso de construcción social, el flujo de interacción que establecen originalmente entre sí

[16] Mientras que los cimientos de la soberanía se encuentran localizados en el derecho internacional, las realidades sobre el terreno cibernético imponen limites sobre la autoridad y el control estatal (Choucri, 2012, pág, 241).

entidades autónomas, crea de hecho un nuevo ámbito; una dimensión cualitativamente diferenciada de la realidad social y una nueva dinámica de acción entre los seres humanos (Santa Cruz, 2000, pág. 117); es decir, "los actores no reproducen mecánicamente las estructuras, sino que las alteran por medio de la práctica" (Kratochwil & Ruggie, 1986).

Al mismo tiempo, el planteamiento constructivista subraya que las estructuras clave del sistema internacional son intersubjetivas, y que las identidades y los intereses de los agentes son construidos fundamentalmente por las estructuras sociales (Bukovansky, 1999) (Santa Cruz, 2000, pág. 166). Además, este enfoque analítico sostiene que estos elementos son 'construcciones intersubjetivas'.[17] Asimismo, sustenta que la política internacional no es armónica, pero que simplemente las capacidades sin consideración intersubjetiva, no son suficientes para desarrollar una teoría estructural de la política mundial, *en este caso la política mundial cibernética* (Santa Cruz, 2000, pág. 167).

Por ello, para este trabajo de investigación se elige el enfoque constructivista de Relaciones Internacionales porque se considera útil y pertinente, debido a que es un planteamiento estructural, que sugiere que "los agentes y las estructuras se constituyen recíprocamente, en pocas palabras no se pueden explicar unos sin los otros" (Wendt A. , 1987). Por un lado, el constructivismo tiene una estrecha relación con el realismo científico y la teoría de la estructuración.[18] Por otro lado, el constructivismo es interpretativo en tanto que niega que las teorías sean válidas sólo si corresponden inequívocamente con los hechos que se presentan en la realidad externa (Santa Cruz, 2000, pág. 162). Sin embargo, a diferencia de otros

[17] Es decir, las estructuras sociales no son objetivas como, por ejemplo, un océano, pero tampoco son mera subjetividad, como sería el caso de los sueños (Wendt, 1992).

[18] De acuerdo con esta escuela de pensamiento, los objetos sociales no son reducibles ni equiparables directamente a los objetos naturales, por lo que no pueden ser estudiados de la misma manera. Sin embargo, la diferencia entre los objetos naturales y sociales no significa que el estudio científico de los últimos no sea posible, sino que el proceso mediante el cual se lleva a cabo la investigación es diferente (Santa Cruz, 2013, pág. 39)

enfoques interpretativos, el constructivismo considera que "sí existe una realidad externa que constriñe y genera acción social" (Shapiro & Wendt, 1992).[19]

Además, su pertinencia como herramienta analítica también radica en su capacidad para explicar el cambio y la transformación, asociada primordialmente a su génesis como enfoque teórico dentro de las Relaciones Internacionales. Como resultado de la incapacidad de los enfoques tradicionales de la disciplina para anticipar, explicar y predecir el final de la Guerra Fría (en especial la forma en la que finalizó) abrió la puerta para la entrada de la perspectiva constructivista y su orientación a la interpretación de las transformaciones (Kratochwil, 1993). Por esa razón, a finales de la década de 1980, a este programa emergente de investigación se le llegó a denominar *reflexivista* (Santa Cruz, 2013, pág. 38).[20]

Al mismo tiempo, otra razón más para la elección de este enfoque es que ofrece puentes entre los niveles de análisis, y en el plano teórico permite explorar los múltiples mecanismos que conectan a lo internacional con lo interno (Santa Cruz, 2000). Por ejemplo, John G. Ruggie utiliza el concepto de "densidad dinámica" para referirse a la cantidad, velocidad y diversidad de transacciones que tienen lugar en una sociedad (Ruggie J. G., 1983). De acuerdo con él, la correcta determinación del concepto contiene tanto efectos estructurales como procesos agregados a nivel unitario, y ya que en cualquier sistema social el cambio estructural debe venir de los procesos a nivel de las unidades, su inclusión en el análisis lo hace más sensible a procesos transformativos (Santa Cruz, 2000, pág. 82).

Debido a que es un enfoque que llegó recientemente a la disciplina de Relaciones Internacionales, muchas de las premisas nucleares siguen siendo cuestión de debate, tanto por los enfoques racionales y tradicionales de la disciplina de Relaciones Internacionales, como en su interior y en sus propias distinciones

[19] Ian Shapiro y Alexander Wendt (1992) hacen la distinción entre constructivistas modernistas y postmodernistas, lo que estos grupos tendrían en común es, que están interesados en las prácticas que constituyen a los sujetos, así como en lo que se refiere a las identidades e intereses (Santa Cruz, 2000, pág. 162). E trabajo se centrará en la variante modernista.

[20] El enfoque constructivista niega que el individuo sea la unidad de análisis adecuada para la teoría social, pero al considerar que existe una realidad externa, niega también que todo se reduzca a una mera interpretación subjetiva.

(López, 2015).[21] Cabe notar, sin embargo, que el constructivismo no es una teoría sustantiva de la disciplina. Se trata más bien de una inclinación filosófica o marco analítico amplio para analizar la política mundial (Santa Cruz, 2013, pág. 38).

Y aunque sigue siendo un marco social analítico en consolidación para los fenómenos sociales, el enfoque constructivista ha producido importantes contribuciones empíricas en temas tan diversos y relevantes para las Relaciones Internacionales como la anarquía, la soberanía, la *seguridad*, los cambios en y entre los sistemas internacionales, regímenes internacionales, intervención militar y derechos humanos (Santa Cruz, 2013, pág. 38). Por ello, se considera valiosa su capacidad explicativa para analizar el importante papel de las acciones estatales en el dominio digital y los efectos sobre una posible transformación en la constitución del entorno de ciberseguridad.

Primero, en el constructivismo, la estructura está constituida por tres elementos: *conocimiento compartido*, *recursos materiales* y *prácticas sociales* (Wendt A. , 1995). Luego, mantiene que los intereses y sus acciones relacionadas no pueden entenderse sin considerar los entendimientos compartidos (entendimientos intersubjetivos) que constituyen cualquier sistema de interacción social (Bukovansky, 1997). En suma, se parte del principio de que los actores sociales se relacionan con otros objetos y entre ellos sobre la base del significado colectivo (Santa Cruz, 2000, pág. 168).

Asimismo, el constructivismo reconoce la influencia de las *ideas*, las *percepciones*, y los *intereses* sobre el producto final de las interacciones sociales internacionales (Campbell, 1998). Con base en esto, el constructivismo considera que el significado que se les otorga a las acciones humanas no es meramente descriptivo sino *constitutivo*, pues el proceso mismo de interpretación las constituye como referentes sociales, lo cual da soporte para la explicación de la construcción

[21] Existen cuatros genealogías reconocidas en el constructivismo. La primera división se da en lo que se conoce como constructivismo moderado (moderno o convencional) y el crítico. En un segundo nivel, la diferencia es entre tres visiones: moderno, consistente y crítico, a los cuales también se les identifica como positivista, interpretativista y posmoderno. En un tercer escalafón de diferenciación se encuentra el modernista, el modernista lingüista, el crítico y el posmoderno. En una cuarta distinción se localiza el sistémico, el de unidad constitutivas y el holístico (Santa Cruz, 2009) (Wendt, 1992). Cabe resaltar que, las diferencias son más bien de énfasis o de lenguaje que sustantivas (Santa Cruz, 2013).

binaria en el campo de la seguridad internacional, en virtud de los comportamientos diferentes y el de referenciación de los objetos (amigo-enemigo, tranquilidad-intranquilidad, amenazante-inofensivo) (Wendt, 1992). En suma, el entendimiento compartido constituye las estructuras que organizan las acciones de los actores. En otras palabras, la estructura digital internacional está constituida por algo más que las meras capacidades materiales, así como el enmarcado de la amenaza cibernética (Wendt,1992; Santa Cruz, 2013).

De acuerdo con el constructivismo, “los recursos materiales no se les puede concebir aisladamente de las ideas que los identifican como tales” (Santa Cruz, 2000, pág. 169). Esto significa que, los fundamentos físicos e infraestructuras que permiten el desarrollo del campo cibernético no tienen significado alguno sin la apropiación y usos que los agentes le otorguen, lo que generan un proceso de formación estructural contingente. Esto contribuye a falsear o verificar la premisa de que las prácticas de los agentes tienen efectos directos sobre la reestructuración de las normas conductuales digitales, pero que éstas a su vez también son modificadas por las acciones de otros actores. Parafraseando y reconstruyendo el famoso aforismo de Alexander Wendt (1992) “hacer que el ciberespacio sea lo que los Estados quieran de él”. (Deibert R. J., 2013).

2.2.2 Constructivismo: identidad, prácticas sociales y cambio

Por otra parte, en el ámbito de la conformación de los intereses, primordialmente en la *mutabilidad* de éstos, el constructivismo indaga sobre la problematización de los intereses a través de su coligación con las identidades, para mostrar que ambos están determinados por su elaboración social en un contexto espacial y temporal específico. Además, las prácticas regularizadas son el enlace entre agentes y estructura, pues funcionan como mecanismo de reproducción mutua (Santa Cruz, 2013).

Dentro de este orden de ideas, en relación con las identidades de los actores, Alexander Wendt (1992, pág. 397) menciona que son “conceptualizaciones específicas del papel y las expectativas que tienen los actores acerca de sí mismos”. Por su parte, Arturo Santa Cruz (2000, pág. 174) argumenta que “las identidades no

son estáticas, ni tienen esencia, pero se consolidan mediante la interacción social". Como complemento, Ted Hopf (1998) indica que "las identidades [e intereses] de un actor conforman una variable que depende de los contextos histórico, cultural, político, social y espacial" (Bravo, 2017). En efecto, como menciona Mlada Bukovansky (1999) "los principios que constituyen la identidad de los actores moldean la estructura del sistema internacional", por lo que la introducción de un nuevo concepto que cuestione las normas establecidas puede tener efectos sistémicos (Santa Cruz, 2000, pág. 167).[22]

Justamente, las identidades realizan tres funciones necesarias en la sociedad: *1)* señalamiento; *2)* interpretación; y *3)* respuesta. En otras palabras, les dicen a los agentes quiénes no son, quiénes son los otros y enmarca la forma de interacción (Bravo, 2017).[23] Al decir a los agentes quiénes son, "las identidades reflejan un conjunto de intereses y preferencias respecto a las elecciones disponibles para la ejecución de sus acciones. Asimismo, las identidades reflejan la posición de un agente frente a los demás y permiten la percepción acerca de la posición de los demás frente a él" (Bravo, 2017, pág. 877).

En efecto, esta articulación analítica permite tener una base explicativa sólida para comprender el abanico de acciones estatales dentro del ciberespacio y sus efectos sobre el cambio de la constitución de la ciberseguridad a nivel global. Cabe recordar que, en su génesis los actores no estatales configuraron las monturas, el diseño, y desarrollaron gran parte de la estructura digital actual con valores

[22] La legitimidad es la percepción o reconocimiento del derecho de alguien de ostentar o tener autoridad. Dentro del campo de la sociología, Max Weber estableció una tipología del poder en función de los motivos o de los objetivos que pretenda cada dominación. En palabras de Weber "el tipo de motivo caracteriza en gran medida el tipo de dominación". Con esto, se da pie para el funcionamiento de la dominación, la creencia en la *legitimidad*. Para mantener esa legitimidad, se deben procurar mecanismos que la cuiden y la mantengan. Según sea el tipo de legitimidad pretendida, así será el tipo de obediencia y el tipo de aparato administrativo que la garantice y la índole del ejercicio de dominación y sus efectos. (Weber, 2009, pág. 61).

[23] Como lo demostró en su obra clásica Edward Said, los actores construyen representaciones del "otro" significativo, incluso antes de entrar en contacto con ellos (Said, 1978). Estas preconcepciones sugieren que la estructura depende, por lo menos en parte, de las ideas, propósitos e intenciones que los actores traen consigo al encuentro con otros. Esto podría dar pauta a explicar la acción gubernamental en el ciberespacio y por qué han elegido tener un enfoque que pone el acento en las consideraciones de seguridad antes que en cuestiones como operatividad, funcionamiento y resiliencia del sistema.

inherentes a esta y, la injerencia o participación activa de los agentes estatales es más reciente, que pretende enmarcar y (re)configurar una nueva estructura normativa, especialmente en el rubro de la seguridad (Levy, 2010; Lessig, 2006).[24] Por consiguiente, es necesario analizar el rango y profundidad de las prácticas estatales y los efectos que generan sobre una nueva cimentación del espacio digital, y en particular, sobre la ciberseguridad.

2.2.3 Estructura, identidad e intereses en el ciberespacio

Justamente, se pueden encontrar dos posturas relacionadas con las prácticas estatales en el dominio cibernético, por un lado, algunos gobiernos y organizaciones internacionales han identificado el terreno digital como un nuevo dominio estratégico (aunado a la tierra, mar, aire y espacio ulterior) donde debe llevarse a cabo una intervención amplía puesto que aquí es donde se desempeñará una lucha clave por la preponderancia global. Dentro de esta perspectiva, esta visión menciona que debe existir una injerencia profunda en la gestión de los asuntos cibernéticos bajo un marco internacional normativo consensuado, muy parecido a la práctica diplomática internacional tradicional (Mueller M. L., 2010; Riordan, 2019). Por otro lado, hay una perspectiva que subraya la importancia de mantener las condiciones de gestión y gobernabilidad del esquema digital global actual (*multistakeholder governance*), el cual insiste en un modelo de múltiples-partes interesadas que propugna por una participación gubernamental limitada (Klimburg, 2017, págs. 105-110) (DeNardis, 2014). En resumen, ambas comparten una aclamación por un mayor juego en la conformación de la arena digital.

Por otra parte, es necesario subrayar que los agentes sociales no tienen intereses inherentemente específicos desde el momento en que sus identidades son conformadas, pues, desde la perspectiva constructivista "los intereses son construcciones sociales hechas por los actores como objetos que producen una

[24] Los principios o valores que estructuraron en un principio el espacio digital son el intercambio igualitario y la circulación libre y gratuita de la información en el marco de una red cooperativa gestionada por sus usuarios (Mattelart, 2007, pág. 66). También se le conoce como la "doctrina del libre flujo de información" (*free flow of information*).

serie de significados intersubjetivos establecidos para comprender el lugar que un agente ocupa en la estructura del sistema en un determinado tiempo" (Bravo, 2017, pág. 877) (Weldes, 1996, pág. 275). En suma, la explicación acerca de la conformación de la identidad y los intereses nos permite realizar cuestionamientos como, ¿quién representa una amenaza cibernética para quién?, una práctica común en el discurso enmarcado por la seguridad (particularmente en la variable cibernética).

Como lo señala Alexander Wendt (1987) el problema agente-estructura tiene sus orígenes en dos axiomas de la vida social: *1)* que los individuos y sus organizaciones son actores propositivos cuyas acciones contribuyen a (re)producir o transformar la sociedad en la que viven; y *2)* que la sociedad está compuesta de relaciones sociales, las cuales estructuran las relaciones entre los actores. Si bien no pueden rechazarse del todo los factores materiales, en un sentido amplio, la identidad, la ideología y la cultura cobran un papel causal pleno en la vida social (Wendt A. , 1999, pág. 108).

En relación con lo anterior, el primer desafío es reconocer y representar las interconexiones críticas entre los sistemas de interacción, no sólo los sistemas sociales y ambientales, sino también el sistema cibernético, un sistema con cualidades distintivas cuyas características difieren de las interacciones del sistema social o el sistema ambiental.[25] Es por eso, que una propuesta teórica debe tener en cuenta la intersección del entorno *cinético* y la construcción del ámbito *cibernético* (Choucri, 2012, págs. 15-16). Para ello, una forma de abordar los ejes de intersección entre estructura, identidad e intereses en el espacio cibernético es por medio del análisis de los principios constitutivos del sistema, y cuáles son las nuevas contribuciones que buscan cambiar estos elementos, cuestiones que serán profundizadas en el siguiente capítulo de esta investigación.

[25] En ocasiones esa separación tajante no se realiza en la práctica, antes bien, se observa un traslape de acción e intercambio espacial en los tres terrenos.

Asimismo, el segundo desafío es abordar la dinámica de transformación y cambio; comprender que se requiere de un análisis a profundidad de los factores subyacentes que dan forma a la naturaleza de la transformación (Gilping, 1987).[26] Por tanto, el reto es examinar las raíces del cambio y sus interconexiones. Se reconoce que las interacciones basadas en el ámbito cibernético influyen en todos los niveles de análisis de las actividades humanas, sin embargo, el enfoque de este trabajo no se centra en la experiencia del individuo, sino en su conformación sistémica. Bajo esta lógica de reflexión, también se pretende utilizar las propuestas de las imágenes sociales y los niveles de análisis, para comprender dichos enlaces, su interconexión y sus traslapes.[27] No obstante, este trabajo de investigación se aboca principalmente entre el segundo nivel de análisis de Waltz (1959) y sus posibles impactos en el tercer nivel de análisis.

Con este trabajo, se presentan dos cuestionamientos implícitos, apoyados en las propuestas de Peter Katzenstein (1985), uno sobre la desdibujada división canónica entre temas de "alta" política y "baja" política, y el segundo que enfatiza la no tan clara distinción entre la política internacional y la política doméstica. Con base en ello, se justifica la importancia de estudiar las percepciones estatales sobre la ciberseguridad para así comprender sus efectos sistémicos y su influencia sobre la composición del entorno cibernético global (Santa Cruz, A., 2012, pág. 14). En suma, la explicación acerca de la conformación de la identidad y los intereses nos

[26] Robert Gilpin (1987) argumenta que, en el corto plazo, la distribución del poder y la influencia en el sistema internacional conforma las reglas de interacción y el marco para la conducta política y económica. En el largo plazo, los cambios en la eficiencia y el desempeño económico alteran la distribución del poder prevaleciente y cambian la estructura del sistema internacional. Estos cambios están conformados por el poder y las preferencias del Estado ascendente, cuya nueva posición de poder le permite reclamar en el sistema internacional, así como influir en las reglas y regulaciones que rigen las relaciones entre Estados. Esta lógica general tiene cierto grado de portabilidad en el ciberespacio (Choucri, 2012, pág. 242). En este trabajo, se considera el ciberespacio como un elemento relevante y una consecuencia de la transformación y el cambio, sin embargo, no se observa como una variable abstracta y exógena, sino como algo inherentemente endógeno a la política global. Con base en ello, se puede identificar una dinámica competitiva por erigir los cimientos y el andamiaje de la estructura cibernética global, en particular, de los arreglos y configuraciones de ciberseguridad.

[27] Kenneth Boulding (1956) introdujo el concepto de imagen como objeto de referencia de estudio, por su parte, Kenneth Waltz (1959) fue quien desarrolló el concepto como un dispositivo para describir y analizar las relaciones internaciones en términos del *individuo*, el *Estado* y el *sistema internacional*.

permite realizar una serie de cuestionamientos sobre quién representa una amenaza para quién y la forma en que los significados compartidos dan forma a la interpretación de cualquier evento en particular.

2.3. Los estudios internacionales de seguridad y la ciberseguridad

La ciberseguridad está conformada por la interacción estratégica de muchos actores con características diferentes y desafía cualquier interpretación simple (Lindsay J. R., 2015a, pág. 6). Tanto la promesa como el peligro son posibilidades que derivan de una función de ubicuidad del ciberespacio. Además, la diversidad de intereses crea enredos políticos y problemas de acción colectiva. Por un lado, las empresas comerciales utilizan las redes para mejorar el comercio, ampliar la cuota de mercado y catalizar la innovación (Goldsmith & Wu, 2006). Por otro lado, las agencias de inteligencia explotan la capacidad digital para establecer mecanismos de vigilancia de amenazas nacionales y extranjeras (Inkster, 2013). A su vez, grupos militares y paramilitares buscan oportunidades para interrumpir los sistemas de mando y control del adversario mientras protegen a los suyos (Farwell & Rohozinski, 2011; Owens, Dam, & Lin, 2009). Asimismo, los grupos de la sociedad civil presionan por redes abiertas y protección de la privacidad en línea (Fu, 2017; Han, 2018; Roberts, 2018). Igualmente, los usuarios desean tener fácil acceso a noticias, entretenimiento, plataformas de comunicación y socialización digital, así como adquirir productos y servicios en línea (Singer & Friedman, 2014).

Por otro lado, aunque el Estado no está construyendo una nueva identidad en el espacio digital, diferente a su identidad tradicional, si está ampliando el rango y alcance de sus prerrogativas a través de sus narrativas y acciones que tienen efectos directos sobre los principios constitutivos del ciberespacio. No obstante, esto no se limita al abordaje de los componentes normativos, sino que revela la conformación de los intereses estatales a través de prácticas que enmarcan la ciberseguridad como una cuestión de que deber ser atendida con “extrema urgencia” o que es vital para la “supervivencia” de la sociedad moderna.

Con base en lo anterior, para apoyar y apuntalar la parsimonia explicativa del argumento teórico de este trabajo de investigación se recurre a la subdisciplina de los Estudios Internacionales de Seguridad (*International Security Studies*, ISS, por sus siglas en inglés) para explicar cómo los agentes definen el concepto de seguridad, cómo llevan a cabo la señalización de las amenazas, cómo construyen y reconstruyen éstas, y qué acciones realizan para contrarrestarlas. Con ello, el planteamiento de esta investigación busca tender un puente intra y trans-disciplinario entre el enfoque racionalista y reflexivista de Relaciones Internacionales.

2.3.1 Seguridad internacional y ciberseguridad

Respecto al debate sobre la seguridad internacional, el enfoque de estudio tendía a establecer una relación casi automática entre ésta y las capacidades militares estatales junto con la amplitud del sector de defensa (Booth, 1994, pág. 3). Es cierto que esta visión aún tiene un amplio espectro de aceptación, y hasta cierto punto validez, debido a que en muchas ocasiones las políticas estatales han favorecido notablemente la ambigüedad simbólica del concepto de seguridad, para poder justificar acciones y políticas que de otra forma tendrían que ser explicadas como instrumentos políticos de conveniencia para una gran gama de intereses que se originan en sectores limitados dentro del poder dichos estados (Wolfers, 1952) (Mesa, 2009) (Buzan B. , 1991).

En cuanto a las diversas acepciones del término, Barry Buzan (1991), Barry Buzan, Ole Waever, Jaap de Wilde (1998), Emma Rothschild (1995), Ann J. Tickner (1995) David D. Baldwin (1997) han hecho interesantes observaciones y señalamientos sobre las políticas que favorecen al mantenimiento de la ambigüedad simbólica del concepto (Wolfers, 1952). Anteriormente, el foco de atención era señalar cómo los Estados deberían usar la fuerza o la amenaza del uso de la fuerza

con la intención de alcanzar sus intereses nacionales (Baldwin, 1996) (Herz, 2013, pág. 124).[28]

No obstante, los estudios de seguridad han evolucionado desde una preocupación inicial por las consecuencias estratégicas de la rivalidad entre potencias y la capacidad destructiva de las armas nucleares, hasta su diversidad temática actual en la que se incluye la seguridad ambiental, económica, social, humana y de otro tipo participan en igual medida que la seguridad militar (Buzan & Hansen, 2009). Llama la atención que haya un vacío epistémico desde la subdisciplina de estudios de seguridad internacional sobre la variante cibernética. Ciertamente, se ha considerado que la ciberseguridad es un objeto que únicamente debe ser abordado desde una perspectiva técnica, sin embargo, en este trabajo se considera que la inclusión de esta es necesaria y pertinente

Por otra parte, desde finales de la Guerra Fría, y con mayor intensidad, con el inicio del periodo de Posguerra Fría emergió un nuevo contexto para el análisis integral de los problemas de seguridad, asimismo, el debate sobre la seguridad se ha enriquecido al incluir nuevos enfoques de estudio que permiten la observación de nuevos objetos no considerados con anterioridad. Sin embargo, para el caso de esta investigación, estos esfuerzos han enfocado limitadamente su atención sobre la revolución de la información y su impacto en la seguridad (Eriksson & Giacomello, 2006).

Los llamados tradicionalistas han abordado el desarrollo de las tecnologías de la información en relación con la mejora que representa para las capacidades militares, por ejemplo, su utilidad para la recaudación de inteligencia y el conflicto

[28] Algunos conceptos centrales desarrollados en la subdisciplina de estudios de seguridad (dilema de seguridad, balance de poder, seguridad nacional y disuasión nuclear) son cruciales para entender los debates relevantes del funcionamiento del sistema internacional (Buzan & Hansen, 2009). La primera referencia a una subdisciplina de estudios de seguridad aparece en los trabajos realizados por la RAND Corporation, establecida en 1948 en California, Estados Unidos, que congregó a especialistas civiles de diferentes áreas (Herz, 2013). Esta rama de la disciplina de las Relaciones Internacionales se ha enfocado en discutir profusamente la esencia del concepto de seguridad. Dentro de ella, se pueden encontrar claramente dos posturas divergentes, a las cuales se les ha denominado tradicionalistas y ampliacionistas (Eriksson & Giacomello, 2006). Los tradicionalistas han estado orientados a los estudios estratégicos-militares y a las prácticas de los Estados en esta arena. Por su parte, los ampliacionistas reclaman por una ampliación del concepto de seguridad que incorpore un rango nuevo de actores en sus análisis (Eriksson & Giacomello, 2006).

psicológico son consideradas capacidades materiales dentro de esta perspectiva. Incluso, se ha hablado sobre guerra electrónica (*electronic warfare*) por décadas en el contexto militar.[29] Por ello, para los tradicionalistas, las tecnologías de información son meramente un nuevo y sofisticado aditamento en el ejercicio de la defensa (Eriksson & Giacomello, 2006, pág. 228).

Por otra parte, la ampliación del concepto de *seguridad* comprende tres diferentes dinámicas teóricas: *1)* internacionalización de la seguridad, *2)* incorporación de esferas no militares de interacción al subcampo y *3)* la incorporación de nuevas fuentes de amenazas, objetos referentes y temas para el debate (Herz, 2013, pág. 126).[30] Con base en esto, la literatura es distintiva por sí misma porque toma al concepto *seguridad* como su idea clave, en lugar de hacer referencia a cuestiones de defensa o guerra, un cambio conceptual que abre el estudio a un conjunto más amplio de cuestiones políticas, incluida la importancia de la cohesión social y la relación entre las amenazas y vulnerabilidades militares y no militares (Buzan & Hansen, 2009, pág. 1).

Además, se ha insistido en la necesidad de identificar diversos niveles de seguridad (global, interestatal, grupal, individual) en aras de buscar estrategias y respuestas frente amenazas que pudieran surgir en cada uno de estos planos, de manera que se fortalezca la idea de que la *seguridad humana* debe adquirir un lugar prioritario dentro de la agenda de discusión (Mesa, 2009, pág. 10; Kaldor, 2007). Este proceso ha implicado una discusión sobre qué significa la seguridad, a quién o qué se debe estudiar y, por tanto, una nueva definición del campo en sí mismo (Booth, 1994; Rothschild, 1995).

---

[29] Por ejemplo, el Departamento de Defensa de los Estados Unidos ha cambiado el nombre de guerra de información (*electronic warfare* [EW] por sus siglas en inglés) por operaciones de información (*information operations* [IO] por sus siglas en inglés). Asimismo, la Organización del Tratado del Atlántico Norte también ha adoptado la misma definición para las (IO), las cuales son definidas como "las acciones tomadas para afectar la información del adversario y los sistemas de información mientras se defiende la información y sistemas de información propios" (Eriksson & Giacomello, 2006, pág. 237).

[30] Las cuestiones que plantean sobre una ampliación de la agenda (incluir amenazas más allá de la rúbrica estrecha de lo militar) y profundización (incluir las preocupaciones de seguridad de actores individuales y subestatales, formulada bajo la rúbrica de la “seguridad humana” (Williams, 2003).

Aunque el tema de la seguridad es muy profuso y amplio, no deja de plantear dificultades el hecho de querer presentar una síntesis en torno a la literatura existente al respecto, y que además ilustre la variación de perspectivas que se han articulado (Mesa, 2009), además de querer integrar una variable que ha sido desdeñada en el interior del campo de estudio. Si bien es cierto que, este trabajo no pretende realizar una revisión exhaustiva de ello, pues para ello, existen trabajos de gran calidad y precisión como los realizados por Barry Buzan y Lene Hansen (2009), Paul D. Williams (2008), Alan R. Collins (2007), Mary Kaldor (2007), Michael Sheehan (2005) que ofrecen recuentos históricos de la génesis, desarrollo y evolución de los estudios de seguridad, así como el tratamiento de diversas temáticas bajo este lente analítico, sí pretende mostrar los desarrollos teóricos-conceptuales más relevantes de la subdisciplina.

No obstante, este trabajo no pierde la perspectiva histórica que ha tenido el debate sobre la seguridad e intenta estructurar una visión holística de la información por medio de una revisión crítica de la bibliografía más relevante, sobre todo cimentada en la insistencia en la reinterpretación y expansión del concepto.[31] Sin embargo, la expansión del concepto de seguridad generó y todavía genera controversias. Se argumenta que tratar un nuevo grupo de temas y actores en términos de seguridad redefine la jerarquía de prioridades y distribución de recursos, de modo que se presta más atención a la cuestión apremiante, a que se escuchen más voces y a una comprensión más amplia de las conexiones entre los diferentes aspectos de la realidad (Herz, 2013, pág. 129) (Deudney & Matthews, 1999) (Huysmans, 1995) (Huysmans, 2006).

Precisamente, hay autores e instituciones que han intentado brindar una definición exacta para el concepto de seguridad (en especial en su vertiente nacional) (Buzan B. , 1991) (Wolfers, 1952) (Tuchman, 1989) (Allison & Treverton,

[31] Los objetos referentes de la seguridad (actores u objetos, más allá de lo militar). En el sector militar el objeto de referencia es la integridad territorial del Estado. Las amenazas se definen como externas a éste. En el sector político las amenazas se dan a la legitimidad de la autoridad gubernamental, amenazas internas. La seguridad *societal* en el cual la identidad de un grupo se ve amenazada por la integración económica, flujos culturales, movimientos de población (Waever, 1995).

1992). En sus argumentos aparece una extensa gama interpretativa que concibe la seguridad como: ausencia de amenazas exteriores, ausencia de conflicto militar; capacidad para la defensa del interés nacional; potenciales militares y no militares; capacidad para rechazar agresiones desde el exterior; garantía de bienestar futuro; no erosión de intereses políticos, económicos y sociales; preservación de valores; garantía de desarrollo, entre otros (Buzan B. , 1991) (Mesa, 2009, pág. 20).

Por otra parte, autores como Kenneth Booth (1994), Emma Rothschild (1995), David A. Baldwin (1997), Barry Buzan (1991) señalan que tradicionalmente los gobiernos han sido el referente principal en el discurso y la práctica de la seguridad, debido a que tienden a ser el ente más poderoso y, a que la teoría política los ha concebido también como máximos garantes de la seguridad, tanto desde el punto de vista externo como interno (Booth, 1994, pág. 5). Por ello, la *seguridad* es un concepto que ha servido como guía para el diseño de políticas destinadas a incrementar las capacidades militares del Estado, ya sea a través de la asignación de recursos a la defensa o a la formación de alianzas de carácter militar (Baldwin, 1997). Con base en lo mencionado en apartados anteriores y, en relación con la seguridad y el enfoque constructivista, será de utilidad observar el proceso de enmarcado de amenazas cibernéticas, etapa mediante la cual los agentes estatales desarrollan esquemas interpretativos específicos sobre lo que cuenta como amenaza o riesgo, cómo responder a esta y quién es el responsable para llevar a cabo dicha acción (Dunn Cavelty, 2008b, pág. 30).

Del mismo modo, Kenneth Booth (1994), recalca que teóricamente el problema del concepto de seguridad encuentra numerosas contradicciones enmarcadas en las preguntas: ¿qué es la seguridad?, ¿seguridad de quién?, ¿seguridad de qué objeto? ¿para quién?, ¿del Estado?, ¿del gobierno?, ¿de una clase?, ¿de una nación?, ¿cuáles son las amenazas?, ¿ en qué dimensión se encuentra la seguridad, regional o global?[32] Con base en estas ideas, es posible

[32] Autores como Richard Ullman (1983), David Baldwin (1997), Charles Schultze (1973), Michael Williams (1997) y Raimo Väyrynen (1995) han reflexionado sobre estas dificultades de definición conceptual, de ambigüedades terminológicas, de manejo parcializado de la seguridad, así como de las incongruencias que emanan de la labor de análisis y de las realidades que son objeto de estudio (Mesa, 2009, págs. 30-31).

conocer la forma en que se encuadra un problema, quién es responsable y las potenciales soluciones transmitidas por imágenes, estereotipos, mensajes y metáforas (Ryan, 1991, pág. 59). En efecto, la alta relevancia del enmarcado como patrón social es el resultado de los marcos que definen el significado y determinan las acciones de los agentes (Dunn Cavelty, 2008b, pág. 30).

De esta forma, la teoría de la securitización está enlazada directamente con explicaciones sobre el papel de la argumentación, la acción y la ética de la teoría constructivista de Relaciones Internacionales (Risse, 2000). Asimismo, la acción retórica se da cuando los actores no están dispuesto a cambiar sus propias creencias o dejarse convencer por el mejor argumento en torno a un tema, pero sí intentan cambiar la visión del mundo, las creencias normativas y las preferencias de sus contrapartes (Risse, 2000, pág. 277). A su vez, la principal forma de la acción comunicativa en las prácticas de seguridad crecientemente se incrusta dentro de imágenes o referentes visuales. De esta manera, los procesos de securitización se vuelven dinámicos en sus formas institucionales, aunque, no pueden ser únicamente evaluadas a través de los actos discursivos y las representaciones simbólicas (Williams M. C., 2003). Por ello, se debe desarrollar un amplio entendimiento de los medios, estructuras e instituciones de la conformación de la comunicación política contemporánea para abordar adecuadamente las explicaciones empíricas y éticas de las prácticas de ciberseguridad (Williams M. C., 2003) (Risse, 2000) (Hansen, 2000).

En el caso de enmarcado de amenazas cibernéticas, el proceso de categorizar algo como una amenaza particular tiene consecuencias prácticas cuando los actores clave comienzan a ver el mundo según estas categorías (Dunn Cavelty, 2008b, pág. 30). Asimismo, las creencias y los recursos influyen directamente en el proceso de estructuración del riesgo[33]. Además, cabe resaltar que tanto las prácticas sociales como los recursos materiales se subordinan a los entendimientos intersubjetivos. Lo cual lleva a deducir que las percepciones de

[33] Una creencia es una idea o imagen mental de cómo está estructurado el mundo, cómo funciona y cómo debería funcionar. Las creencias son un recurso cultural para enmarcar, y los marcos de creencias construidos alrededor de la amaneza se originan en los sistemas de creencias de los actores (Dunn Cavelty, 2008b, pág. 31)

amenaza hacia la seguridad estarán condicionadas por los entendimientos intersubjetivos. Por lo tanto, la formación de marcos interpretativos en relación con la amenaza está influenciado por las instituciones y por el contexto más amplio en el que se produce el marco de éstas (Dunn Cavelty, 2008b, pág. 36). Por eso, actores específicos o agrupaciones de actores desarrollan un marco específico sobre la amenaza y, a su vez, este marco puede deducirse de sus declaraciones y puede identificarse a partir de documentos oficiales, fundamentales para establecer la agenda de toma de decisiones (Dunn Cavelty, 2008b, pág. 37).

2.4 Propuestas sobre la ampliación del concepto de seguridad y su impacto sobre la discusión de la ciberseguridad

Por otra parte, dentro de los esfuerzos que se inclinan a favor de una reforma radical de los estudios de seguridad internacional, se identifica a quienes exhortan a una ampliación del foco de atención, donde se inserten temas económicos, de derechos humanos, ambientales, crimen internacional e injusticia social, e incluso cibernéticos (Mesa, 2009, págs. 30-31) (Lindsay J. R., 2015a) (Kello, 2013). En ese tenor, Barry Buzan, en su obra seminal, *People, States, and Fear* (publicada por primera vez en 1983) consideraba que el concepto de seguridad es, en sí mismo, más versátil, penetrante y útil que los conceptos de paz y poder en el estudio de relaciones internacionales, y reconoce que la tarea fundamental radica en habilitar dicho concepto a través de su desarrollo y análisis (Buzan B. , 1991, pág. 15).

Debido a su origen histórico y teórico, los estudios de seguridad se enfocaron inicialmente en cómo garantizar la seguridad del Estado contra amenazas internas y externas y en cómo el uso de la fuerza puede servir para esos fines (Herz, 2013, pág. 123). Una causa de la estrechez en la definición conceptual de seguridad se debe a la hegemonía intelectual ejercida por el realismo de las Relaciones Internacionales, donde “la seguridad era virtualmente un sinónimo de defensa” (Booth, 1994, pág. 3). Con base en ello, el realismo ha caracterizado a la seguridad a partir de tres elementos: *1)* un énfasis en las amenazas militares y la necesidad de responder a través de la fuerza a éstas; *2)* una orientación a mantener el *statu quo*; y *3)* un enfoque centrado exclusivamente en los Estados (Booth, 1994).

No obstante, una de las propuestas de reevaluación sobre los estudios de seguridad que probablemente ha tenido más impacto en la Posguerra Fría proviene de la Escuela de Copenhague, representada por Barry Buzan, Ole Waever, Jaap de Wilde, Lene Hansen entre otros (Mesa, 2009). Su proposición de una redefinición ha implicado, por un lado, una *epistemología objetiva* cuando los estudios subrayan algo que sucede fuera del sujeto, como por ejemplo las nuevas formas de interacción; y por el otro, una *epistemología subjetiva* cuando los estudios recalcan cómo diferentes discursos, actores y prácticas redefinen lo que es la seguridad (Herz, 2013, pág. 127).

Sobre la base de esas ideas, Ole Waever (1995) es uno de los primeros en rechazar la preponderancia del Estado como objeto referente en temáticas de seguridad, y ha conferido importancia a otros objetos y dimensiones como sociedad, medio ambiente, género e identidad como asuntos referentes de seguridad. Para Ole Waever, la seguridad no es un concepto con significado invariable, ni una condición social determinada; opina que un elemento esencial para entender las relaciones y las políticas de seguridad radica en el proceso mediante el cual determinados asuntos son "securitizados" (*securitized*) (Mesa, 2009, pág. 31; Waever, 1995). Según la Escuela de Seguridad de Copenhague, los asuntos públicos se convierten en un problema de seguridad no necesariamente porque existe una amenaza existencial real, sino porque el problema se presenta y establece con éxito por agentes clave como una amenaza (Buzan, Waever, & de Wilde, 1998).

En torno a ello, en 1995, Ole Waever acuñó el término securitización (*securitization*) como una reacción a los estudios tradicionales sobre seguridad, a las teorías realistas y neorrealistas de la disciplina de las Relaciones Internacionales, que restringían el concepto de 'amenazas' solamente a peligros de tipo de militar, generalmente entre Estados (Treviño, 2016)[34]. En relación con esta aproximación teórica, el estudio de la securitización apunta a obtener una

[34] La noción de securitización se basa en la *teoría del acto discursivo* desarrollada por (Austin, 1962) y (Searle, 1969).

comprensión de quién securitiza (el actor) sobre quién (el sujeto de amenaza), para quién o qué (el objeto referente), por qué (las intenciones y propósitos), con qué resultados, y bajo qué condiciones (la estructura) (Dunn Cavelty, 2008b, pág. 25).

Por ello, en este trabajo se sostiene que no existe la necesidad de teorizar la ciberseguridad como un sector distinto a lo militar, lo político, lo económico, lo cultural, religioso o social (Hansen & Nissenbaum, 2009, pág. 1156),[35] sino como un concepto que abarca estas dimensiones en distintos niveles. Si bien es cierto que, el enfoque de securitización tiene un conjunto de deficiencias, esta explora como ciertos temas pasan de ser "ordinarios" a ser asuntos de seguridad, lo cual exige una mayor atención pública y la legitimización de políticas públicas urgentes (Buzan B. , 1991) (Buzan, Waever, & de Wilde, 1998) (Waever, 1995). En efecto, es un proceso por el cual del cual ciertos actores presentan ante una audiencia ciertos fenómenos sociales bajo el rubro de seguridad, y de la existencia de *supuestas amenazas* (militares o no militares) como un pretexto para desplegar ciertas *medidas emergencia* (Buzan, Waever, & de Wilde, 1998, pág. 24). Este asunto tiene consecuencias concretas como pueden ser: un incremento en el número de elementos encargados de aplicar dichas pautas, un mayor número de recursos y más armamento para mantener la seguridad (Buzan, Waever, & de Wilde, 1998, pág. 23).[36]

Cabe resaltar que, las acciones de securitización únicamente tienen éxito si una audiencia "acepta" el argumento de seguridad y la necesidad de implentar medidas urgentes (Buzan, Waever, & de Wilde, 1998, pág. 25) (Dunn Cavelty, 2008b, pág. 26). Sin embargo, sigue siendo poco claro qué audiencia tiene que

[35] El ciberespacio está en constante evolución. La combinación híbrida entre tecnología y las personas que la usan está siempre cambiando, alterando inexorablemente todo, desde el tamaño y la escala hasta las reglas técnicas y políticas que buscan guiarlo (Singer & Friedman, 2014, pág. 14). Las características esenciales siguen siendo las mismas, pero la topografía está en constante cambio (Singer & Friedman, 2014, pág. 14).

[36] Un ejemplo de esto, es como se presenta la conformación del ciberespacio, y la estructuración de las expectativas sociales sobre el mismo. Por ejemplo, algunos autores mencionan que la expansión del ciberespacio es tal que llega a incluir "sectores vitales para la ejecución de nuestra civilización moderna" también llamados "infraestructura crítica". Estos son los sectores subyacentes que manejan, controlan y ejecutan los procesos de la agricultura y la distribución de alimentos, financieros, de salud, transporte y manejo de agua (Singer & Friedman, 2014, pág. 15).

aceptar qué argumento, en qué medida y durante cuánto tiempo (Dunn Cavelty, 2008b, pág. 26). Por tanto, las medidas excepcionales son altamente contextuales y subjetivas (Dunn Cavelty, 2008b, pág. 26). No obstante, este esfuerzo teórico (Escuela de Copenhague) es partidario de la inclusión de la construcción de amenazas, de la multidimensionalidad de la seguridad y de la comprensión de este concepto como un elemento objetivo y subjetivo al mismo tiempo.

Por ejemplo, alguno de sus postulantes menciona que una forma de evitar este problema empírico es ignorar la designación de etiquetas como 'normal' y 'extraordinaria' y, en cambio, centrarse en la estructura retórica de las declaraciones y sobre las medidas que pretenden aplicarse (Waever, 1995). En otras palabras, el proceso de securitización no puede reducirse a una simple retórica, sino que implica la evaluación o el rastreo de una amplia movilización de recursos para apoyar el discurso, la ejecución de nuevas prácticas o la creación de instituciones para hacer frente al peligro casi ubicuo que constituyen las nuevas amenazas (Bigo, 1994) (Huysmans, 1998)

Además, la incorporación de la subjetividad al debate permite formular preguntas sobre el significado de la seguridad e indagar en los cambios históricos del concepto y la sociología de la construcción de las amenazas. La idea del peligro como condición objetiva, vista como realidad independiente, es cuestionada, ¿cómo se interpreta y se articula el peligro?, ¿quién lo hace?, ¿con qué consecuencias? (Herz, 2013, pág. 129). Con base en esto, la Escuela de Copenhague entiende la seguridad como una modalidad discursiva compuesta de una estructura retórica particular que a su vez produce efectos políticos particulares, lo que la hace valiosa para el estudio de la formación y evolución del discurso de la ciberseguridad (Hansen & Nissenbaum, 2009). Como un acto discursivo se encuentra localizado en el terreno de la argumentación política y la legitimación discursiva, y por ello las prácticas de seguridad son susceptibles de la crítica y de la transformación (Williams M. C., 2003).

Asimismo, se enfoca principalmente en la acción de aquellos actores que están dotados tanto del 'capital simbólico' como de la capacidad de interconectar discursos heterogéneos al establecer la condición de ciertos objetos como

amenazas (Dunn Cavelty, 2008b, pág. 27). De esta manera, ciertas voces están inherentemente dotadas y con más peso que otras debido a su disposición en puestos de autoridad (Dunn Cavelty, 2008b, pág. 27). Con base en esto, la seguridad es un acto discursivo que *securitiza*, esto significa que constituye uno o más objetos referentes, históricamente la nación o el Estado, como componentes amenazados físicamente o ideacionalmente, y por consiguiente se requiere de una protección urgente de éstos (Hansen & Nissenbaum, 2009, pág. 1156). El mecanismo teórico que hace posible la identificación de la seguridad con la lógica de la amenaza existencial y la extrema necesidad es la condición de intensidad: ¿quién decide la calidad de la amenaza?, ¿qué tanto riesgo representa? ¿qué acciones se deben hacer para eliminarla? (Williams M. C., 2003).

Por tanto, la securitización se observa más como un proceso objetivo y una posibilidad social intrínseca de la vida política: una realidad existente y una posibilidad continua (Hansen & Nissenbaum, 2009). El acto discursivo de la securitización no se reduce estrictamente a actos verbales o retóricas lingüísticas es un acto representativo más amplio el cual recurre a una variedad de recursos contextuales, institucionales y simbólicos para su efectividad (Mattelart, 2007) (Williams M. C., 2003). Junto con ello, la acción comunicativa involucra un proceso de argumentación, provisión de razonamientos, presentación de evidencia y el compromiso de convencer a otros sobre la validez de un posicionamiento (Risse, 2000).

Como actos discursivos, las “securitizaciones” están obligadas en principio a entrar en la arena de la legitimación discursiva (Williams M. C., 2003) (Risse, 2000) (Buzan, Waever, & de Wilde, 1998) (Waever, 1995). Simultáneamente, la teoría de los actos discursivos implica la posibilidad del argumento, del diálogo y de este modo tiende a potencializar la transformación de las percepciones de seguridad dentro de las sociedades. Por lo tanto, el éxito de la securitización no es decidido por el actor que ‘securitiza’ un objeto sino por la aceptación de la audiencia (Hansen, 2000).

De esta manera, las condiciones de la producción y recepción de los actos comunicativos estarán influidas fundamentalmente por el medio a través del cual

son transmitidos. En otras palabras, los diferentes medios no son neutrales en su impacto comunicativo (Deibert R. J., 1997) (McLuhan, 1964). Una vez que el tema en cuestión llega a ser visto como un *peligro* por el público, estos mismos actores pueden entonces diseñar y disponer justificadamente de acciones, leyes, reglas, instituciones, presupuestos y mecanismos de emergencia para acabar, evitar, detener, contener o controlar dicho peligro, incluso si estas disposiciones violan la ley, las normas internacionales, los derechos humanos o si van en contra del sentido común (Treviño, 2016, págs. 260-261).

Es por ello que, el cómo la forma en la cual las representaciones visuales son representadas, cómo las imágenes son capaces de contribuir a los procesos de securitización o desecuritización y cómo están ligados a componentes discursivos convencionales, recursos materiales e institucionales que los actores pueden desplegar, son cruciales y fundamentales para entender las prácticas estatales en el espacio digital. De esta manera, será importante corroborar qué efectos tiene la ciberseguridad sobre la reestructuración de las actividades estatales dentro del ciberespacio, que transitaron del desentendimiento a una participación intensa, que se refleja a través del proceso de securitización, cuestión que será abordada en el siguiente capítulo de este trabajo de investigación.

Capítulo 3. Gobernanza global en materia de ciberseguridad

Introducción

Una característica común de la mayoría de la literatura especializada sobre la sociedad de la información es la creencia particular de que, en esta etapa histórica, ésta adquiere un papel primordial como recurso de poder (Dunn Cavelty, 2007, pág. 19). El predominio aparente y la prevalencia de la información en muchos aspectos de la vida moderna ha hecho incluso que se denomine a esta fase histórica precisamente como "la era de la información". Durante la historia de la humanidad han existido diversas revoluciones en las tecnologías de la comunicación que han provocado una transformación en el orden establecido y han conducido a la formación de una dinámica social novedosa (Deibert R. J., 1997). Estas modificaciones han sido recibidas en su momento de dos maneras, como una celebración o como un rechazo, dependiendo de la afectación que éstas han tenido sobre diversos grupos sociales (Dunn Cavelty, 2008b).

El tema clave, por lo tanto, es identificar las características y las cualidades especiales de la transformación actual, especialmente el impacto que tienen sobre el entorno de seguridad internacional. Para este apartado de la investigación, se pretende analizar el papel de la *ciberseguridad* sobre la forma de participación de los Estados en el espacio digital y sus implicaciones sobre la configuración de normas en el ciberespacio. Primero, se presentan algunas delimitaciones conceptuales de la ciberseguridad, que permiten saber qué se está gestionado y de qué manera. En segundo lugar, se describe la evolución del sistema de gobernanza del ciberespacio,[37] lo que permite responder sobre cuándo y cómo los gobiernos juegan un papel en la edificación de la arquitectura del ciberespacio a nivel global. De allí se exponen los esquemas de ciberseguridad, el tipo de reglas, normas y principios que los Estados buscan establecer en la agenda internacional del

[3737] Para este trabajo, se entiende a la gobernanza global como la dinámica entre actores estatales y no estatales que buscan identificar, entender y abordar temáticas globales transversales y problemáticas en un proceso continuo que busca encontrar posicionamientos comunes para intereses divergentes (Karns, Mingst, & Stiles, 2015, pág. 2)

fenómeno, y cómo interactúan con agentes no estatales y sobre las divergencias de percepciones entre estos dentro de la comunidad estatal.

3.1 Significados y aproximaciones conceptuales de la ciberseguridad

Como han subrayado algunos teóricos, las dificultades para estudiar la era de la información y, en particular, sus implicaciones para las relaciones internacionales y la seguridad son considerables, entre otras cosas “porque el trabajo previo sobre el tema es relativamente escaso, desorganizado y difícilmente abordado por la teoría de Relaciones Internacionales” (Dunn Cavelty, 2007, pág. 20); cuestión que ha sido abordada de manera más explícita en los capítulos anteriores.

Por un lado, la llamada “revolución de la información” está estrechamente relacionada con el desarrollo tecnológico relativamente reciente en el procesamiento de la información y las tecnologías de comunicación y, por otro lado, con la rápida dispersión global de estas tecnologías, sobre todo con el ascenso de "Internet", una red de comunicación descentralizada de redes de computadoras (Dunn Cavelty & Brunner, 2007, pág. 2). A su vez, es difícil asegurar cuándo apareció por primera vez la expresión “sociedad de la información”.

A principios de la década de 1990, algunos periodistas y comentaristas comenzaron a hablar y escribir sobre “autopistas de la información” (*information highway*), especialmente cuando la administración del ex presidente William Clinton popularizó el término (Eriksson & Giacomello, 2006, pág. 223). En el campo académico, el sociólogo Manuel Castells ha sido uno de los más influyentes sugerentes de la era digital. Desde finales de la década de 1980 enfatizó que la información se había convertido en el mayor recurso de productividad en la nueva “economía del conocimiento” (Castells, 1989) (Eriksson & Giacomello, 2006, pág. 223). Incluso ha dedicado una extensa trilogía para explicar el nacimiento de la “sociedad global en red”, señalando la pérdida de soberanía de los Estados y el surgimiento de dinámicas centradas en actores no estatales (Castells, 1996) (Castells, 1997) (Castells, 1998).

Además, otra de las dificultades para el análisis es la imprecisión conceptual existente, lo que ha impedido la proliferación de estudios sistemáticos y teóricamente significativos. Aunque este trabajo pretender llenar una parte este vacío epistémico, se reconoce que tampoco se está brindando una teoría acabada sobre la ciberseguridad a escala global y que aún quedan elementos teóricos conceptuales por depurar, pero que este puede servir como un punto de arranqe para la profundización de investigaciones sobre el tema.

De esta manera, conforme con algunos especialistas, existen tres elementos semánticos fundamentales que se interrelacionan con la temática tecnológica: "información", "digital" y el prefijo "ciber" (Dunn Cavelty, 2007, pág. 20). En muchas ocasiones, el nuevo vocabulario se crea simplemente colocando el prefijo 'ciber' ante conceptos familiares (ciber-seguridad, ciber-amenaza, ciber-ataque, ciber-conflicto, ciber-guerra, ciber-terrorismo, ciber-contraterrorismo, ciber-crimen, ciber-acoso, entre otros). En otros casos, se agrega el concepto digital o información después de una idea conocida como, por ejemplo: gobierno digital, comercio digital, economía digital, sociedad digital, identidad digital. Por su parte, para el otro vocablo, se han creado conceptos como info-esfera, infotopia, info-conflictos, info-cooperación, des-información, sociedad de información (Krishna-Hensel, 2007). Como resultado, estas expresiones comienzan a ser comunes en discursos políticos, medios de comunicación, revistas académicas e incluso en conversaciones cotidianas (Dunn Cavelty, 2007), pero, ¿cuál es la importancia de diseccionar estas concepciones?

En efecto, como bien lo subraya la experta Myriam Dunn Cavelty de la Universidad ETH Zurich, el uso cotidiano de estos términos y la imprecisión han conducido a un proceso de ambigüedad que puede significar "todo y nada" (Dunn Cavelty, 2008b, pág. 14). Sin embargo, la importancia de la información no es una característica única de nuestro tiempo, sino que siempre ha sido vital para la humanidad y sus interacciones (Dunn Cavelty, 2008b, pág. 12). Además, a lo largo de la historia, los avances en los campos científico-técnicos han desempeñado repetidamente un papel importante en el cambio de los asuntos humanos, los cuales han dado forma significativa a la historia y las instituciones sociales (Papp, Alberts,

& Tuyahov, 1997; Borgmann, 1999; Deibert R. J., 1997; Waldrop, 1998; Hobart & Schiffman, 2000; Freeman & Louca, 2002). Sin embargo, como se ha subrayado anteriormente, el rango y amplitud de estas concepciones crea confusión sobre la naturaleza de sus implicaciones y, a su vez, complica el análisis teórico-conceptual, puesto que abarca una gran cantidad de entornos taxonómicos.

Con respecto a lo anterior, el siguiente apartado tiene como objetivo esclarecer algunos conceptos y desarrollos tecnológicos para ilustrar cómo el Estado se involucra en la dinámica de la política internacional cibernética. Además, este tiene como propósito servir de puente entre la delimitación de la problemática, el planteamiento teórico y las evidencias que ayudan a comprobar la hipótesis central del trabajo de la investigación presentadas en los siguientes dos capítulos. Asimismo, pretende dar luz específica sobre el accionar que han tenido los actores estatales (sin excluir a los actores no estatales) en el área de ciberseguridad internacional.

3.1.1 Ciberseguridad: revisión conceptual

En términos generales, la ciberseguridad se ha convertido en una palabra genérica, o en un concepto paraguas (*umbrella concept*) que abarca una amplitud de cuestiones, que, si bien se interrelacionan, en ocasiones, se utiliza de manera copiosa para describir una gran amplitud de cuestiones. Justamente, el término comprende una vasta cantidad de problemas, demasiado amplios como para encajar adecuadamente en una sola palabra.

Primeramente, la idea de ciberseguridad fue utilizada por primera vez por aquellos científicos computacionales a principios de la década de 1990, para enfatizar una serie de inseguridades relacionadas con las computadoras que trabajaban de forma reticular (Hansen & Nissenbaum, 2009, pág. 1155). Uno de los primeros usos del término apareció en el informe del año 1991 de la Junta de Informática y Telecomunicaciones de los Estados Unidos de América, que se titulaba *Computers at Risk: Safe Computing in the Information Age*, el cual definía la ciberseguridad como “la protección contra la divulgación de información no

deseada, la modificación o destrucción de datos en un sistema y también lo relativo a la protección de los mismos sistemas" (Hansen & Nissenbaum, 2009, pág. 1160).

Además, el uso del término *ciberseguridad* se aplica desde la amenaza de computadoras infectadas con *malware* organizadas en *botnets*, controlados a distancia que pueden usarse para enviar *spam* o para ejecutar ataques DDoS[38] (Mueller M. L., 2010, pág. 159). También, el concepto cubre tanto la intrusión no autorizada en redes privadas por parte de personas externas como los esfuerzos de las organizaciones para evitar que los usuarios no deseados roben datos, identidades y activos financieros (Mueller M. L., 2010, pág. 159). Igualmente, se refiere a errores en sistemas operativos y protocolos de computadoras, teléfonos móviles y otros dispositivos que produzcan oportunidades para la explotación por parte de programadores inteligentes. (Mueller M. L., 2010, págs. 159-160) E incluso, se usa comúnmente en relación con los derechos de privacidad y la protección de datos. Todos estos fenómenos han caído bajo el paraguas del discurso de seguridad en Internet (*ciberseguridad*) (Mueller M. L., 2010, pág. 160). Como muestra de lo anterior, en la tabla 3.1 se ejemplifican algunas de las herramientas cibernéticas maliciosas más utilizadas para aprovechar alguna vulnerabilidad de los mecanismos de ciberseguridad.

Tabla 3.1 Definición de herramientas cibernéticas maliciosas

Herramientas Cibernéticas	**Definición**
Botnet	Una red de dispositivos utilizados por *hackers* para ataques masivos coordinados sobre sistemas informáticos. El uso de una red de *bots* para enviar solicitudes masivas y simultáneas a los servidores evita el uso legítimo de los servidores y produce un ataque de denegación de servicio.

[38] Un ataque distribuido de denegación de servicio, (*distributed denial of service*, DDoS) tiene como objetivo inhabilitar una red, un servidor o infraestructura a través de la saturación o agotamiento de los recursos de un sistema para dificultar su capacidad de respuesta, generando así inaccesibilidad y no disponibilidad del servicio para los usuarios legítimos (Singer & Friedman, 2014, pág. 295)

DDoS	Tiene como objetivo inhabilitar una red, un servidor o infraestructura a través de la saturación o agotamiento de los recursos de un sistema para dificultar su capacidad de respuesta, generando así inaccesibilidad y no disponibilidad del servicio para los usuarios legítimos
Bomba Lógica (*Logic Bomb*)	Son programas camuflados segmentados que destruyen datos cuando se cumplen ciertas condiciones.
Troyano (*Trojan horse*)	Es un código que se ejecuta bajo la apariencia de un programa útil pero que realiza actos maliciosos como la destrucción de archivos, la transmisión de datos privados y la apertura de una puerta trasera (*back door*) para permitir el control de un dispositivo por parte de terceros.
Virus	Código malicioso que puede auto-replicarse y causar daños al sistema que infecta. El código puede eliminar información, infectar programas, cambiar la estructura para ejecutar programas no deseados e infectar la parte vital del sistema operativo que une cómo se almacenan los archivos.
Gusano (*worm*)	Similar a un virus, se distingue por su capacidad para auto-replicarse sin infectar otros archivos para reproducirse.
Zombie	Un dispositivo que ha sido comprometido de forma encubierta y controlada por una tercera parte.

Malware	Es una abreviatura de *software* malicioso cuyo objetivo es infiltrarse y después dañar u obtener información de un sistema informático sin el consentimiento del propietario.
Ransomware	Es un tipo de *malware* que impide o restringe el acceso de los usuarios a su sistema, ya sea bloqueando la pantalla o los archivos a menos que se pague un rescate.
Spyware	Es un *software* cuyo objetivo es monitorear las acciones de un usuario de computadora (por ejemplo, sitios web visitados) e informar estas acciones a un tercero, sin el consentimiento informado del propietario o usuario legítimo
Phishing	Con esta técnica, se intenta conseguir datos confidenciales, como por ejemplo números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un sitio web y en los que se engaña al usuario para que se exponga a una intrusión.

Fuente: (Reveron, 2012, pág. 8), (Riquelme & Martinez, 2018)

Ciertamente Internet se está utilizando en formas creativas e inesperadas para propagar actividades de participación social, política y económica, tanto legales como ilegales, progresivas, subversivas, benéficas y perjudiciales, por ende, cualquier respuesta para regular o controlar esas actividades impacta sobre los principios que subyacen a la cuestión cibernética (Krishna-Hensel, 2007, pág. xi). Como recalcan algunos especialistas, una gran cantidad de investigación sobre internet se enfoca en el contenido y uso de éste. Dicho enfoque aborda, principalmente, la experiencia centrada en el usuario (*user-centric experience*), en las interacciones de contenido y cómo estas interacciones afectan el discurso político, los patrones comerciales y de consumo, así como las interacciones sociales (DeNardis, 2014, pág. 20).

Por un lado, temas relacionados con el contenido incluyen las implicaciones económicas y políticas generadas por los usuarios, cuestiones de periodismo

ciudadano, nuevos modelos producción de conocimiento en red, las implicaciones políticas de la esfera pública digital y las normativas sobre usos en internet (DeNardis, 2014, pág. 20; Benkler, 2006; Karpf, 2012; Kreiss, 2012). Por otro lado, otros temas relacionados con el contenido incluyen la política de representación visual en línea o los efectos de los mundos virtuales y los efectos de los juegos en línea sobre el comportamiento y la sociabilidad (DeNardis, 2014, pág. 20). Asimismo, algunos estudios de Internet se centran en cómo los actores políticos tradicionales o los ciudadanos utilizan Internet (DeNardis, 2014, pág. 20; Perloff, 2014; Sunstein, 2017).

Conjuntamente, otros estudios abordan los asuntos sociales como la igualdad digital, la interacción entre comunidades sociales digitales, la formación de la identidad y variadas formas de interconectiviad humana (Perry & Roda, 2017; Shirky, 2011; Pariser, 2011) (Singer & Brooking, 2018) (Pariser, 2011) Asimismo, algunos análisis examinan las implicaciones de los nuevos mecanismos de negocio de las industrias de la información (Schneier B. , 2015) (Vaidhyanathan, 2011) (Vaidhyanathan, 2018). En general, estos trabajos abordan la producción de conocimiento o los efectos políticos, económicos y sociales del contenido en línea, en lugar del control de las tecnologías sobre las que fluye este contenido, sin embargo, están fuera del ámbito específico de la gobernanza de Internet, que es la cuestión a la que se aboca esta investigación (DeNardis, 2014, pág. 20).

Con base en lo anterior, algunos autores consideran que “la ciberseguridad es un bien público global porque permite el acceso a comunicaciones confiables para todos los usuarios” (Rovner & Moore, 2017, pág. 184; McPherson & Zimmerman, 2010; Mulligan & Schneider, 2011). Por ejemplo, la consideración hecha por los analistas Joshua Rovner y Tayler Moore (2017, pág. 188) es que “la ciberseguridad beneficia a todos los usuarios cuando pueden comunicarse de manera segura en línea, pues previene el fraude y el abuso, y a su vez, permite el comercio y las finanzas internacionales y, además, proporciona una cantidad asombrosa de información a un costo muy bajo”.

Sin embargo, la ciberseguridad tiene una contraparte, es decir, “las mismas protecciones que permiten a las personas comunicarse de manera segura también

permiten actividades dañinas para la sociedad" (Rovner & Moore, 2017, pág. 184). En otras palabras, las herramientas de seguridad de la información que coadyuvan a autentificar a los usuarios y a proteger la integridad del contenido, mantener el anonimato en línea, también sirven para el desarrollo de operaciones cibernéticas ofensivas tales como denegación de servicio, virus, gusanos y otros problemas que se muestran en la tabla 3.1.

De ahí que si esta sociedad multi-conectada depende en gran medida de los nuevos enlaces de comunicación que convergen con un desarrollo tecnológico exponencial y, que a su vez contribuyen a que los mensajes tengan mayor alcance, que afecta en gran medida la totalidad de las actividades de la agencia humana, se convierte en un imperativo analizar y observar la relación entre el cambio tecnológico y la política global, poniendo énfasis en la viabilidad y seguridad, así como en la competencia técnico-científica de las principales entidades estatales. Es por ello que, la ciberseguridad a menudo se asocia con esfuerzos para reafirmar la jerarquía y el control conducidos por varios actores, tanto estatales como no estatales (Mueller M. L., 2010, pág. 159). De ahí que, desmenuzar el papel que las analogías, metáforas y escenarios que reivindican ciberataques con efectos similares a ataques militares de gran calado, desastres naturales y al desarrollo de armas nucleares se convierta en un elemento a considerar, cuestiones que han sido comunes en el debate sobre la ciberseguridad como se mencionaba en el capítulo anterior.

Si bien es cierto que, la política cibernética internacional está evolucionando, "su complejidad, dinamismo, escala y alcance son cada vez más diversos en sus modos y manifestaciones" (Choucri, 2012, pág. 125). Asimismo, tal como apuntan algunos académicos, "la complejidad y el cambio no son cuestiones novedosas y únicas para la sociedad humana, no obstante, los desarrollos en la esfera técnica parecerían superar constantemente la capacidad de adaptación de los individuos y de los sistemas sociales a medida que la velocidad de la innovación tecnológica se acelera, lo cual, hace más difícil pronosticar o anticipar el rango de efectos que tendrán estas innovaciones" (Dunn Cavelty, 2008b, pág. 13).

En efecto, los actores son diversos, con diferentes grados de poder y capacidades tanto técnicas como de gestión, con diferentes niveles de desarrollo de infraestructura que permiten el acceso cibernético (Choucri, 2012, pág. 133), sin embargo, para algunos analistas, el Estado continúa siendo el jugador principal en el terreno de la seguridad y mantiene su papel como el máximo proveedor de ésta, incluso en el ciberespacio (Fountain, 2001) (Kramer, Starr, Wentz, & (eds.), 2009). De forma más reciente, algunos especialistas enfatizan que "los jugadores más notables en el ciberespacio, en términos de capacidad, organización, alcance e infraestructura siguen siendo los Estados" (Valeriano & Maness, Cyber war versus cyber realities: cyber conflict in the international system, 2015). E incluso, esta perspectiva recalca que "los Estados-nación de todo el mundo están reafirmando visiblemente su control sobre el ciberespacio y el flujo de datos e información en busca de poder, riqueza e influencia" (Segal A. , 2016, pág. 1).

Por otra parte, la intervención estatal en el ciberespacio ha generado preocupaciones, primordialmente, sobre los efectos que puede tener sobre el libre intercambio de ideas, a medida que estos lo utilizan para su propios propósitos, e incluso, para algunos expertos "esto podría erosionar la universalidad de los nombres de dominio, complicar la seguridad global de los datos y la administración de la infraestructura de Internet, lo que puede transformar Internet de una infraestructura universal, a una que varía de un país a otro" (DeNardis, 2014, pág. 4). Es por ello que, en el próximo apartado se explica cómo participan los agentes estatales en la configuración y ordenación del esqueleto que conforma el ciberespacio.

3.2 Gobernanza del ciberespacio: espacios en disputa

Para algunos académicos y funcionarios gubernamentales, "las acciones cibernéticas son emblemáticas de un nuevo estilo de competencia en un mundo donde el poder se desconcentra" (Flournoy & Sulmeyer, 2018, pág. 41). Para otros, los diferendos sobre la gobernanza de Internet representan los nuevos espacios de competencia en el siglo XXI, en aspectos relacionados con el control, regulación y

estructuración del desarrollo tecnológico, que tienen efectos profundos sobre el poder político y económico a nivel global (DeNardis, 2014, pág. 1).

Asimismo, desde que Internet creció de una pequeña red entre centros de investigación y universidades hasta convertirse en el pilar fundamental de la sociedad contemporánea, cuestionamientos, interrogantes y controversias sobre quién y cómo se deben gestionar los destinos y la interoperabilidad de la red mundial se han hecho más evidentes (Singer & Friedman, 2014, pág. 26). No obstante, el complejo andamiaje institucional y técnico de la gobernanza del ciberespacio sigue siendo sumamente invisible para la gran mayoría usuarios, a diferencia del uso de las aplicaciones y el contenido que son permitidos por esta estructura (DeNardis, 2014; Klimburg, 2017).

De esta manera, uno de los componentes más importantes, dentro un mundo digital de recursos aparentemente interminables, son las cuestiones tradicionales de gobernanza en el ciberespacio, tales como la representación, el poder y la legitimidad (Singer & Friedman, 2014, pág. 26). Como lo mencionan algunos analistas, "las tensiones políticas y culturales en las decisiones de diseño de internet se producen porque éstas dan forma a estructuras sociales y económicas que van desde las libertades civiles individuales hasta la política de innovación global" (DeNardis, 2014, pág. 7). No obstante, antes de profundizar sobre la estructuración de la gobernanza del ciberespacio, es necesario tratar de puntualizar brevemente que se entiende por el concepto de gobernanza.

En primer lugar, la acuñación del término *gobernanza* se remonta a la formulación original de James Rosenau y Ernst Czempiel (1992) de "gobernanza sin gobierno". Para estos autores, el concepto refiere a un sinfín de formas de autoridad y de procesos formales e informales que pueden ejercer la *gobernanza*, "es decir, configurar, y en distintos grados, conducir algunos aspectos de la vida global sin que necesariamente guarden relación alguna con el gobierno formal" (Weiss & Wilkilson, 2014, pág. 29). Para los especialistas Thomas G. Weiss y Rorden Wikilson (2014, pág. 30) "el propósito fundamental de la investigación en torno a la gobernanza global reside justamente en descifrar tanto la suma total como los elementos que la integran, así como las contradicciones y fuerzas

compensatorias que ahí coexisten". Es necesario entender que, para que tenga sentido, la gobernanza no puede reducirse a describir únicamente un momento histórico determinado, sino que "debe aspirar a representar un conjunto legítimo de preguntas sobre cómo está gobernado, ordenado y organizado el mundo en cada periodo histórico" (Weiss & Wilkilson, 2014, pág. 30).

Para el caso particular de la gobernanza en el ciberespacio y su relación con la ciberseguridad, esta engloba el diseño y la administración de las tecnologías necesarias para mantener el funcionamiento, así como la promulgación de políticas sustantivas en torno a estas tecnologías (DeNardis, 2014, pág. 6). Con base en esto, la arquitectura operacional de éste incluye estándares técnicos, recursos críticos como las direcciones binarias necesarias para acceder a Internet, el sistema de nombres de dominio (DNS)[39], los sistemas de intermediación de información como motores de búsqueda, las redes necesarias para las transacciones financieras, sistemas de acceso a Internet, puntos de intercambio de Internet e intermediarios de seguridad de internet (DeNardis, 2014, págs. 6-7)

Asimismo, la gobernanza global del ciberespacio se lleva a cabo principalmente a través de las relacione informales entre los miembros de la comunidad operativa de Internet, Estados, grupos no gubernamentales e instituciones intergubernamentales basadas principalmente en el principio de confianza (Mueller, 2010). Estas interacciones pueden caracterizarse como una organización de redes o como un tipo de producción entre pares, o ambos procedimientos de manera simultánea. Como lo subrayan algunos especialistas, "los protocolos de internet descentralizan y distribuyen la participación y la autoridad sobre la creación de redes y garantizan que las unidades de toma de decisiones sobre las operaciones ya no estén estrechamente alineadas con las unidades políticas" (Mueller M. L., 2010, pág. 5).

[39] Los nombres de dominio son los nombres alfanuméricos únicos, que hacen que los sitios web sean fácilmente localizables para las personas. El sistema de nombres de dominio (DNS) es el conjunto distribuido de servidores que traducen los nombres de dominio alfanuméricos a sus direcciones de Internet asociadas (DeNardis, 2014, pág. 25)

Por un lado, el estudio de la gobernanza del ciberespacio es un subconjunto de un ámbito más amplio de la investigación sobre estudios de Internet (DeNardis, 2014, pág. 19). A su vez, el análisis se edifica bajo cuatro preceptos: *1)* el estudio de la gobernanza de internet es distinto del estudio del uso de internet; *2)* los problemas de la gobernanza de Internet se relacionan con la arquitectura técnica única de Internet en lugar de la esfera más amplia del diseño y la política de la tecnología de la información y la comunicación; *3)* la práctica de la gobernanza de Internet se extiende más allá de instituciones como las organizaciones que establecen estándares, las políticas de la industria privada, las políticas nacionales, los tratados internacionales y el diseño de la arquitectura técnica y; *4)* la gobernanza de Internet incluye formas de control arquitectónico orientadas a promover la interoperabilidad y el acceso al conocimiento, pero desafortunadamente también incluye aquellas técnicas dirigidas a restringir la libertad de Internet (DeNardis, 2014, págs. 19-20).

En otras palabras, "la gobernanza global de Internet considera como objeto principal de investigación a los sistemas técnicos e institucionales necesarios para la operatividad de internet" (DeNardis, 2014, pág. 21). Para otros autores, la gobernanza global de internet es simplemente "aquellos principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos que dan forma a la evolución y el uso de Internet" (Mueller M. L., 2010, pág. 9). Por otro lado, el estudio de la gobernanza de Internet históricamente ha centrado su atención en dos áreas específicas: *1)* los marcos regulatorios nacionales e internacionales y; *2)* la función de gobernanza de ICAAN (*Internet Corporation for Assigned Names and Numbers*) y las instituciones asociadas que administran los recursos críticos de Internet (DeNardis, 2014, pág. 22).

Es por ello que, las acciones en el ciberespacio requieren que los actores sigan reglas básicas que garanticen la interoperabilidad, conocidas como estándares.[40] Este enfoque basado en estándares se remonta al comienzo de Internet cuando

[40] La autoridad para la toma de decisiones sobre los estándares y los recursos críticos de Internet descansa en manos de una red transnacional de actores que surgió orgánicamente junto con Internet, fuera del sistema gubernamental (Mueller, 2010).

varios ingenieros crearon los sistemas iniciales para buscar retroalimentación sobre los estándares propuestos (*Requests for Comments*) (Singer & Friedman, 2014, pág. 27). Con el tiempo, este grupo de ingenieros e investigadores se convirtió en una organización internacional de estándares llamada *Internet Engineering Task Force* (IETF).[41] En la actualidad, la tarea de IETF es desarrollar nuevos estándares y protocolos de internet y modificar los existentes para un mejor rendimiento. Además, la IETF se reúne tres veces al año, en grupos de investigadores que deciden lo que constituye el sistema nervioso de internet: protocolos, sistema de nombres de dominio (*domain name system,* DNS) y los protocolos de puerta de enlace de frontera (*border gateway protocol*, BGP) (Klimburg, 2017, pág. 95).

En efecto, los identificadores como las direcciones de los protocolos de internet (*internet protocol*) y los dominios deben ser únicos. Internet no funcionaría si varias partes intentaran usar la misma dirección IP.[42] Todas las actividades en Internet son datos que se dirigen desde una dirección de protocolo de internet (*internet protocol address*) hacia otra dirección. Los dominios definen la identidad en Internet, lo que genera un fuerte interés comercial y político que puede desembocar en conflicto (Singer & Friedman, 2014, págs. 28-29). Por ende, la asignación de nombres y números significa controlar quién puede acceder a Internet y cómo (Klimburg, 2017). Las decisiones sobre quién obtiene qué en Internet crea intrínsecamente ganadores y perdedores (DeNardis, 2014). Como bien lo mencionan P.W. Singer y Allan Friedman (2014, págs. 28-29) “Internet puede tener un tamaño aparentemente infinito, pero todavía tiene juegos de suma cero”.

Por esta razón, la asignación de números de protocolo de internet (IPN) y los sistemas autónomos de numeración asociados[43], junto con la gestión del sistema

[41] El IEFT no tiene una estructura orgánica oficial, junta de consejo o liderazgo formal. Esta organización está bajo los auspicios de la llamada *Internet Society* (ISOC), un grupo internacional formado en 1992 que supervisa la mayor parte del proceso de estándares técnicos. Para algunos especialistas, la ISOC surgió cuando la gobernanza de Internet se movió más allá de cuestiones de coordinación técnica (Singer & Friedman, 2014, pág. 28).

[42] Los protocolos son convenciones que gobiernan la conmutación de paquetes. Es similar a poner la dirección en una carta siguiendo las convenciones como: colocación del destino, la dirección del remitente, la ubicación y cantidad de estampillas, sin importar el contenido o tamaña de la carta (Ceruzzi, 2018, pág. 173)

[43] Los sistemas autónomos de numeración (ASN, *Autonomous System Numbers*) son combinaciones numéricas binarias únicas asignadas a un operador de red. En conjunto, estos son

de nombres de dominio (DNS) se concentró en la Autoridad de Números Asignados de Internet (IANA, *Internet Assigned Numbers Authority*) (Klimburg, 2017, pág. 100)[44]. Sin embargo, la creciente presión por el desarrollo de una Internet comercial y la constatación de que esta estructura no podía ser manejada bajo el auspicio único del gobierno de los Estados Unidos de manera prolongada y, después de un período de consulta entre la opinión pública y las organizaciones y líderes clave de Internet, la responsabilidad se trasladó a una corporación independiente con una estructura de gobierno que pretendía "reflejar la diversidad geográfica y funcional de Internet" (Singer & Friedman, 2014, pág. 29).

Con esto, en 1998, nació la Corporación de Internet para la Asignación de Nombres y Números (ICANN, *Internet Corporation for Assigned Names and Numbers*) (Klimburg, 2017, pág. 101). A razón de lo anterior, la ICANN tenía la facultad para gestionar nombres y números de Internet, donde incluía a IANA, los registradores de Internet y los registros regionales de Internet (RIR) (DeNardis, 2014, pág. 22)[45]. Algunos expertos en el tema de la gestión de ICAAN han utilizado el término “proceso de múltiples partes interesadas” (*multi-stakeholder process*) para describir el enfoque procedimental de la organización, como orgánico, abierto y flexible (Singer & Friedman, 2014).

Bajo este esquema, las prácticas de los operadores de Internet se pueden conceptualizar como un tipo de gobernanza en red (Mueller M. L., 2010, pág. 7). Con base en esto, los proveedores de servicios de Internet, asociaciones empresariales, grupos transnacionales de defensa, gobiernos y expertos individuales establecen políticas y negocian entre ellas qué se bloquea y qué puede fluir, qué se autentica y qué no, así cómo la respuesta a las amenazas y fallos de la

los principales identificadores virtuales que mantienen el funcionamiento de Internet (DeNardis, 2014, pág. 25)

[44] La IANA funcionó por medio de un contrato de funciones bajo la supervisión del Departamento de Comercio del gobierno de los Estados Unidos de América hasta 2016 (Klimburg, 2017, pág. 100).

[45] Los registros regionales de internet a nivel mundial son los siguientes: Centro de Información de la Red Africana (AfriNIC), Centro de Información de la Red Asia Pacífico (APNIC), el Registro Americano para los Números de Internet (ARIN, que conforman Estados Unidos, Canadá e islas en el Atlántico Norte), Centro de Información de la Red de Latinoamérica y el Caribe (LACNIC) y el Centro de Coordinación de la Red Europea-Réseaux IP Européens (RIPE NCC) (DeNardis, 2014, pág. 53)

red (Mueller M. L., 2010, pág. 8). Por tanto, se supone que las decisiones se toman por consenso, mientras que un de comité anfitrión de asesores ayuda a representar a las principales partes interesadas en las operaciones de Internet. Por su parte, los intereses gubernamentales están representados a través de un Comité Consultivo Gubernamental (GAC, por sus siglas en inglés, *Governmental Advisory Committee*) (Singer & Friedman, 2014, pág. 30).

En suma, esta forma en cómo se organizan diversos agentes y procesos de gestión, quién puede participar, quién está representado y cómo interactúan los interesados se le conoce como "gobierno de múltiples partes interesadas" (*multistakeholder governance*) (Mueller M. L., 2010, págs. 7-8). Asimismo, otras instituciones importantes de gobernanza de internet que establecen estándares son el *World Wide Web Consortium* (W3C), el IETF, la Unión Internacional de Telecomunicaciones (ITU), el *Institute of Electrical and Electronics Engineers* (IEEE), la *International Electrotechnical Commission* y *la International Organization for Standardization* (DeNardis, 2014, págs. 22-23).

Por ejemplo, algunas de ellas realizan funciones de autenticación de datos e información. En otras palabras, cuando alguien accede a un sitio web debe tener certeza de que estos sitios son realmente operados por compañías certificadas en lugar de sitios falsificados. Es decir, en la realización de operaciones comerciales y financieras en línea se depende en gran medida de procesos de autenticación confiables que verifican la legitimidad de los sitios en línea. Este enfoque de seguridad es conocido como 'criptografía de clave pública'. Esta función se realiza al asociar un código de encriptación único o certificado, con un servidor web, para que un navegador sepa si un sitio web visitado es auténtico o no. Estas entidades son conocidas como autoridades de certificación (DeNardis, 2014, pág. 93).

Finalmente, también se encuentran organismos público-privados llamados equipos de respuesta ante incidentes de seguridad informática o equipos de respuesta ante emergencias informáticas (CSIRT, *computer security incident response teams* o CERT, *computer emergency response teams*), que tiene como tarea coordinar respuestas a problemas e incidentes de seguridad en internet, además de crear programas pedagógicos sobre ciberseguridad para el público en

general.[46] Los CERT funcionan como centros de enlace entre proveedores de productos o servicios digitales y personas, en particular, a través de la identificación de vulnerabilidades y riesgos, así como emisión de soluciones técnicas. En la tabla 3.2, se puede apreciar de manera más sistemática cómo es la organización de la gobernanza de Internet, qué entidades participan y sus principales funciones para mantener la operatividad de la red y e infraestructura informática global.

Tabla 3.2 Organizaciones que participan en la gobernanza global de Internet

Organización	**Materia de competencia**	**Participación en cuestiones de ciberseguridad**
• ICANN (Internet Corporation for Assigned Names and Numbers) IANA (Internet Assigned Numbers and Authority) Registros Regionales de Internet (RIR)	Supervisan el sistema de nombres de dominio (DNS), la asignación del espacio de direcciones del protocolo de Internet y supervisan los servidores de la zona raíz que proporcionan información básica para la búsqueda del tráfico de Internet.	X
• ISOC (Internet Society) • IETF (Internet Engineering Task Force) • Internet Engineering Steering Group • Internet Architecture Board	Desarrollan estándares para el funcionamiento de internet y su arquitectura global. Desarrollar nuevos estándares y protocolos de internet y modificar los existentes para un mejor rendimiento	X

[46] En 1988 nace el primer Equipo de Respuesta ante Emergencias Informáticas (CERT) debido al incidente Morris (*Morris Worm*), un código malicioso que llegó a infectar hasta un 10% de los dispositivos conectados a la Internet. Con base en ello, en Estados Unidos se establecieron el CERT/CC en el Instituto de Ingeniería de la Universidad Carniege Mellon y el US-CERT dentro del Departamento de Defensa de los Estados Unidos de América. Actualmente existen más de 250 equipos de respuesta ante emergencias informáticas en el mundo, algunos son entidades públicas, privadas o compuestas tanto por agentes públicos como privados (DeNardis, 2014, pág. 91).

• World Wide Web Consortium	Desarrolla estándares para la World Wide Web.	
• Unión Internacional de Telecomunicaciones	Desarrolla estándares para telecomunicaciones, incluyendo interfaz de internet y sistemas de telecomunicaciones.	X
• Agencias de las Naciones Unidas • Organización para la Cooperación y Desarrollo Económico • Unión Europea, Consejo de Europa	Desarrollo de políticas en temas de interés crítico para sus miembros**.**	X*
• Gobiernos Nacionales y Registros Nacionales de Internet	Desarrollo de política relacionadas principalmente con ciberdelincuencia, usos de la red, y cuestiones de reglamentaciones comerciales digitales	
• Institute of Electrical and Electronics Engineers • International Electrotechnical Commission • International Organization for Standardization	Desarrolla normas para productos y para procesos de fabricación electrónicos. Las operaciones de estas entidades se relacionan solo periféricamente con la operación de Internet en sí misma.	X**
• Equipos de Respuesta a ante Incidentes de Seguridad Informática, *Computer Emergency Response Teams* (CERT) o *Computer Security Incident Response Teams* (CSIRT)	Coordinan respuestas a problemas e incidentes de seguridad en internet. Crear programas pedagógicos sobre ciberseguridad para el público en general	X

Fuente: (Kwalwasser, 2009, pág. 494) (Starr, 2009, págs. 68-69)

* La Organización de las Naciones Unidas no participa directamente en el establecimiento de estándares sobre ciberseguridad a diferencia de los otros mecanismos internacionales
** Únicamente la *International Organization of Standarization* participa en el establecimiento de normas y estándares de ciberseguridad.

Por ende, la intersección entre los aspectos técnicos y no técnicos del manejo del sistema de dominios es lo que está produciendo diferendos sobre la gobernanza global del ciberespacio (Singer & Friedman, 2014). De acuerdo con algunos autores, la competencia por la preeminencia de poder global en este plano, "muestra lo importante que es la tecnología para el futuro de la competencia interestatal global, del poder económico e incluso de la seguridad internacional" (Knight, 2019). Sin embargo, si bien es cierto que, los gobiernos supervisan y ejecutan muchas funciones de gobernanza en el ciberespacio, la mayoría de las funciones de gestión y administración de Internet no han sido históricamente el dominio de los gobiernos, sino que se han ejecutadas a través de mecanismos privados de diseño técnico y formas institucionales no gubernamentales (DeNardis, 2014, pág. 11).

No obstante, los gobiernos han buscado decididamente tener una mayor participación y un papel relevante en cuanto a la formulación de las políticas de comunicación e información a nivel global que se suscitan en el ciberespacio. Para el especialista Milton Mueller (2010, pág. 10), "el nacimiento de la Cumbre Mundial sobre la Sociedad de la Información en 2002 (WSIS, *World Summit on the Information Society*) marcó un hito sin precedentes sobre los objetivos y estrategias gubernamentales relacionadas con la sociedad de la información". Sobre todo, estos espacios de deliberación política proporcionaban por primera vez una plataforma para que algunos gobiernos pudieran desafiar la preeminencia del gobierno estadounidense en el régimen de gobernanza vigente y la poca participación estatal. Asimismo, las acciones gubernamentales han movilizado una amplia gama de redes de defensa como contra respuesta a las acciones estatales en torno a cuestiones de formulación de política de comunicación e información de carácter global (Mueller M. L., 2010, págs. 10-11).

De acuerdo con este enfoque, aquellas voces que pugnan por una participación gubernamental más decidida en el régimen global ciberespacial y de ciberseguridad sugieren que los gobiernos deben ayudar a codificar un conjunto de reglas

duraderas para un mejor desempeño de éste, así como crear una estructura de incentivos para reducir las actividades de espionaje y sabotaje cibernético; crear mecanismos para alertar a las empresas de tecnología sobre las vulnerabilidades en software y; tomar medidas adicionales para hacer inviolables las comunicaciones en Internet (Rovner & Moore, 2017, págs. 185-186). Actualmente, la apuesta gubernamental es tener mayor injerencia en los aspectos técnicos, es decir, en el núcleo y la raíz del centro operativo del ciberespacio (Broeders, 2015; Mueller, Mathiason, & Klein, 2007; Mueller M. , 2002).

Bajo esta perspectiva, el debate en curso sobre el nivel apropiado de intervención estatal es en realidad una discusión sobre si el ciberespacio puede funcionar o no por su cuenta (Rovner & Moore, 2017, pág. 188). Existen argumentos que subrayan que Internet y el ciberespacio han demostrado ser notablemente auto-regulables y resistentes a las conmociones a través de reglas informales de gobierno que han fomentado un flujo libre de información e innovación ininterrumpido. Además, plantean que las empresas y los usuarios de Internet tienen enormes incentivos para mantener el sistema en funcionamiento, independientemente de cómo se comporten los Estados (Rovner & Moore, 2017, pág. 188).[47]

Como consecuencia, la seguridad y los procesos de securitización se están convirtiendo en palancas y conductores de la gobernanza del ciberespacio. Entre los Estados, por un lado, el problema de la ciberseguridad intensifica la necesidad de cooperación y armonización jurídica internacional, y por otro lado, también fomenta respuestas nacionales particulares en competencia. (Mueller M. L., 2010, pág. 161). La realidad de la gobernanza de ciberseguridad es de cambio estructural y adaptación a nivel nacional e internacional en relación con respuesta coordinadas para minimizar el impacto de diversas amenazas sobre la operatividad del ciberespacio (Mueller M. L., 2010, pág. 161; DeNardis, 2014). Una transformación relevante es cómo las organizaciones y los involucrados responden a las amenazas

[47] Bajo esta perspectiva, los ataques cibernéticos pueden interrumpir temporalmente el servicio, pero el sistema en su conjunto continuará funcionando porque los actores acelerarán los esfuerzos para fortalecer la defensa cibernética y restablecer el acceso y funcionamiento de la red (Rovner & Moore, 2017)

cibernéticas, cómo perciben las acciones cibernéticas de otros y cómo se convierten en un elemento normal del proceso de construcción de la amenaza en las Relaciones Internacionales cibernéticas. Para comprender esto, en la tabla 3.3 se pueden observar algunos de las formas en las que está compuesta la gobernanza del ciberespacio en el área de la seguridad.

Tabla 3.3 Esquemas de gobernanza de ciberseguridad

Tipo de gobernanza	**Prácticas y normativas**
Institucionalización cibernética internacional	• Gobernanza en red de cuestiones digitales • Instituciones para el manejo de lo cibernético • Instituciones internacionales de ciberseguridad • Tratados internacionales cibernéticos
Normas globales y producción de bienes públicos	• Derechos políticos cibernéticos • Facilitar el abastecimiento y el intercambio de conocimiento e información • Consolidación de normas internacionales cibernéticas
Construcción de agenda global	• Exploración de precedentes internacionales y buenas prácticas de asuntos internacionales similares • Desarrollo de comportamientos, normas cibernéticas y discusión pública relacionados con la gobernanza del ciberespacio

Fuente: (Choucri, 2012, pág. 158; Mueller M. L., 2010)

Al mismo tiempo, una diversidad de partes interesadas sostiene un conjunto variado de ideas acerca de cómo el ciberespacio deber ser utilizado y gobernado. Para algunos expertos, “esto ha impedido que la conducta maliciosa en el ciberespacio decrezca”, e incluso claman por “un esfuerzo diplomático concertado para construir una coalición sustancial de Estados con ideas afines, dispuestos no solo a adherirse

a *normas cibernéticas* sino también a imponer costos económicos y políticos graves a quienes las violan" (Flournoy & Sulmeyer, 2018, pág. 44).

Es importante destacar que los Estados son jugadores en estos acuerdos, pero "rara vez están en posición de ejercer un poder jerárquico" (Mueller M. L., 2010, pág. 163). A nivel internacional se lleva a cabo un proceso de institucionalización incipiente que busca consolidar e implementar nuevas normas cibernéticas, y de esa manera obligar a los actores cibernéticos internacionales a que se ajusten a los entendimientos colectivos como: *a)* reducir la incertidumbre en los procesos y resultados de la información generada; *b)* generar y mantener modos compartidos de comunicación, comprensión y explicaciones de los procesos; *c)* facilitar la mediación entre actores en conflicto; *d)* mejorar las perspectivas generales para la resolución de problemas (Choucri, 2012, págs. 156-157). Es por ello que coordinar la actividad en el ciberespacio se ha convertido en un desafío crucial. Para tal fin, en el siguiente apartado se busca exponer cómo se dan estos arreglos y cuáles siguen siendo las cuestiones en las que el debate sobre la gobernanza global de la ciberseguridad sigue abierto.

3.2.1 Reglas, normas y principios sobre la ciberseguridad a nivel gubernamental y global

Virtualmente cada sector de la sociedad de una gran cantidad de países depende de la comunicación en Internet y de las interacciones en el ciberespacio para desempeñar las funciones básicas de la vida moderna (Finnemore M. , 2011, pág. 89). A nivel internacional, un conjunto de gobiernos ha tratado de diseñar normas para orientar la conducta en el ciberespacio en tiempos de paz (Flournoy & Sulmeyer, 2018). Por ejemplo, en 1998, Rusia propuso por primera vez, en el marco las Naciones Unidas, un tratado para prohibir el desarrollo de armas electrónicas y de información, incluso con fines de propaganda (Nye J. S., 2018). No obstante, la propuesta no fue acogida por otros gobiernos y quedó en letra muerta.

Después de esto, en octubre de 2001, el Consejo de Europa concluyó las negociaciones sobre el Convenio de Budapest sobre Delito Cibernético. Cabe resaltar que este es el único acuerdo vinculante que regula específicamente algún

aspecto del comportamiento en el ciberespacio (Klimburg, 2017, págs. 320-321). Por su parte, algunos mecanismos gubernamentales internacionales como el G-7 y el G-20 han emitido declaraciones conjuntas comprometiendo a sus miembros a sostener un buen comportamiento en línea, pero carecen de aspectos vinculantes (Flournoy & Sulmeyer, 2018, pág. 44). Por otra parte, se creó un Grupo de Expertos Gubernamentales (UNGGE, *United Nations Group of Govermental Experts*) que se reunió por primera vez en 2004, y en julio de 2015 donde se planteó un conjunto de normas que luego fue respaldado por los países que componen el foro G-20.

En este sentido, algunas perspectivas académicas han enfatizado sobre la importancia del desarrollo de normas sobre privacidad y seguridad con respecto la programación, encriptado y cifrado de la información, la eliminación de las puertas traseras en hardware (*backdoors*), la mitigación de los discursos de odio, la desinformación y las amenazas terroristas para el mantenimiento del funcionamiento del ciberespacio (Nye J. S., 2018).[48] Por consiguiente, hay quienes han recalcado que "sin algunas reglas básicas, el conflicto entre valores y visiones en competencia sobre la gestión de recursos en el ciberespacio se intensificará" (Finnemore M. , 2011, pág. 89).

Por un lado, expertos militares y de seguridad conciben la Internet como una herramienta para coordinar actividades de combate al terrorismo y al crimen organizado (Weimann, 2005) (Wills, 2017). Por otro lado, varios gobiernos nacionales tienen diferentes puntos de vista sobre cuáles son los usos legítimos de Internet y están presionando para obtener reglas que reflejen su preferencia (Finnemore M. , 2011, pág. 89). Por su parte, algunos gobiernos perciben que su capacidad para influir y gobernar a sus poblaciones se ve socavada por un libre flujo de información (Krishna-Hensel, 2007, pág. xi). Para otros gobiernos, la ciberseguridad es vista como una herramienta que permite resguardar la seguridad nacional. En suma, el rango y el grado de control estatal, así como la censura, y la percepción sobre los mecanismos para fortalecerla varían en función del enmarcado

[48] Para 2020, el número estimado de contraseñas mundiales crecerá hasta alcanzar los 300 mil millones (CISCO/Cybersecurity Ventures, 2019).

de los intereses, así como del entorno de amenaza percibido, lo cual conduce a la imposición de controles estatales específicos (Krishna-Hensel, 2007, pág. xii).

Por consiguiente, el ámbito cibernético presenta desafíos únicos para el desarrollo de normas, pues pocas áreas problemáticas penetran en todos los aspectos de la sociedad tan a fondo como éste (Finnemore M. , 2011). Sin embargo, el hecho de que las leyes tradicionales sean cada vez más difíciles de aplicar no significa que el mundo cibernético sea el "Salvaje Oeste" (Chappell, 2015).[49] Si bien es cierto que, la coordinación de las partes interesadas no es sencilla, no obstante, se están haciendo esfuerzos para actualizar los códigos antiguos o crear otros nuevos.

Por ejemplo, después del incidente de Estonia en 2007 (Rid, 2012; Davis, 2007; Blank, 2008), se creó el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (*Cooperative Cyber Defense Centre of Excellence*), el Centro de Capacidad de Respuesta a Incidentes Computacionales de la OTAN (*Computer Incident Response Capability*) y la Autoridad de Gestión de Defensa Cibernética (*Cyber Defence Management Authority*) (Kuehl, 2009).[50] Junto con este esfuerzo, se encargó a veinte profesores de derecho que examinaran formalmente cómo las leyes de guerra tradicionales se aplican al ciberespacio, en un documento titulado "*Tallin Manual on the International Law Applicable to Cyber Warfare*" (Singer & Friedman, 2014, pág. 123) (Schmitt, M. N., 2017).

[49] Esta analogía fue utilizada por el ex presidente de los Estados Unidos de América, Barack Obama en 2015. Esto puede ser una muestra de una percepción gubernamental sobre el ciberespacio, y sobre el papel que están dispuestos a desempeñar los agentes estatales como 'pacificadores' de un terreno 'agreste y sin ley'.

[50] Para varios analistas, lo que sucedió en Estonia entre abril y mayo de 2007 se considera el primer caso de una 'guerra cibernética'. En ese momento, el gobierno estonio había decidido la remoción de una estatua de un combatiente soviético de la Segunda Guerra Mundial. Esto generó fuertes protestas por las comunidades rusas en Estonia, que también se manifestaron en el espacio digital. Durante los sucesos, los sitios web gubernamentales, diarios, compañías comerciales y las redes financieras fueron paralizados durante un par de semanas a través de mecanismos distribuidos de denegación de servicios (DDoS). Para algunos circulos gubernamentales, era preocupante las consecuencias de la interrupción de servicios, porque Estonia era uno de los países más interconectados en el mundo. Esto ha creado que la ansiedad sobre un cataclismo cibernético sea mayor (Rid, 2012). Los incidentes cibernéticos duraron alrededor de tres semanas y fueron de una escala amplia. Para una versión detallada del suceso ver (Traynor, 2007).

Con ello, en el ámbito bilateral gubernamental son cada vez más recurrentes los mecanismos de diálogo en temas de ciberseguridad (Lu C. , 2017). En relación con las implicaciones, algunos especialistas apuntan a que la forma principal de determinar cuándo un ataque cibernético constituye un uso de la fuerza que legalmente justifica la guerra es través de sopesar sus efectos (Liff, 2012) (Rid, 2012). A partir de ello, bajo este lente, se debe observar la cantidad de daño causado o la intención de provocar perjuicio, y establecer un paralelismo con el plano físico.[51] Aunque, enfocarse en el impacto es importante, el verdadero desafío es el área intermedia entre incidentes de destrucción e interrupción de servicios e infraestructura (Singer & Friedman, 2014, pág. 124). No obstante, para algunos autores el objetivo de los gobiernos no es controlar cierta clase de armas, "sino controlar las expectativas y desarrollar un conjunto de principios, reglas y procedimientos y normas sobre de comportamiento con respecto a un dominio completo" (Deibert R. , 2011). Es por ello que, cultivar las normas cibernéticas puede verse como un desafío continuo. Ciertamente, como apunta la académica Martha Finnemore (2011, pág. 90) "es probable que la inseguridad cibernética sea una enfermedad crónica que debe ser tratada constantemente en lugar de ser un problema único que debe resolverse y descartarse".

3.2.2 Participación de actores no estatales en la conformación de las políticas de ciberseguridad

En efecto, los gobiernos también pueden no ser los mejores o los únicos actores que están haciendo las reglas en esta área, ya que gran parte de la tecnología está en manos privadas (Deibert R. J., 2013). Aunque las corporaciones tecnológicas y de medios globales controlan un número desproporcionado de procesos de producción y distribución, no tienen el monopolio de los mercados en los que

[51] En agosto de 2008, hubo un enfrentamiento armado entre Rusia y Georgia, el cual combinó ataques militares terrestres rusos con varios incidentes el campo cibernético, principalmente la desconfiguración de los sitios gubernamentales georgianos y la desfiguración de la imagen del entonces presidente Mikheil Saakashvili, suplantada por la de Adolf Hittler. Para diversos analistas esta es la primera guerra híbrida que combina medios cinéticos con mecanismos cibernéticos. No obstante, la atribución de las acciones cibernéticas rusas no ha podido ser esclarecida completamente (Danchev, 2008)

operan, “hay contraflujos que influyen en la forma y estructura del funcionamiento de los gigantes mediáticos” (Castells, 2009, pág. 132). Si bien algunos Estados mantienen una gran parte del control sobre la estructura y el contenido de su participación en el ciberespacio (Palfrey, 2010; Goldsmith & Wu, 2006), a medida que la red global de comunicaciones continúa desarrollándose a un ritmo rápido impulsado por desarrollos innovadores en tecnología, la capacidad gubernamental para asegurar que el buen funcionamiento de las redes se basa cada vez más en la interdependencia entre las agencias gubernamentales y los agentes privados (Krishna-Hensel, 2007, pág. xi; Harris S. , 2014).

En otras palabras, estos actores privados poseen y gestionan una gran proporción del tráfico de banda ancha que circula por las superautopistas de la información (Vaidhyanathan, 2018; Pariser, 2011). Asimismo, una gran cantidad del flujo de Internet cruza por redes controladas por compañías de telecomunicaciones de primer nivel mundial, principalmente estadounidenses, aunque no únicamente (AT&T, CenturyLink, XO Communications, Verizon, Tencent) (Choucri, 2012, pág. 128). Asimismo, los servicios de redes sociales son en su mayoría proporcionados por grandes corporaciones que tienen su sede principal en los Estados Unidos y en la República Popular de China (Google, Facebook, Yahoo!, Twitter, YouTube, WeChat, Weibo, QQ). De esta manera, estas empresas en su conjunto se han convertido en responsables de limitar el espacio virtual gratuito (Deibert R. J., 2013, pág. xv).

A su vez, un desarrollo interesante es el reconocimiento por parte de la industria privada de que la intervención del gobierno es necesaria para soluciones de seguridad de la información (Krishna-Hensel, 2007, pág. xii). Este cambio de actitud refleja la conciencia de que las fuerzas del mercado no pueden ser el único impulsor de las mejoras de la industria. Y aunque, las vulnerabilidades en el ciberespacio han sido evidentes para los gobiernos y las empresas, estos no han logrado solucionar los problemas de coordinación (Flournoy & Sulmeyer, 2018). No obstante, se ha identificado que las acciones tomadas en el sector público afectan al sector privado y viceversa, de esta manera, el ciberespacio ha sido de naturaleza híbrida (Flournoy & Sulmeyer, 2018, pág. 40).

Por un lado, una característica única en la gobernanza del ciberespacio es la expectativa de que algunas entidades privadas están obligadas a llevar a cabo las funciones de aplicación de la ley que tradicionalmente realiza el Estado sin compensación y, a menudo, con gastos adicionales, incluso con repercusiones sobre su reputación (DeNardis, 2014, pág. 13). Sin embargo, este fenómeno de privatización y delegación no es exclusivo de los problemas de control de Internet, sino que forma parte de una condición de un fenómeno global de privatización de funciones tradicionalmente realizadas por el Estado (DeNardis, 2014, pág. 13).

Por otro lado, los gobiernos han reconocido cada vez más que solos no pueden proporcionar el creciente número de servicios públicos que necesitan las sociedades modernas, especialmente en el ciberespacio. A la inversa, los sectores privados han reconocido que la ayuda gubernamental en el contexto de la ciberseguridad es necesaria. En general, los Estados colaboran en la búsqueda de intereses comunes y en la gestión de las aversiones comunes (Choucri, 2012). En primera instancia, los gobiernos buscan cooperar como una forma de perseguir conjuntamente un objetivo que tal vez no puedan alcanzar individualmente. En segunda instancia, hay un reconocimiento de que enfrentan condiciones adversas compartidas que requieren una acción coordinada para la administración del riesgo más efectiva (Choucri, 2012, pág. 156).

Para autores como Alexander Klimburg (2017), el gobierno y la industria pueden trabajar juntos para proteger Internet y promover un mejor comportamiento en línea. Incluso para analistas y consejeros gubernamentales como Michèle Flournoy[52] y Michael Sulmeyer[53] mencionan que “construir dicha asociación es esencial, aunque también es difícil, ya que las dos partes a menudo tienen intereses en conflicto” (2018, pág. 44). Para tal efecto, la cooperación entre gobiernos y el sector privado principalmente gira en torno al intercambio de información. Justamente, el intercambio de información se ha consolidado fundamentalmente entre las

[52] Se desempeñó como subsecretaría de asuntos políticos en el Departamento de Defensa de los Estados Unidos de América de 2009 a 2012.

[53] Es director del Programa de Ciberseguridad en el Belfer Center de la Universidad de Harvard. De 2012 a 2015 fungió como Director para Operaciones y Planes Cibernéticos en la oficina del Secretario de Defensa de Estados Unidos de América.

instituciones financieras, los contratistas de defensa y el ejército, pero en otras áreas, esta dinámica ha quedado sin realizarse (Flournoy & Sulmeyer, 2018, pág. 44).[54] Con base en ello, ciertos especialistas, reconocen que el mayor desafío para los gobiernos es "comprender cómo fomentar la seguridad de la información sin tratar de luchar contra la arquitectura de operaciones y socavar los beneficios del ciberespacio" (Singer & Friedman, 2014, págs. 196-197).

3.2.3 Los actores estatales y la conformación de las políticas de ciberseguridad

Con objeto de dar respuesta a amenazas globales cada vez más difusas que se presentan en el ciberespacio, algunas perspectivas apuntan a que se requiere una acción coordinada, así como también, la participación e interacción de numerosos agentes, con diferentes responsabilidades, estructuras de gestión e incentivos. (Singer & Friedman, 2014, pág. 215). Algunas de las fuentes de amenazas más constantes en el ciberespacio, sus ejecutores, sus diversas motivaciones y las principales herramientas que utilizan cada uno se detallan en la tabla 3.4.

Tabla 3.4 Fuentes de amenaza para la ciberseguridad

Fuente de amenaza	**Motivación**	**Herramientas utilizadas**
Servicios de inteligencia	Uso de herramientas cibernéticas como parte de sus actividades de recopilación de información y tareas de espionaje. Estos incluyen la explotación, interrupción o posible destrucción de la infraestructura de información	• Desarrollo de herramientas *zero-da*y • Gusanos • Amenazas persistentes avanzadas (APT)
Grupos criminales		• Botnet

[54] El aumento de la ciberseguridad como problemática ha ido de la mano con un auge en el número de empresas que intentan obtener réditos con esta. Por ejemplo, en 2013, el valor del mercado de la ciberseguridad los Estados Unidos se estimó en $65 mil millones de dólares y se prevé que crezca a una tasa del 6 al 9 por ciento al año durante al menos los próximos cinco años (Singer & Friedman, 2014, pág. 163)

	Utilizan con el objetivo de obtener ganancias económicas	• Phishing • Virus • Ransomware
Grupos terroristas	Buscan destruir, incapacitar o desestabilizar infraestructuras críticas con el propósito de amenazar la seguridad nacional, debilitar la economía, dañar la moral pública y socavar la confianza (infundir terror)	• DDoS • Botnet • Virus • Malware
Hackers	Penetrar en diversas redes informáticas, con el propósito de demostrar habilidades de programación, tratar de observar las vulnerabilidades de alguna red, o buscar explotar las debilidades de alguna red a beneficios personal o de alguna organización.	• Desarrollo de herramientas *zero-da*y • Gusanos • Virus • DDoS • Botnet • Phishing
Activistas digitales	Conducir ataques con motivos políticos para modificar comportamientos y establecer nuevos temas en la agenda política, económica y social	• DDoS • Botnet
Internos insatisfechos (*insider disgruntled*)	Cuentan con acceso a sistemas de seguridad informáticos que les permiten causar daños a las redes o les facilita el acceso a datos que	• DDoS • Revelaciones de información • Chantaje

	pueden aprovechar para cometer diversos actos delictivos informáticos.	

Fuente: (Reveron, 2012, pág. 12)

Una de las características más sobresalientes de la ciberseguridad es que incluye tanto los límites tradicionales como no tradicionales de ejecución de políticas públicas. Además, la ciberseguridad es un fenómeno que se desenvuelve en diferentes escalafones de acción, es decir, el gobierno tiene un papel en la aplicación de la regulación, la industria tiene la responsabilidad en la provisión de estándares y de hacer de cumplir los marcos regulatorios, pero, también el ciudadano individual tiene responsabilidad en cuanto a 'higiene digital' (Singer & Friedman, 2014, pág. 241).

Aunado a lo anterior, se está poniendo gran énfasis en la necesidad de desarrollar una cultura global de ciberseguridad en respuesta al reconocimiento de que la seguridad de la red es una garantía para la supervivencia económica y para la infraestructura global de información (Krishna-Hensel, 2007, pág. xii). Esto debido a que la infraestructura crítica que alimenta el desarrollo global, en gran medida, opera en lo que se ha convertido en una red globalizada de redes.

Por otra parte, los usos más desafiantes y expansivos de la ciberseguridad vienen cuando se entrelaza con la seguridad militar o la política del Estado (Mueller M. L., 2010, pág. 160). De esta manera, las advertencias sobre amenazas a la "infraestructura crítica" que pueden surgir de los ciberataques están proliferando, a menudo basadas en fuentes no atribuibles (Mueller M. L., 2010, pág. 160)[55]. Esto

[55] No existe una definición académica consensuada para el término "infraestructura crítica". Comúnmente, los gobiernos definen los alcances y los ámbitos que abarca esta, por ello, esta puede variar dependiendo de cada Estado.
Para diversos analistas uno de los problemas más graves en cuanto a la actividad maliciosa en el ciberespacio se relaciona con el problema de la atribución. Muchas formas de *malware* toman el control de los dispositivos de las víctimas formando *botnes* que vinculan diferentes aparatos no relacionados, permitiendo que el controlador aproveche sus capacidades combinadas de transmisión. Es difícil determinar la identidad de quienes están ejecutando el programa contaminado, su nacionalidad o la organización que representan. Además, la atribución se complica aún más por el hecho de que en algunos tipos de ataques, es difícil determinar inicialmente si lo que está sucediendo es una acción hostil (Singer & Friedman, 2014, pág. 73)

es un ejemplo del incipiente proceso de securitización que está surgiendo en el ámbito del ciberespacio. Asimismo, refleja un entorno político imbuido por el enmarcado de la amenaza que trae aparejado el proceso de securitización, donde elementos no relacionados directamente con la seguridad, por ejemplo, la protección de los derechos de autor y el control de contenido ilegal se comienzan a definir, como problemas de seguridad (Mueller M. L., 2010, pág. 160), elementos que se ilustraran en los siguientes capítulos. Si bien la interpretación de intereses y aversiones puede diferir, al igual que las realidades subyacentes, el factor importante aquí es la voluntad de participar en una acción internacional para afrontar dicho desafío (Choucri, 2012, pág. 156), suponiendo que los gobiernos nacionales puedan determinar las condiciones bajo las cuales la acción unilateral es apropiada o las operaciones bilaterales serán efectivas o a la inversa, que no son convenientes.

3.3 El espacio digital, la participación gubernamental y la ciberseguridad

Algunos académicos como el sociólogo Ulrich Beck ubican el riesgo como el centro del cambio social contemporáneo y enfatizan que las preocupaciones se encuentran en el centro de este debate (Beck, 1992). Esto sugiere que los desafíos sociales internacionales no son esencialmente nuevos, sino que la forma en que se tipifican es lo que determina el riesgo que plantean para la sociedad en su conjunto (Krishna-Hensel, 2007, pág. x). Por ejemplo, Ulrich Beck precisa que el riesgo “puede definirse como una forma sistemática de lidiar con los peligros e inseguridades inducidas e introducidas por la modernización en sí misma” (Beck, 1992, pág. 21). Este autor realiza una crítica de la visión liberal utópica del liberalismo; en su análisis, el desarrollo y la creciente dependencia en las tecnologías modernas tienen el efecto constante de producir nuevos riesgos (Beck, 1992) (Beck, 1999). No obstante, su enfoque se concentra en los efectos que las tecnologías de información y comunicación tienen sobre la producción energética y en el comercio, no en su impacto sobre la seguridad (Beck, 1992) (Beck, 1999) (Eriksson & Giacomello, 2006).

A medida que la red global de comunicaciones continúa desarrollándose a un ritmo vertiginoso, y que las actividades sociales dependen cada vez más de disposiciones digitales, los gobiernos y agentes privados se enfrentan con problemáticas en el mundo cibernético y buscan hacerles cara de forma diversa. Estos desafíos, difíciles en sí mismos, se vuelven aún más complejos a medida que el entorno tecnológico cambia rápidamente y que a menudo supera la capacidad de respuesta gubernamental y no gubernamental (Krishna-Hensel, 2007, pág. xi)

Lo que hace particular a la «sociedad de la información» en comparación con otras configuraciones sociales anteriores es la *amplia utilización de la información digital* y la tecnología de comunicación basadas en micro-electrónica (Castells, 1996). Además, cuando Internet surgió, lo hizo sin una coordinación clara o control gubernamental, en lugar de ello, dependió de un grupo de individuos influenciados por ideas liberales y utópicas sobre el papel de la tecnología para su gestación (Peterson, 2011). Los debates sobre las decisiones y los cimientos de la arquitectura digital se debieron en gran parte a una visión de perspectivas abiertas que, de acuerdo con sus primeros arquitectos, debía realizarse mediante un diseño deliberado (Choucri, 2012, pág. 127). De acuerdo con Milton L. Mueller (2010) “la libertad de Internet fue diseñada en sus protocolos; no se necesitó ninguna constitución particular o proceso político para desarrollar sus capacidades (2010, pág. 2).

Conforme con la visión de mundo de los primeros desarrolladores de la Internet no había necesidad de ningún ejercicio de autoridad convincente, por ende, no existiría ningún conflicto distributivo que tuviera que generar una política pública o una necesidad de acción colectiva vinculante (Mueller M. L., 2010, pág. 2; Peterson, 2011). Había una tendencia a ver el ciberespacio como el gran nivelador, lo que permitiría una amplia participación en escenarios virtuales. Como mencionan los académicos Johan Eriksson y Giampiero Giacomello (2006, pág. 225) , “Internet fue diseñado para maximizar la simpleza en la comunicación, no para hacer a la comunicación segura”.

Cuando en 1969 apareció ARPANET, la predecesora de Internet, se trataba de un programa experimental de conexión en red de ordenadores originado en la

Agencia de Proyectos Investigación Avanzados del Departamento de Defensa estadounidense, más conocida por su acrónimo, DARPA, (*Defense Advanced Research Projects Agency*), ejecutado y utilizado en gran medida por los científicos e ingenieros que lo crearon (Castells, 2009, pág. 145). A partir de ese momento, algunos individuos y organizaciones se han concentrado en establecer un ciberespacio independiente, un entorno en el que los gobiernos deben tener poco o ningún poder (Dunn Cavelty & Brunner, 2007).

Una de las muestras más extremas de esta postura es el manifiesto del activista cibernético John Perry Barlow (Barlow, 1996) cuando público su "Declaración de Independencia del Ciberespacio" la cual dice lo siguiente:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> John Berry Barlow,
>
> *A Declaration of the Independence of Cyberspace*, 1996.[56]

Incluso, uno de los más destacados pensadores sobre la revolución digital y de las comunicaciones como Alvin Toffler reafirmaba esta postura, cuando mencionaba que "la humanidad ha pasado de la primera ola de la revolución agrícola a la segunda ola de la revolución industrial, y ahora se encuentra en medio de una tercera ola de turbulencias, donde la tecnología impulsa a una sociedad de la información libre de restricciones económicas, políticas y culturales tradicionales" (Toffler, 1980) (Krishna-Hensel, 2007).

A estos puntos de vista se les ha denominado como entusiastas cibernéticos (o ciberlibertarios) (Mueller M. L., 2010), quienes se han concentrado en las crecientes oportunidades que la aplicación mundial de las nuevas tecnologías de información y la comunicación abren para todos los actores sociales (Dunn Cavelty & Brunner, 2007, pág. 5). Dentro de esta perspectiva, hay una tendencia a ver el ciberespacio

[56] No se ha realizado una traducción al texto original para no perder la esencia y el impacto pretendido por el texto original.

como un espacio de igualdad social (Madrigal, 2019). Los entusiastas cibernéticos enfatizan que el acceso a todo tipo de información, y la capacidad de difundirla ampliamente, conduce a un empoderamiento de los actores sociales frente al Estado o la autoridad, sea esta gubernamental o no (Dunn Cavelty & Brunner, 2007, pág. 5). Implícita en esta visión está la posibilidad eventual de la democratización política a gran escala (Choucri, 2012, pág. 128), y de una comunidad global digital gracias a un mundo completamente conectado (Shirky, 2011).

En efecto, diversos teóricos y políticos de la era de la información afirman que Internet tiene un efecto democratizador (Castells, 2009; Dutton, 1999; Loader, 1997). Como resultado, estas ideas han conducido a debates sobre la "democracia digital", la neutralidad de la red (*network neutrality*)[57] y el uso de Internet como una herramienta indispensable para apoyar una mayor participación cívica en el proceso democrático y las medidas que se deben llevar a cabo para alcanzar un acceso universal a la información y el conocimiento (Dunn Cavelty & Brunner, 2007, pág. 6; Schwartz, 1996; Yang, 2009; Wu T. , 2011; Bi, 2018). Sin embargo, esta visión se ha encontrado con gran resistencia casi tan pronto como apareció (Dunn Cavelty & Brunner, 2007, pág. 5). Según uno de los principales teóricos de la sociedad de la información, Frank Webster (1997), este enfoque tecnológicamente determinista es sólo una de las cinco posibles definiciones analíticas de esta llamada "revolución de la información" (Dunn Cavelty & Brunner, 2007).[58]

Según algunas críticas como Myriam Dunn Cavelty y Elgin Brunner (2007, pág. 6), aquellos que exaltan las muchas virtudes de Internet, parecen olvidar que el entorno cibernético está completamente formado por seres humanos y, “por sí solo

[57] La neutralidad de la red (*network neutrality*) significa que los proveedores de Internet no deben discriminar ni restringir el acceso de los usuarios a las aplicaciones o el contenido. La política de neutralidad de la red exige a los proveedores de servicios de Internet (ISP), ofrecer un acceso equitativo a todo el contenido web. Además, prohíbe a los ISP cobrar discrecionalmente a los clientes según el contenido, sitios web, aplicaciones o métodos de comunicación utilizados. El principio básico era mantener internet libre y abierto, protegiendo el derecho de una persona a compartir y acceder a contenido en línea sin interferencias. No obstante, dentro de los Estados Unidos la Comisión Federal de Comunicaciones (FCC) votó para derogar la neutralidad de la red el 14 de diciembre de 2017 (Bi, 2018). Sin embargo, esta cláusula de no discriminación continúa en el centro de los debates sobre la gestión y el control del campo cibernético.

[58] Las otras que identifica son económica, espacial, cultural y ocupacional.

no es más que un recipiente, o un medio de distribución de contenido".[59] Por un lado, hay autores como Niall Ferguson que recalcan que este optimismo sobre la hiper-conectividad, permitido por la expansión de las redes sociales digitales no conduce necesariamente a la ecualización social (Ferguson, 2017). Por ejemplo, con base en la teoría de redes, Ferguson (2017) explica que "los miembros individuales de una red social son simples nodos conectados mediante lazos. Sin embargo, no todos los nodos o lazos en una red social son iguales. Por lo general, ciertos nodos y lazos son más importantes que otros".

Por un lado, incluso el mismo término de "revolución de la información" es algo exagerado y debe analizarse y utilizarse con sumo cuidado. Por ejemplo, para las académicas Myriam Dunn Cavelty y Elgin Brunner, "el concepto de revolución, debe suplirse, puesto que, revolución generalmente designa un cambio repentino, radical o completo" (2007, pág. 2), situación que para ellas aún no se ha presentado. Estas autoras mencionan que "el término 'evolución' parece mucho más apropiado para describir mejor el ajuste gradual y la no linealidad del desarrollo científico-tecnológico" (Dunn Cavelty & Brunner, 2007, pág. 3).

Por otro lado, observadores como Thomas Rid, Andrew L. Shapiro y Niall Ferguson son aún más escépticos sobre el impacto económico y social de las tecnologías de la información, el cual califican de 'limitado' (Shapiro A. L., 1999a; Rid, 2012; Ferguson, 2017), puesto que, el acceso a las tecnologías de la información es desigual, las formas de acceso varían entre sociedades altamente industrializadas y aquellas que no lo son, y las actualizaciones tecnológicas llegan de manera vertical entre distintas sociedades nacionales, algo que se ha denominado como brecha digital o *digital divide* (Norris, 2001).

De modo similar, otros analistas enfatizan las implicaciones 'negativas' de la llamada "revolución de la información" y señalan los múltiples peligros y amenazas que conlleva la aplicación de las nuevas tecnologías a todo el espectro de la actividad social, es por ello que se les ha llamado 'ciberpesimistas' (Mueller M. L., 2010; Clarke & Knake, 2010) (Dunn Cavelty & Brunner, 2007, pág. 6). Por ejemplo,

[59] Puede verse el esquema del capítulo 1 que describe los cuatro sistemas que componen el ciberespacio, en el cual el sistema social es un elemento de estos.

David Rothkopf (1999) señala diversas consecuencias potencialmente desastrosas en un mundo económicamente globalizado que denomina como “prácticas de desinformación”. De la misma manera, hay autores que mencionan que Internet no es por sí mismo un factor democratizador o que incluso la tecnología puede causar el efecto contrario, algo similar a una “revolución de control” (Shapiro A. L., 1999a). Dentro de este orden de idas, algunos estudiosos subrayan que la sobrecarga informativa amenaza la habilidad social para adquirir conocimientos y que debilita la cohesión social (Shenk, 1997).

Por consiguiente, algunos expertos como Brandon Valeriano y Ryan C. Maness recalcan que esto conduce a establecer la incertidumbre como el factor dominante en el sistema internacional *cibernético* (Valeriano & Maness, 2015, pág. 1). Con base en esto, se aduce que el perjuicio es un factor constante en la vida internacional, y que cualquier cosa es un peligro para todo, y todo puede dañar a la mayoría (Valeriano & Maness, 2015, pág. 1). Es por ello que, con la emergencia de una sociedad digital y una creciente interconectividad, algunas voces como las de Richard A. Clarke y Robert Knake arguyen que “la humanidad debe preocuparse por la vulnerabilidad que estas interconexiones traen consigo” (Clarke & Knake, 2010).

Por otro lado, académicos como Saskia Sassen (1998) y Henry H. Perritt (1998) señalaron en su momento, cómo la comercialización de internet podría amenazar su potencial democrático como resultado del crecimiento de redes digitales privadas. Tanto pronto como Internet se reconoció como una forma extraordinariamente importante de comunicación en red, con numerosas aplicaciones posibles, el deseo de las empresas de comercializar Internet creció de forma exponencial (Castells, 2009, pág. 150). En este periodo, comenzó a tener lugar la introducción de derechos de autor (*copyrights*) y *firewalls* (cortafuegos), y otras apropiaciones privadas de Internet como espacio público (Palfrey, 2010) (Nagelhus Schia & Gjesvik, 2018a) (Deibert & Rohozinsky, 2010). Para algunos como Michéle Flournoy y Michael Sulmeyer, esto solamente demuestra que “el ciberespacio no es simplemente parte de los bienes comunes globales, puesto que, Estados y compañías privadas afirman su jurisdicción sobre la infraestructura física

que compone Internet y los datos que la atraviesan" (Flournoy & Sulmeyer, 2018, pág. 40).

En este sentido, se puede comprender lo que algunos observadores identifican como una tendencia hacia la convergencia entre las tecnologías militares y civiles, lo que lleva a la militarización de la sociedad en general y del ciberespacio en particular, convirtiendo cada conflicto en una 'guerra de información' (Krutskikh, 1999, pág. 32) (Deibert & Rohozinsky, 2010) (Sierra Caballero, 2003) (Harris S. , 2014). Por consiguiente, las distinciones en jurisdicción, competencias y deberes que solían pertenecer a diferentes segmentos gubernamentales se han difuminado en el terreno digital (Eriksson & Giacomello, 2006). Esto puede verse como "la civilización de lo militar o la militarización de lo civil" (Eriksson & Giacomello, 2006, pág. 231).

Con base en esto, la preocupación por el mantenimiento de una "frontera electrónica libre", "la fragmentación de Internet" o sobre el fin de "la era del internet abierto" se ha está posicionando como un tema prioritario en la agenda internacional (Schneier B. , 2012; Adee, 2019). De allí pues que, la opinión pública y los ciudadanos perciban que la participación e intervención del gobierno, o de los principales operadores de la internet, amenazan principios básicos como la apertura, la libertad y la privacidad.[60]

De acuerdo con Nazli Choucri (2012, pág. 148), "para algunos estrategas militares, el uso militar del ciberespacio es una extensión natural del despliegue de tecnologías de información avanzadas, junto con la expansión necesaria de las capacidades institucionales y organizativas". Dentro de esta perspectiva, Ronald Deibert y Janet Gross Stein (2003) refieren este proceso de la militarización del ciberespacio como una extensión 'silenciosa' de la política de defensa. Para algunos analistas, el mundo digital o virtual es un dominio en el que las agencias de inteligencia de algunos gobiernos están ejerciendo un enérgico control en el terreno y, que los servicios de inteligencia no sólo utilizan la información para detectar y detener amenazas a su seguridad nacional, sino también para: *a)* obtener ventajas

[60] Este señalamiento se basa en los estudios realizados por autores como Robert Deibert et al (2008, 2010), Siva Vaidhyanathan (2018), Susan Perry y Claudia Roda (2017).

comerciales en nichos de oportunidad a través del espionaje industrial, comercial y económico, y *b)* poseer medios de presión política y militar (Arreola García, 2015, pág. 9; Palfrey, 2010) (Stokes, 2015a)

No obstante, tampoco puede decirse que la integración de lo civil y lo militar sea un fenómeno nuevo. Para algunos autores, la única novedad es "la centralidad de los sistemas de control y comunicaciones para la política de defensa" (Sierra Caballero, 2003, pág. 258). Por ello, muchos aspectos de las llamadas guerras modernas están conformados por nuevas doctrinas que buscan llevar a cabo las llamadas "operaciones de información", con importantes implicaciones para los asuntos militares, la política y la sociedad en general (Dunn Cavelty & Brunner, 2007, pág. 10).[61] En atención a lo expuesto, para algunos académicos, esto es preocupante, ya que "las operaciones cibernéticas y las acciones retóricas han creado una estructura digital en la cual los miedos exagerados sobre la parálisis de la infraestructura digital y las crecientes preocupaciones sobre la ventaja competitiva exacerban el espiral de desconfianza en lo cibernético" (Lindsay J. R., 2015a, pág. 8).

De ahí que, dada la naturaleza única del campo de batalla en línea, la relevancia de esta tendencia se extiende más allá de las operaciones militares, ya que es probable que los civiles puedan llegar a sufrir daños colaterales importantes por los ataques dirigidos a los Estados (Flournoy & Sulmeyer, 2018, pág. 43). No obstante, para la experta Myriam Dunn Cavelty (2007, págs. 21-22) dos puntos son de hecho nuevos, en el sentido de que no tienen precedentes: *1)* la tecnología que alimenta la actual revolución de la información es nueva; *2)* la alta dependencia que la sociedad tiene en la tecnología también lo es.

Si bien es cierto que, las fuerzas convencionales y los presupuestos militares se han reducido en general después del final de la guerra fría, el nuevo énfasis en la seguridad de la información y las amenazas cibernéticas es una excepción notable. En América del Norte, Europa, Rusia, China y otras partes del mundo, los gobiernos están estableciendo nuevas unidades y empleando personal para

[61] Un *incidente cibernético* es una acción aislada lanzada contra un Estado que dura sólo una cuestión de horas, días o semanas, mientras que una *disputa cibernética* es una operación a largo plazo, que puede contener varios incidentes (Valeriano y Maness, 2015, pág. 8).

monitorear, analizar y contrarrestar los riesgos y amenazas percibidos en el ciberespacio (Klimburg, 2017; Harris S. , 2014), lo que queda como interrogante es si estos esfuerzos representan una solución viable o son contraproducentes con sus objetivos planteados.

3.4 La ciberseguridad: su impacto en las prácticas y narrativas estatales

Las operaciones cibernéticas y las acciones retóricas han creado una estructura digital en la cual los miedos exagerados comienzan a tener mayor ahínco (Lindsay J. R., 2015a, pág. 8). Para algunos autores, los desafíos y la confusión en el tema de la ciberseguridad son particularmente agudos para el caso de China y Estados Unidos de América, las cuales tienen unas de las economías electrónicas de mayor crecimiento, así como uno de los programas más activos sobre operaciones de seguridad cibernética (Lindsay J. R., 2015a). Para una mayor lucidez empírica, estas variables se revisarán con mayor detalle en la última sección de este capítulo y en los subsiguientes apartados de la investigación.

En efecto, la importancia del conocimiento y la información como fuente de riqueza ha llevado a la idea de que el futuro podría pertenecer a "Estados virtuales" que tienen poco poder militar y recursos naturales, pero que están altamente capacitados en el uso de recursos administrativos, herramientas financieras y creativas para administrar activos digitales en otras partes del mundo (Dunn Cavelty & Brunner, 2007, pág. 9) (Rosecrance, 1999, pág. 4). En consecuencia, tal razonamiento implica que "el país que mejor pueda liderar la *revolución de la información* será más poderoso que cualquier otro" (Nye & Owens, 1996, pág. 20).

Sobre el asunto, el aspecto más notable de esta idea es la noción de que, en última instancia, estas entidades competirán por los recursos de información. En este tenor, Miryam Dunn Cavelty y Elgin Brunner recalcan que “las naciones desarrolladas ya no lucharán por el dominio político, sino por su participación en la producción de información global” (2007, pág. 10). Por su parte, Jeffrey Hart y Singbae Kim (2000) analizan la revolución de la información como parte de un

desarrollo tecnológico perpetuo y, por lo tanto, identifican un vínculo creciente entre el poder tecnológico y el poder informativo, que denominan "cornisa tecnológica" (*technoledge*) (Dunn Cavelty & Brunner, 2007, pág. 8). Este concepto, Jeffrey Hart y Singbae Kim argumentan, constituye un cambio cualitativo (Hart & Kim, 2000). Este cambio cualitativo podría deberse al hecho de que, por un lado, "la información en todas partes se ve y se utiliza como un recurso estratégico del Estado", mientras que, por otro lado, simultáneamente, “la información se está convirtiendo en un objeto producido y de consumo masivo en todas partes”, “que en muchas ocasiones desafía la autoridad gubernamental” (Dunn Cavelty & Brunner, 2007, pág. 8) (Chernov, 2004, pág. 6).

Con respecto a si la revolución de la información representa o no un desafío para la función y el estatuto del Estado como actor principal, el debate y la discusión entre los estudiosos se ha tornado cada vez más complejo (Rothkopf, 1998; Kello, 2013; Goldsmith & Wu, 2006). Por ejemplo, una opinión dentro del espectro es que las ‘villas globales’ y los actores no territoriales harán que el Estado-nación quede obsoleto por completo (Toffler & Toffler, 1993; Mattelart, 2007). Sin embargo, para algunos académicos, los agentes tradicionales de las Relaciones Internacionales (a saber, los Estados) parecen ser los actores cibernéticos más dominantes porque cuentan con recursos materiales, capacidades humanas y financieras para llevar a cabo acciones cibernéticas masivas y de gran alcance (Valeriano & Maness, 2015, pág. 25; Lindsay J. , 2013).

Sobre el asunto, Brandon Valeriano y Ryan C. Maness opinan que, actualmente, la arena del ciberespacio es la principal zona de conflicto internacional (Valeriano & Maness, 2015; Wu T. , 2011; Toca, 2019). De ahí que, Lene Hansen y Helen Nissenbaum subrayen que es a través de este prisma que una parte de la comunidad de asuntos internacionales está abordando el desarrollo tecnológico y lo hace con trepidación y desconfianza (Hansen & Nissenbaum, 2009). Como bien lo apuntan Brando Valeriano y Ryan C. Maness (2015, pág. 25) “el enfoque dominante en el ciberespacio es la conformación de un proceso de construcción de la amenaza cimentado en el miedo”.

En virtud de esto, algunos académicos como Nazli Choucri, mencionan que, “a pesar de las diferencias en el acceso cibernético y en los usos del ciberespacio, existe una considerable creatividad en la manipulación de este nuevo espacio con fines políticos” (Choucri, 2012, pág. 126). Por ello, no sólo existe el temor de que los flujos de información no regulados puedan comprometer objetivos políticos, sino que también existe la preocupación de que la información, como propaganda o imperialismo cultural, no puede ser restringida. (Krishna-Hensel, 2007, pág. xi; Vaidhyanathan, 2018). Es por eso que, muchos gobiernos comparten el temor de que su capacidad para influir y gobernar a sus poblaciones se vea socavada por un libre flujo de información (Deibert, Palfrrey, Rohozinski, & Zittrain, 2008; Austin, 2018).

Por consiguiente, existen análisis que argumentan que esta puede ser una causa de la hipérbole que rodea a la idea del desarrollo de arsenales cibernéticos (*cyber weaponry*), e incluso, subrayan que “el paso siguiente para las interacciones cibernéticas internacionales podría ser muy similar a una perspectiva ‘hobbesiana’” (Valeriano & Maness, 2015, pág. 26; Krebs, 2014). A medida que las naciones reconocen su creciente dependencia de las infraestructuras tecnológicas, la responsabilidad de salvaguardar la Protección de Infraestructura de Información Crítica (*Critical Information Infrastructure Protection*, CIIP, por sus siglas en inglés) y el papel de los flujos informativos se han convertido en un componente importante de las políticas de seguridad nacional en muchos países (Krishna-Hensel, 2007, pág. xii; Sanger, Barnes, Zhong, & Santora, 2019).

Como consecuencia, la percepción común es que “las sociedades y gobiernos al ser más dependientes con respecto a la tecnología de la información, también son más vulnerables a todo tipo de amenazas cibernéticas” (Eriksson & Giacomello, 2006, pág. 226; Segal A. , 2016). Típicamente las amenazas cibernéticas involucran una muy amplia gama de adversarios y objetivos, incluyendo tanto a los actores estatales como a los no estatales (Eriksson & Giacomello, 2006, pág. 226; Valeriano & Maness, 2015) [Ver tabla 3.4]. Por ende, algunos gobiernos y gobernantes consideran seriamente el supuesto que “los grupos terroristas podrían realizar más acciones con un teclado que con una bomba” (Denning D. E.,

2001, pág. 282) (Bendrath, 2003).[62] De modo que, con frecuencia, se realicen advertencias sobre las consecuencias de aplicar las nuevas tecnologías de la información y la comunicación al ámbito militar. Algunos expertos generalmente refutan la noción de que la 'guerra de información' es menos violenta que los conflictos convencionales, puesto que para algunos es "una percepción errónea y peligrosa que se ve agravada por una confusión entre los límites de los entornos civiles y militares" (Dunn Cavelty & Brunner, 2007, pág. 7).

En general, la actividad cibernética se correlaciona con el poder, la tecnología o los recursos y la capacidad de los actores para utilizar estos elementos. En otras palabras, estas tácticas son parte de una función más amplia de disputas activas de política exterior entre los actores estatales y no estatales (Valeriano & Maness, 2015, pág. 9) (Kramer, Starr, Wentz, & (eds.), 2009). Por su parte, Ronald Deibert y Janet Gross Stein (2003) han referido a este proceso como "la militarización del ciberespacio", una extensión 'silenciosa' de la política de defensa. Por otro lado, para otros expertos, el creciente miedo al combate cibernético y el auge del discurso de las amenazas cibernéticas ha provocado una reorientación de los asuntos político-militares y económicos a nivel global (Valeriano & Maness, 2015, pág. 6). Por lo tanto, el problema correspondiente es que el debate sobre la naturaleza del conflicto cibernético a menudo está encabezado por empresas de seguridad de Internet y gobiernos que velan por sus propios intereses y que se benefician de la inflación de la amenaza cibernética (Klimburg, 2017).

En efecto, el enmarcado extensamente reconocido de las amenazas cibernéticas implica que los límites entre lo internacional, lo doméstico, entre las esferas civil o militar, lo público y lo privado y entre la guerra y la paz se difuminen. Si esto es tomado en serio, este enmarcado sugiere que no sólo la seguridad de los sistemas de información es desafiada, sino también, y fundamentalmente, la capacidad de acción y coordinación de los agentes sociales, económicos y políticos a nivel global (Eriksson & Giacomello, 2006, pág. 227) (Fountain, 2001) (Everard, 2000) (Rosecrance, 1999) (Giacomello, 2005).

[62] Esta afirmación puede rastrearse hasta 1990 en un reporte hecho por la Academia Nacional de Ciencias de los Estados Unidos, a través del *Computer Science and Telecommunications Board*.

3.5 Percepciones divergentes sobre la ciberseguridad en las grandes potencias

De acuerdo con el analista James Andrew Lewis, del centro de investigación *Center for Strategic & International Studies* (CSIS), “el vínculo entre tecnología, innovación, seguridad nacional y poder internacional ahora es ampliamente reconocido” (Lewis, 2018). Es por esta razón, que “los líderes políticos reconocen que la capacidad de innovar es una pujante fuente de poder nacional” (Lewis, 2018). En resumen, Lewis abrevia que “en la era digital, la seguridad nacional y el poder nacional tienen diferentes requisitos en función del cambio tecnológico y el ciberespacio” (Lewis, 2018).

De igual manera, algunos analistas del MIT (*Massachusetts Institute of Technology*) han identificado y analizado que el ciberespacio y las relaciones internacionales están formando un sistema socio-técnico integrado que han llamado Sistema de Relaciones Internacionales Cibernético (*Cyber-IR System*) (Vaishnav, Choucri, & Clark, 2013). Dentro de este orden de ideas, Chintan Vaishnav, Nazli Choucri y David Clark buscan delinear cuáles son los actores y funciones centrales de este sistema, qué dinámicas se presentan y cómo se dan las interacciones dentro de este esquema. Es por ello que, dada su importancia para la política, la seguridad internacional y el crecimiento económico, las tecnologías e infraestructuras digitales se han convertido en factores clave en la relación entre potencias, principalmente entre los Estados Unidos y la República Popular de China (Lewis, 2018).

De este modo, dentro de la literatura, existe una vertiente que dramatiza los resultados de un cataclismo cibernético entre potencias, haciendo alusión a la posibilidad de escenarios hipotéticos que resultan en un trastorno masivo de las infraestructuras críticas, lo que conduce a serias pérdidas económicas, caos social o el colapso de la civilización humana. Dentro de estos recuentos, se han utilizado metáforas como: ‘Pearl Harbor electrónico’, ‘Hiroshima electrónico’, ‘9/11 digital’ o una ‘pandemia cibernética’ o un escenario cibernético fatal (*cyber-doom*) (Bendrath, 2003) (Shcwartau, 1996) (Everard, 2000) (O'Day, A., 2004) (Lawson S. , 2013). En esta visión, la infraestructura general sería interrumpida o trastornada a tal punto

que sociedad y gobiernos no tendrían la habilidad de funcionar normalmente (Eriksson & Giacomello, 2006); aunque teóricamente es posible, para algunos estudiosos la presentación de este tipo de escenarios es altamente improbable (Lawson, Yeo, Yu, & Greene, 2016, pág. 67).

No obstante, las nociones de la amenaza cibernética se han originado tanto en la esfera pública como privada, en actores civiles y militares (Eriksson & Giacomello, 2006, pág. 225). Es cierto que la acción cibernética generalmente es identificable, pero para determinar la procedencia, y la atribución de la acción desde la fuente es un proceso más complejo (Singer & Friedman, 2014). Sin embargo, para autores como Thomas Rid, los ataques cibernéticos pasados y presentes son meramente versiones sofisticadas de tres actividades que son tan antiguas como la guerra misma: *subversión*, *espionaje* y *sabotaje* (Rid, 2012, pág. 6).

Dentro de la comunidad de expertos de computación, técnicos informáticos y operadores de redes computaciones el énfasis se ha puesto en las vulnerabilidades estructurales o en conflictos de software que conducen al colapso de los sistemas (Eriksson & Giacomello, 2006, pág. 226). Como bien subrayan Lene Hansen y Helen Nissenbaum, “las amenazas a la ciberseguridad no sólo surgen de *agentes intencionales*, sino también se generan de *cuestiones sistémicas*” (Hansen & Nissenbaum, 2009: 1160). Ciertamente, lo que queda de manifiesto es que, las amenazas cibernéticas, reales o no, han recibido una importancia indiscutible en el pensamiento de seguridad de la posguerra fría.

Se aprecia claramente una competencia por el liderazgo tecnológico, un punto que se ha vuelto neurálgico en la relación sino-estadounidense. Ambos países temen que las tecnologías obtenidas en diferentes puntos de sus cadenas de suministro, ampliamente interconectadas, se vean corrompidas y puedan ser aprovechadas por otros de formas perjudiciales (Cheung, 2009). Justamente, en una estrategia agresiva por parte del gobierno estadounidense, se ha acusado a diversas empresas de origen chino de conducir actividades de ciberespionaje para beneficio industrial y para apoyar estratégicamente al gobierno de Beijing (Yuan, 2018; Sanger, Barnes, Zhong, & Santora, 2019).

Durante una buena parte del gobierno de Barack Obama, la ciberseguridad se convirtió en un punto delicado de la relación bilateral. En este período, los medios estadounidenses se centraron en representar lo que consideraban una posible guerra cibernética entre Estados Unidos y la República Popular de China, y en la amenaza que representaba la actividad informática maliciosa proveniente de China (Gady, 2016; Lu C. , 2017). Las principales diferencias entre los dos países son sus valoraciones sobre el concepto ciberseguridad, la forma de conducir la gobernanza en el ciberespacio y lo que se considera un uso de la fuerza indebido en este terreno (Li Z. , 2016; Gady, 2016), cuestiones que serán retomadas en el sexto capítulo.

Por un lado, las estimaciones chinas sobre ciberseguridad se reflejan en la idea de una comunidad de ciberespacio de destino común, cuyo núcleo se basa en el respeto a la soberanía cibernética de cada nación y la necesidad de establecer directrices para el ciberespacio mediante una amplia cooperación intergubernamental. Por otro lado, la valoración estadounidense de ciberseguridad se basa en poner a Estados Unidos en primer lugar (*America First*), lo que significa que sus intereses nacionales están por encima de los intereses nacionales de otros países, y que sus ventajas tecnológicas no deben ser cuestionadas por otros países (Li Z. , 2016).

En cuanto, la gobernanza del ciberespacio, el gobierno estadounidense prefiere un enfoque de múltiples partes interesadas (*multi-stakeholder*), por su parte, el gobierno chino se inclina por un enfoque multilateral centrado en el Estado (*cyber-sovereignty*) (Gady, 2016). Por último, en relación con el uso de la fuerza en el ciberespacio, China se interesa en mantener una definición laxa y amplia, para que no se pueda establecer una norma internacional para favorecer las represalias contra los ataques cibernéticos, lo que dificulta que los Estados Unidos y sus aliados presenten una respuesta común a las actividades cibernéticas maliciosas patrocinadas por los Estados (Gady, 2016)

En el siguiente cuadro, se brinda una lista de términos que ayudan a la comprensión del fenómeno de la ciberseguridad, que en ocasiones se utilizan de forma intercambiable, pero que significan cuestiones nítidamente distintas. En los siguientes capítulos se presentan las concepciones que los gobiernos de la

República Popular de China y de Estados Unidos de América tienen sobre estos conceptos, y que se traducen en sus aproximaciones, tácticas y estrategias sobre el ciberespacio.

Tabla 3.5 Términos clave para entender la ciberseguridad

Inglés	**Chino**	**Español**
information space	信息空间 *xinxi kongjian*	espacio de información
infomation warfare	信息战争 *xinxi zhanzheng*	guerra de información
information weapon	信息武器 *xinxi wuqi*	arma de información
information security	信息安全 *xinxi anquan*	seguridad de la información
cyber warfare	网络战争 *wangluo zhanzheng*	guerra cibernética o ciberguerra
cyberpace	网络空间 *wangluo kongjian*	ciberespacio
network warfare	网络战 *wangluo zhan*	guerra de redes
cyber weaponry	网络武器 *wangluo wuqi*	arsenal cibernético
cybersecurity	网络安全 *wangluo anquan*	seguridad cibernética o ciberseguridad
cyber crime	网络犯罪 *wangluo fanzui*	crimen cibernético
cyberterrorism	网络恐怖主义 *wangluo kongbuzhuyi*	terrorismo cibernético

Fuente: elaboración propia

Sin embargo, ninguno de los dos países desea ver la estabilidad del ciberespacio interrumpida por el terrorismo, las organizaciones criminales o que las nuevas tecnologías están fuera de su control, a su vez, ninguno tolera algún tipo comportamiento digital que interfiera con sus objetivos. Para ello, en los dos siguientes capítulos, se muestran cómo enfrenta cada uno los desafíos planteadas por las actividades cibernéticas maliciosas, cuál es el enfoque que utilizan para resolver las situaciones de riesgo, qué organizaciones e instituciones participan en la elaboración de la política de ciberseguridad, y cuáles son las narrativas que utilizan para justificar sus acciones en el ciberespacio.

Capítulo 4. Origen y evolución de las estrategias chinas de seguridad sobre el espacio digital

Introducción

La idea central de este capítulo es analizar profusamente el tema de la ciberseguridad como eje toral en las políticas internas y externas chinas y su efecto sobre su conducta internacional cibernética, esto con el objeto de verificar o falsear la hipótesis central de este trabajo de investigación. Ciertamente, el ciberespacio cumple una función importante en los continuos esfuerzos de desarrollo y de innovación tecnológica-científica de la República Popular de China. A través de esta área, se interconectan infraestructuras básicas como energía eléctrica, telecomunicaciones, transporte, suministro de agua, asimismo, provee servicios en sectores como finanzas, educación, trámites gubernamentales, ayuda en desastres naturales, entre otros, conocidos también como "infraestructura crítica de la información".

Asimismo, el desarrollo de Internet en la República Popular de China ha sido rápido y completo, no únicamente en términos de cantidad de usuarios y recursos de información en red, sino también en términos de desarrollo industrial e inversión extranjera. Como resultado, la Internet ha traído grandes cambios a la sociedad china, en general. Ha aumentado el acceso a la información y el fortalecimiento de la comunicación, no obstante, junto con la promesa del desarrollo, se han derivado posibilidades de riesgo inherentes en el ciberespacio. Para algunos analistas chinos como Li Yuxiao y Xu Lu,[63] junto con estos beneficios indiscutibles que brinda el rápido desarrollo de Internet, "la ciberseguridad se ha convertido en un desafío desalentador" (Li & Xu, 2015, págs. 226-227). Por ejemplo, algunos medios oficiales como Xinhua han informado que, en la última década, el número de ciberataques en computadoras y sitios web chinos ha aumentado en más del 80 por ciento. De la misma manera, mencionan que el 20 por ciento de la actividad maliciosa en el

[63] Li Yuxiao es el decano de la Facultad de Telecomunicaciones de la Universidad de Beijing. Asimismo, dirige el Centro de Investigación sobre Derecho y Gobernanza de Internet. Xu Lu es investigadora de la Facultad de Telecomunicaciones de la Universidad de Beijing.

ciberespacio a nivel global se origina en IP provenientes de China (Symantec, 2018). Además, resaltan que la escalada del problema ha llegado a tal punto, que, para principios del 2017, el gobierno chino arrestó a 19,000 personas por fraude cibernético o con crímenes relacionados a las telecomunicaciones (Xinhua, 2017c). En efecto, como se mencionó anteriormente, “tanto la promesa como el peligro son posibilidades que derivan de la función de ubicuidad del ciberespacio” (Eriksson & Giacomello, 2006). Además, la *ciberseguridad* está conformada por la interacción estratégica de muchos actores con características diferentes y desafía cualquier interpretación simple (Lindsay J. R., Introduction, 2015b, pág. 6).

En el caso de la República Popular de China un conjunto grande de actores tiene intereses muy diferentes y perspectivas diversas sobre cómo se debe ejecutar la política de ciberseguridad (Finnemore M. , 2011).Por tanto, toda esta diversidad crea enredos de coordinación, de ejecución política y de compromiso de acción, así como problemas de acción colectiva. A su vez, la complejidad de las relaciones intra-gubernamentales e intergubernamentales en cualquier nación complica los esfuerzos para definir y hacer cumplir la política de seguridad cibernética (Raud, 2016) (Finnemore M. , 2011) (Lindsay J. R., 2015b, pág. 7).

Por su parte, el gobierno chino ha desarrollado una nueva comprensión de la importancia de la ciberseguridad y ha comenzado a acelerar el desarrollo de políticas y normas en este ámbito (Li & Xu, 2015, pág. 229). Por ello, comprender la estructura, la organización, las normas y prácticas que dan forma a la arquitectura cibernética de la República Popular de China no es una tarea sencilla. Es por eso que, la razón de este capítulo es mostrar cuáles son las iniciativas chinas en materia de ciberseguridad que dan forma a un enfoque particularmente distintivo a nivel global.

En razón de ello, se presenta la función otorgada al ciberespacio por parte de los dirigentes de la República Popular de China, cómo se ha estudiado el fenómeno de la ciberseguridad para este sujeto de estudio y en qué parte de la discusión se encuentra este trabajo de investigación. Después, se muestra la estructura institucional que se encarga de perfilar y delinear las acciones en materia de ciberseguridad al interior de China, cómo estructuran dicha política y qué

mecanismos emplean para llevarla a cabo. Con base en esto, se presentan las principales iniciativas gubernamentales chinas en materia de ciberseguridad, basadas en la interpretación y perspectivas que tienen sobre el papel que juega ésta en el desarrollo tecnológico, presentado en la última división de este capítulo.

Para efectos de esta investigación se realiza una revisión de la mayor cantidad de información abierta sobre el tema, así como en opiniones de especialistas reconocidos en el tema, a través de una comprobación cruzada de datos sensibles para corroborar su veracidad y autenticidad. Asimismo, se busca que este capítulo sirva como la primera parte del ejercicio de comparación entre dos esquemas de participación estatal en la seguridad del ciberespacio.

4.1 El estudio de la ciberseguridad en China

En la literatura especializada sobre ciberseguridad, existe un número limitado de títulos que aborden profundamente y de forma holística a China como caso de estudio (Lindsay, Cheung, & Reveron, 2015) (Austin, 2014) (Inkster, 2013) (Austin, 2018).[64] Esto puede ser producto de la siguiente cuestión: en el origen de las prácticas sobre ciberseguridad, la República Popular de China estaba escasamente conectada y era una economía digital en ciernes, por ello no se veía como un problema de gran magnitud o un ejemplo paradigmático.

Al hacer una revisión extensiva mas no exhaustiva del estado del arte, se puede inferir que los diversos estudios que han abordado el problema únicamente se abocan a un aspecto del fenómeno. Por ejemplo, los estudios relativos a la modernización militar china a menudo discuten la interpretación china del "conflicto cibernético" o la "guerra cibernética" (Feigenbaum, 2003) (Goldman & Mahnken, 2004) (Cheung, 2009) (Ventre, 2014) (Cheng D. , 2017), pero generalmente tienen poco que decir sobre la política de ciberseguridad civil o la integración de mecanismos civiles-militares en la República Popular de China que atañen a dicha

[64] Debo en gran medida estas observaciones al trabajo coordinado por Jon R. Lindsay, Tai Ming Cheung y Derek S. Reveron publicado en su libro *China and Cybersecurity*.

política, a pesar de que la mayoría de la tecnología relevante es creada y utilizada por civiles (Lindsay, 2015).

Por un lado, algunos trabajos han sido directamente financiados por el gobierno de los Estados Unidos para esbozar cuál es la perspectiva de China sobre el conflicto de información (*information warfare*) o las llamadas operaciones de información (Lindsay J. R., 2015b, pág. 5) (Thomas, 2009) (Kamphausen, Li, & Scobell, 2009) (Spade & Caton, 2012). Cabe destacar que, estos tienen un objetivo claro, conocer el desarrollo militar chino y las actualizaciones en sus capacidades, incluidas aquellas en el ciberespacio, por ende, su planteamiento en relación con otras cuestiones cibernéticas es poco profuso.

Por otro lado, en el terreno de los estudios de China, los análisis abordan primordialmente la participación digital y el papel de los medios de comunicación en la conformación del entorno político china. Algunas investigaciones sobre los efectos de los nuevos medios y el desarrollo tecnológico tienden a centrarse en la capacidad o incapacidad de la sociedad y el gobierno chino para promover la democracia y la sociedad civil (Shirk, 2010) (Yang, 2009) (Zhao, 2008). Asimismo, otras investigaciones abordan el alcance de la censura estatal, los esfuerzos de control gubernamental y los mecanismos sociales que buscan romper dicho control, pero pocos indagan sobre el tema de ciberseguridad y las políticas gubernamentales de seguridad cibernética, y si así lo hacen, lo realizan de manera tangencial (Young, 2012; Fu, 2017; Han, 2018; Roberts, 2018).

Por ello, se hace necesario realizar un esfuerzo intelectual por construir una visión holística del tratamiento de la ciberseguridad en China. A pesar de esta sugerencia e identificación de un problema epistemológico, no es la pretensión de esta investigación llenar este vacío, pues, este trabajo se enfoca principalmente en las acciones, conductas y percepciones que tienen los agentes estatales en el ámbito de la ciberseguridad, pero sin olvidar que interactúa con otras entidades y opera en diversos niveles para diseñar, implementar y ejecutar políticas para una cuestión multifacética, multinivel y compleja.

4.2 Instituciones, estructura y organización encargadas de la ejecución de la política de ciberseguridad en China

En virtud de comprender y analizar la estructura, estrategias y organización cibernéticas de China no es una tarea fácil (Raud, 2016). Cabe resaltar que, los procesos institucionales gubernamentales y los procedimientos de la toma de decisiones siguen siendo un rompecabezas para cualquier análisis (Shambaugh, 2013, pág. 61). En gran medida, esto se debe a que el esquema gubernamental chino no permite la desclasificación de documentos oficiales recientes, a las pocas aportaciones de funcionarios retirados y la secrecía de los empleados estatales en funciones (Shambaugh D. , 2013, pág. 61). Además, en muchas ocasiones, para los observadores externos, las jerarquías complejas, las estructuras de mando y los diversos documentos suelen ser confusos (Raud, 2016).

A pesar de ello, análisis sumamente detallados se han publicado para esclarecer el proceso de la toma de decisiones políticas en la República Popular de China (Barnett, 1985; Swaine M. D., 1996; Lu N. , 2000; Lampton D. M., 2001; Hao & Su, 2005; Lai, 2010). Sin embargo, no es propósito de este trabajo ahondar en dicha cuestión, sólo se pretende dar un poco de luz sobre el efecto que tiene la ciberseguridad en las consideraciones y en la dinámica de la política pública en la República Popular de China. Y aunque, las políticas sobre el ciberespacio durante un tiempo fueron fragmentarias e incoherentes, se han vuelto más uniformes y controladas desde la cúspide del poder político chino (Nagelhus Schia & Gjesvik, 2018a). Además, como recalcan algunos especialistas “la regulación de contenido e infraestructura doméstica de Internet en China a menudo ha dejado a los occidentales, e incluso a sus propios ciudadanos, confundidos y desconcertados con respecto a los procedimientos y el contenido que podrían considerarse inadecuados para los usuarios de Internet” (Burgman, 2016).

No obstante, en términos de estructuras formales, la República Popular de China no cuenta con un solo mecanismo para la formulación, ejecución e implementación de la política de ciberseguridad. Esclarecer este proceso requiere delinear de manera breve cuáles entidades están involucradas en el desarrollo de ésta. Antes de iniciar, cabe subrayar que existen dos sistemas de gobernabilidad en

China, las instituciones del partido y las del Estado. Ambas están íntimamente entrelazadas, razón por la cual se le observa como un esquema gubernamental partido-Estado. Es decir, el sistema de partido se le conoce como el "sistema de asuntos del partido" (*dangwu xitong*, 党务系统), y el sistema estatal es llamado el "sistema de asuntos del estado" (*zhengwu xitong* 政务系统) (Zheng & Wen, 2016, pág. 33).[65] En otras palabras, la relación de estos dos sistemas constituye la infraestructura institucional más importante de la organización política formal de China, sin embargo, en la práctica, el Partido Comunista de China (PCCh) está inequívocamente a cargo en todos los niveles, y el aparato estatal simplemente ejecuta las directivas del partido (Cheng L. , 2016, pág. 43).

Asimismo, es necesario hacer otras dos observaciones importantes con respecto a la estructura actual de Partido Comunista de China y del Estado en China. Primero, el Partido tiene el poder de tomar todas las decisiones de asignación de personal y de formulación de políticas más importantes del Estado. Segundo, aunque el Partido es el principal responsable de la toma de decisiones, muchas discusiones políticas importantes, así como la mayoría de las políticas implementadas, tienen lugar en o a través de las instituciones gubernamentales, no de las organizaciones del PCCh (Cheng L. , 2016, pág. 44).[66]

Ciertamente, la República Popular de China en teoría tiene un gobierno unipartidista y centralizado, encabezado por el Partido Comunista de China (PCCh), pero en la práctica está fragmentado funcional y regionalmente**.** Por ejemplo, el primer escalafón de la estructura política lo ocupa el Secretario General del PCCh debajo se localiza el Buró Político del Partido Comunista de China, compuesto por 25 miembros, el cual, está dirigido por un subconjunto de élite conocido como el Comité Permanente del Buró Político (政治局常委 *zhengzhiju changwei*), compuesto actualmente por siete miembros. Este Comité se apoya en un Secretariado (*mishuchu* 秘书处), que contiene a las principales organizaciones

[65] Este trabajo de investigación se utiliza el sistema de transliteración de la fonética china conocido como *hanyu pinyin*.

[66] Aunque los líderes chinos de alto rango han pedido esporádicamente una mayor separación entre el partido y el Estado, en las últimas dos décadas la tendencia abrumadora ha sido consolidar y revitalizar el Partido en lugar de reducir su papel de liderazgo (Cheng, 2016, pág. 43).

centrales de ejecución del Partido que son: la Oficina General del Comité Central, el Departamento de Organización, el Departamento de Propaganda, el Departamento del Trabajo del Frente Unido y el Departamento de Enlace Internacional (Cheng L. , 2016, pág. 44).

El Secretariado se encarga de las tareas administrativas a todos los niveles políticos (provincial, municipal, de condado y niveles subsiguientes). Dentro de esta esfera se encuentran la Comisión Militar Central, el Pequeño Grupo de Liderazgo para Asuntos Exteriores, el Pequeño Grupo de Liderazgo para la Seguridad Nacional, junto con otros Pequeños Grupos de Liderazgo, incluidos el de Energía, Inversión Externa, Finanzas, Cambio Climático y Ciberseguridad. Este último escalafón lo complementan la Oficina de Investigación Política del Comité Central, la Oficina de Asuntos Exteriores del Comité Central y la Oficina de Información del Consejo de Estado (Shambaugh D. , 2013, pág. 63).

Por otra parte, en el vértice del "sistema de asuntos del estado" el Consejo de Estado (*State Council*, 国务院 *guowuyuan*) es el máximo órgano ejecutivo responsable de implementar y ejecutar las políticas públicas, regular las empresas de propiedad estatal y la industria comercial, así como de llevar a cabo las operaciones diarias del gobierno. De este dependen, las organizaciones gubernamentales centrales como ministerios, comisiones, oficinas, despachos y las comisiones de administración y supervisión de activos estatales (央企 *yangqi*).[67]

Dentro de este esquema institucional formal, el Ministerio de Industria y Tecnología de la Información (*Ministry of Industry and Information Technology* 中华人民共和国工业和信息化部 *zhongguo renmin gongheguo gongye he xinxihuabu*) tiene un papel técnico relevante en el establecimiento de las directrices sobre ciberseguridad. Bajo su mandato se localizan el Equipo Técnico de Respuesta de Emergencia de la Red Nacional de Informática de China y el Centro de Coordinación (*Chinese National Computer Network Emergency Response Technical Team and Coordination Center*, CNCERT/CC por sus siglas en inglés) (Lindsay J. R.,

[67] La mayoría de las agencias gubernamentales para el manejo de la seguridad cibernética civil pertenecen al Consejo del Estado (*State Council*).

Introduction, 2015b, pág. 10). El CNCERT/CC es responsable de dar respuesta a situaciones de emergencia relacionadas con 'infecciones informáticas' públicas de gravedad, mejorar la posición nacional en ciberseguridad, proteger la infraestructura crítica de información y, de emitir un informe anual de sobre la cantidad ataques cibernéticos recibidos en China (Lindsay J. R., 2015b, págs. 10-11). Para apoyar las actividades del CNCERT/CC, en 2016, se creó el organismo *Information Security Association of China*, compuesto de 257 miembros, en los cuales incluye la participación corporaciones, investigadores y expertos. Su misión es concentrar recursos humanos para apoyar el desarrollo de un ciberespacio más seguro. En este tenor, en 2017 también fue establecido el Comité de Seguridad de la Información [*Information Security Committee*] (Xinhua, 2016).

De igual manera, el Ministerio de Industria y Tecnología de la Información es el encargado de regular a los seis principales proveedores de servicio de internet en China (*Internet Service Providers*, ISP por sus siglas en inglés, 互联网服务提供商, *hulianwang fuwu tigongshang*), que a su vez se espera que colaboren en el proceso de monitoreo y filtración de contenido en sus redes de acuerdo con las pautas de censura establecidas por la Oficina de Informatización del Consejo de Estado (*State Council Informatization Office*, SCIO) (Lindsay J. R., 2015b, pág. 11) (Wines, 2011) (Deibert, Palfrrey, Rohozinski, & Zittrain, 2008; Deibert R. , Palfrey, Rohozinski, & Zittrain, 2010).

Cabe destacar que el establecimiento de la Oficina de Informatización del Consejo de Estado fue producto del *Plan Nacional de Informatización 2006-2020* (Austin, 2014, pág. 2). Dentro de este documento se enfatizaba sobre el valor intrínseco de la información, redes informáticas y tecnologías avanzadas para el desarrollo de China. Igualmente, otras prioridades del Plan Nacional de Informatización 2006-2020 son las siguientes: *a)* promover la sociedad de la información; *b)* fortalecer el desarrollo y uso de recursos de información; *c)* implementar un gobierno electrónico; *d)* construir una cultura de internet avanzada; *e)* mejorar la integración de infraestructura de información; *f)* mejorar la competitividad de la industria de tecnología de la información; *g)* construir un sistema nacional de seguridad de la información; *h)* crear más recursos humanos

en el campo de la tecnología de la información, *i)* promover un mejor sistema legal en relación con las tecnologías de información; *j)* mejorar los intercambios y la cooperación internacional en tecnologías de la información (Austin, 2014, pág. 3)

De igual manera, en cuanto a otras estructuras gubernamentales, por ejemplo, el Ministerio de Seguridad Pública (中华人民共和国公安部 *zhonghua renmin gongheguo gong'anbu*) es responsable de investigar los delitos informáticos, principalmente a través de su Buró Decimoprimero, y de exigir el cumplimiento de un esquema de protección multi-nivel (*multi-level protection scheme*) que se enmarca en el 'Documento 27'.[68] Igualmente, dentro del Ministerio de Seguridad Pública, el Tercer Instituto de Investigación realiza estudios sobre la "seguridad de la información".

Asimismo, desde 2014, se han establecido unidades policíacas cibernéticas con diferentes capacidades y tareas, pero, en general, conducen actividades de monitoreo digital (Wang, 2017)[69]. Por su parte, el Ministerio de Seguridad del Estado (中华人民共和国 国家安全部 *zhonghua renmin gongheguo guojia anquanbu*) funciona como el brazo de los servicios de inteligencia de China. Además, cuenta con una considerable capacidad técnica para realizar pruebas de vulnerabilidad y fiabilidad de *software* (Lindsay J. R., 2015b) (Microsoft News Center, 2003).

Por otro lado, desde 2013, el gobierno chino ha observado como una tarea estratégica primordial gestionar las cuestiones de seguridad en el ciberespacio (Alsabah, 2016). Para poder ejecutar este objetivo fueron creadas las oficinas administrativas del Grupo de Liderazgo sobre la Informatización y la Ciberseguridad, que a su vez se localizan dentro de la Oficina Estatal de la Información en Internet. Esta oficina también se le conoce como la Administración del Ciberespacio de China (*Cyberspace Administration of China*, CAC por sus siglas en inglés, 国家互联网信息办公室 *guojia hulian wangxinxi bangongshi*) creada en 2013 con el propósito de

[68] Este es un documento clasificado, pero es citado por diversas fuentes y enarbolado en diversos discursos de funcionarios chinos. Supuestamente contiene directrices y normativas relacionadas con la seguridad en el espacio digital. No ha sido posible acudir a la fuente primaria debido a la secrecía de ésta.

[69] Algunas de estas unidades policíacas cibernéticas se las ha llamado como *wumaodang* 五毛党, por el supuesto pago que reciben por cada comentario censurado en diversas redes sociales.

optimizar los traslapes de las estructuras encargadas de gestionar los asuntos del ciberespacio (Lindsay J. R., 2015b).

Dentro de este marco, la *Cyberspace Administration of China* tiene como responsabilidades controlar el contenido digital, reforzar la ciberseguridad y desarrollar la economía digital (Alsabah, 2016) (Segal A. , 2018, pág. 10). A su vez, cuenta con nueve diferentes oficinas, tres centros subordinados y 31 administraciones a nivel provincial (Alsabah, 2016; Zheng W. , 2019).[70] De igual manera, el presidente chino, Xi Jinping, encabeza directamente el CAC, lo que marca un cambio dramático en las actitudes de los líderes hacia la gestión del ciberespacio. Para el gobierno chino es un asunto de seguridad nacional controlar las actividades cibernéticas igual que controla los medios de poder tradicionales (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018) (Austin, 2018).

Por lo observado hasta el momento, se puede inferir que el Estado juega un papel dominante en el establecimiento de prioridades, dirección estratégica y supervisión de la gestión del esquema ciberespacial. De igual forma, se aprecia que los principales líderes chinos a menudo ocupan puestos múltiples en estas diversas organizaciones o en los comités coordinadores que los abarcan (Cheng L. , 2016). La política de seguridad cibernética china debe entenderse dentro de este contexto (Lindsay J. R., 2015b, pág. 6) (Yang, 2009) (Raud, 2016) (Zheng & Wen, 2016). Para un tratamiento más esquemático de las instituciones encargadas de ejecutar la política de ciberseguridad en la República Popular de China puede observarse la tabla 4.1.

Tabla. 4.1 Instituciones encargadas de la ciberseguridad en China

Comité Permanente del Politburó del PCCh	**Consejo de Estado** (State Council) • CAC Cyberspace Administration of	**Comisión Central Militar** (Central Military Commission)

[70] Desde agosto de 2018, su director es Zhuang Rongwen, quien era subdirector de esta, supliendo a Xu Lin, quien a su vez suplió a Lu Wei en julio de 2015. Lu Wei, conocido en su momento como 'el zar de internet' fue sentenciado en marzo de 2019 por actos de corrupción y aceptación de sobornos cuando desempeñaba el cargo de director del CAC.

	China (La Administración para el Ciberespacio de China)	
Grupo de Liderazgo sobre la Informatización y la Ciberseguridad • Buró de Protección de Secretos de Estados • Buró Estatal para el Manejo de la Encriptación	• State Council Information Office (SCIO) [Oficina de Información del Consejo de Estado] • State Internet Information Office (SIIO) [Oficina Estatal para la Información de Internet] • China Internet Network Information Center (CNNIC)	• Departamento General de Personal (*General Staff Department*) • Departamento de Señales de Inteligencia del EPL (3rd Department [SIGINT]) • Departamento para el Conflicto Electrónico del EPL (4th Department [Electronic Warfare])
	• Ministerio de Industria y Tecnología de la Información (Ministry of Industry & Information Technology) • Ministerio de Seguridad Pública (Ministry of Public Security) • Ministerio de Seguridad del Estado (Ministry of State Security) (*intelligence*)	• Fuerzas Áreas del EPL (PLA Air Forces) • Cuerpo de Marina del EPL (PLA Navy) • Cuerpo de Artillería del EPL (PLA Artillery)

Fuente: (Lindsay J. R., 2015b, pág. 9)

Además de estos mecanismos de toma de decisión formales, existen componentes no formales intergubernamentales, pero sí institucionales para la toma de decisiones a nivel nacional, enfocados en áreas que los gobernantes chinos

consideran prioritarias, llamados “Grupos Pequeños de Liderazgo” (*Leading Small Groups*, *lingdao xiaozu* 领导小组), o también conocidos como grupos de coordinación (*coordination groups*, *xietiao xiaozu* 协调小组) (Cheng L. , 2016, pág. 59). El papel de los Grupos Pequeños de Liderazgo es reunir a los principales responsables de la formulación de políticas para debatir y proporcionar asesoramiento y recomendaciones de políticas sobre cuestiones importantes al máximo órgano decisorio de China, el Comité Central Permanente del Buró Político del Partido Comunista Chino (Inkster, 2015, pág. 38). Sin embargo, se sabe muy poco acerca de cómo funcionan realmente los Grupos Pequeños de Liderazgo, qué tipo de información proporcionan a la dirigencia china y cuáles son los impactos de sus políticas. Pero hay algunas tendencias subyacentes generales que, hasta cierto punto, pueden influir en el conocimiento acerca de cómo se realiza el proceso de toma de decisiones en los ámbitos de política exterior y seguridad nacional entre estos dispositivos y la estructura formal (Inkster, 2015, pág. 39).[71]

Una serie de grupos pequeños de liderazgo (*leading small group* 领导小组) se encarga de diversos aspectos relacionados con la seguridad cibernética, un paso que sugiere su creciente deseo de gestionar sus operaciones cibernéticas de manera más eficiente (Alsabah, 2016). Esto quedó reflejado en el Décimo Octavo Congreso Nacional del Partido Comunista Chino, celebrado en noviembre de 2012, donde se ha dado una reorganización gubernamental en torno a la profundización de reformas de diversa índole, en el cual también se inserta la política de ciberseguridad. En efecto, antes de 2014, la responsabilidad sobre la implementación de la política de seguridad cibernética recaía en el Grupo de Liderazgo sobre la Informatización Gubernamental (国家信息化领导小组 *guojia xinxihua lingdao xiaozu*, State *Informatization Leading Group*, SILG por sus siglas en inglés) y la Oficina de Información del Consejo de Estado (国务院新闻办公室 *guowuyuan xinwen bangongshi*, State *Council Information Office*, SCIO, por sus siglas en inglés).

[71] Existen alrededor de 20 grupos de liderazgo bajo la estructura del Comité Central del Partido Comunista de China. Se organizan alrededor de algún tema funcional de suma importancia para la dirigencia china con el objeto de dar respuestas eficientes y expeditas (Miller A. L., 2008)

Con base en esto, el 28 de febrero de 2014, se estableció el Grupo de Liderazgo sobre la Ciberseguridad y la Informatización, encabezado por el presidente la República Popular de China, indicativo de que la seguridad cibernética fue elevada a la más alta prioridad de seguridad nacional. La creación del Grupo Pequeño de Liderazgo sobre Ciberseguridad es conocido también como el Grupo de Liderazgo sobre la Informatización y la Ciberseguridad (*Leading Small Group on Cybersecurity; Cybersecurity and Informatization Leading Group*, 网络安全和信息化领导小组 *wangluo anqua he xinxihua lingdao xiaozu*) (Raud, 2016, pág. 5) (Lindsay J. R., 2015b, pág. 8) (Jiang, 2014).

Para algunos analistas chinos, “las medidas políticas chinas no están plenamente implementadas, y hay una falta de coherencia en las directrices y la implementación de la ciberseguridad” (Li & Xu, 2015, pág. 231). Desde su percepción, “China aún no ha establecido estrategias nacionales o internacionales sobre el ciberespacio, y carece de métodos sistemáticos para la toma de decisiones, procesos y estándares sobre el manejo de problemas de seguridad de red, así como, un claro mecanismo de coordinación de seguridad de la red” (Li & Xu, 2015, pág. 231).

No obstante, desde inicios de la década de 2000, la ciberseguridad se ha convertido en una gran preocupación del gobierno chino y llama la atención de sus líderes más importantes. Desde ese momento, las autoridades chinas se han propuesto como meta convertirse en la sociedad de la información más avanzada, donde las tecnologías de la información y comunicación modernas mejoren el desempeño y desarrollo social (Austin, 2018, pág. 11). Para la consecución de este objetivo, se ha incluido a representantes gubernamentales de los sectores económicos y técnicos relacionados con el espectro digital. No obstante, a partir de 2002, la inclusión y la participación activa de las agencias de seguridad y de las fuerzas armadas chinas ha hecho que las políticas cibernéticas tengan un matiz más *securitizado* (Austin, 2018, pág. 12)

Simultáneamente, esto ha generado una complicación en relación a los esfuerzos de coordinación de un vasto y complejo aparato de formulación de políticas, una tarea que algunos expertos califican como “muy compleja” (Qu, 2010).

Con referencia a esto, Jon R. Lindsay subraya que “la política cibernética nacional en cualquier país debe equilibrar entre aparentes objetivos opuestos que van desde la seguridad nacional, a la aplicación de la ley y la regulación industrial en un contexto internacional de rápidos cambios tecnológicos” (Lindsay J. R., 2015b, pág. 14). Estos cambios resaltan la importancia del control de la información, así como también la relevancia de la defensa técnica de las redes en la noción de seguridad cibernética que tienen los dirigentes de la República Popular de China (Raud, 2016).

4.3 Normas e iniciativas gubernamentales elaboradas para la participación en el espacio digital

Cuando Internet se difundió en China desde finales de la década de 1990, se establecieron normas para los distintos sectores que constituyen los medios de comunicación: diarios, publicaciones periódicas, edición de libros, publicaciones electrónicas, películas, radio y televisión e instalaciones de recepción terrestre y por satélite (Castells, 2009, pág. 366). Asimismo, desde 1994, las regulaciones y normas sobre la seguridad cibernética, que involucran a diferentes agencias y sectores industriales, han buscado tener un enfoque nacional e integral (Austin, 2018, pág. 5). Aunado a ello, el gobierno chino ha adoptado Internet como un negocio, así como una herramienta educativa, cultural, de control y propaganda (Shirk, 2010).

Incluso, el gobierno de la República Popular de China considera que la *informatización*[72] de la sociedad china es un medio para garantizar el crecimiento económico sostenido que le permitirá competir a nivel mundial en el ámbito de la tecnología de la información y garantizar la seguridad nacional contra amenazas nacionales e internacionales (Embajada de la República Popular de China en Estados Unidos de América, 2006). Igualmente, la informatización se considera como la base de los sistemas de seguridad de la información que pueden apoyar la reestructuración económica y la seguridad nacional (Stokes, 2015, pág. 164).

[72] De acuerdos con las autoridades chinas, el concepto de ‘informatización’ significa la aplicación de tecnologías de la información y comunicación avanzadas para el mejoramiento de la vida política, económica y militar del país (Austin, 2018, pág. 10).

Además, otra tarea prioritaria consiste en modernizar el sector de los medios de comunicación y enfocarlo hacia la comercialización y el entretenimiento, pero manteniendo un férreo control político, por lo cual el gobierno ha venido realizando una amplia reforma de los medios de comunicación desde 2003 (Yang, 2009).

Para el caso de la seguridad de las redes, la génesis de su desarrollo se puede situar en el año 2012. En ese año, los problemas de ciberseguridad se discutieron en el *Duodécimo Plan Quinquenal Nacional de Desarrollo Estratégico sobre Industria Emergente* (*Twelfth Five-Year National Strategic Development Plan on Emerging Industry*), así como también en los planes quinquenales para las industrias de internet y comunicaciones (Li & Xu, 2015, pág. 229). Precisamente, el control sobre el ciberespacio en China se ha intensificado desde 2012, y se profundizó tras el establecimiento de la *Cyberspace Administration of China* (CAC por sus siglas en inglés) en el 2013. Desde 2012, Xi Jinping dejó claro el papel que juega el ciberespacio en su visión de China con el objetivo de convertirse en una "superpotencia digital" (Segal A. , 2018). Con esa finalidad, el 12 de diciembre de 2012, el Comité Permanente de la Asamblea Nacional Popular formuló la iniciativa *Decisión sobre el Fortalecimiento de la Protección de la Información de la Red* (*Decision on the Strengthening of Network Information Protection*) que establecía los principios básicos de protección de la información de la red a escala nacional (Li & Xu, 2015, pág. 229).

De igual manera, en consecuencia, el 15 de noviembre de 2013, durante la Tercera Sesión Plenaria del Décimo Octavo Congreso del PCCh fue publicado el documento *Decisión sobre las Principales Cuestiones Relativas a la Profundización Integral de las Reformas* (*The Decision on Major Issues Concerning Comprehensively Deepening Reforms*), donde se enfatiza que China debe "fortalecer la gobernanza de Internet conforme a la ley, acelerar la mejora en el sistema de gestión y su liderazgo sobre la seguridad nacional de las redes y la información" (Li & Xu, 2015, pág. 230) . También, el presidente Xi Jinping apuntó que "la seguridad de las redes y la información está relacionada con la seguridad nacional y la estabilidad social. Es un desafío integral nuevo al cual China se enfrenta" (Li & Xu, 2015, pág. 230).

Para tal efecto, la base de la política nacional de ciberseguridad fue producto de un documento de opinión del Grupo Pequeño de Liderazgo sobre la Informatización Gubernamental (SILG) conocido informalmente como el "Documento 27" (Lindsay J. R., 2015b, pág. 8). En este documento se describen iniciativas y esquemas multinivel para la protección de la infraestructura crítica, así como directrices para su implementación (Lindsay J. R., 2015b).[73] A su vez, otro documento que engloba el pensamiento gubernamental en materia cibernética es el *International Strategy of Cooperation on Cyberspace*, que hace hincapié tanto en la necesidad de una gobernanza multilateral de Internet como en la participación multipartidaria en esta gobernanza, incluidas las empresas, las organizaciones y las comunidades tecnológicas chinas (Nagelhus Schia & Gjesvik, 2018a).

Al mismo tiempo, en febrero de 2014, el presidente Xi Jinping anunció la orientación general para el desarrollo de la industria de ciberseguridad, resaltando la importancia de "conducir correctamente la relación entre seguridad y desarrollo" (Xi, 2014a). Igualmente, en septiembre del mismo año, mencionó que China necesitaba una "nueva estrategia militar cibernética" (Austin, 2018, pág. 10). En consecuencia, en diciembre 2014, el gobierno introdujo nuevas regulaciones que tenían la intención de promover el crecimiento de la industria doméstica de ciberseguridad (Austin, 2018, pág. 10)

Asimismo, durante 2014 también se celebró la primera Conferencia Mundial de Internet (*World Internet Conference*, 世界互联网大会, *shijie hulianwang dahui*). En los últimos cuatro años, la Conferencia Mundial de Internet se ha convertido en una plataforma importante para la cooperación y el intercambio sobre la economía digital global, el gobierno cibernético y la innovación, y ha atraído la atención de las empresas, los medios de comunicación y varios gobiernos, a su vez (Li Z. , 2016). A su vez, es la principal arena en la que China promueve su política exterior sobre

[73] Entre ellos se encuentran los siguientes mecanismos: criptografía para sistemas confiables, sistemas de monitoreo de seguridad de la información, procesos de gestión de crisis, apoyos para la investigación y desarrollo en seguridad, definición precisa de estándares técnicos y financiamiento garantizado para su implementación.

el ciberespacio y su postura sobre seguridad cibernética (Nagelhus Schia & Gvesvik, 2018b).[74]

En este sentido, 2014 puede considerarse en cierto modo, como un año decisivo en la conformación del enfoque gubernamental chino sobre la ciberseguridad. Después, en 2015, China adoptó un nuevo plan llamado *Internet Plus* para transformar su sector de manufactura intensivo en mano de obra hacia una base impulsada por Tecnologías de la Información que es más eficiente y global (Aaronson S. A., 2016). También, en 2015, las autoridades chinas publicaron nuevas regulaciones que requerían de las compañías extranjeras de tecnología de la información que fueran proveedoras de software a bancos comerciales revelar sus códigos fuente de los servicios que brindaban (Austin, 2018, pág. 14).

De acuerdo con Greg Austin (2018, pág. 14) esta medida fue realizada para apuntalar la ciberseguridad doméstica, en especial, buscaba afianzar el desempeño y el desarrollo de la industria interna de ciberseguridad y el robustecimiento de los sistemas financieros. No obstante, esta medida generó una respuesta enérgica de parte del gobierno de los Estados Unidos, que condujeron al régimen chino a suspender estas actividades en abril de 2015 (Austin, 2018, pág. 14) (Shih, 2015).

De igual manera, en mayo de 2015, el Consejo de Estado emitió una nueva estrategia militar, en la cual declaraba que el espacio exterior junto con el ciberespacio "se han convertido en mandatos de altura en una competencia estratégica" (State Council, 2015). Por último, en el mismo mes, la Asamblea Popular Nacional (*Quanguo Renmin Daibiao Dahui*, 全国人民代表大会) emitió una iniciativa de ley (que ya está en funcionamiento) que brindaba un lugar especial a la ciberseguridad como herramienta para fortalecer el control gubernamental sobre tecnología e inversión extranjera relacionada con el rubro tecno-científico en territorio chino (Austin, 2018, pág. 10) (Xinhua, 2017a).

[74] La *World Internet Conference* es una iniciativa del gobierno chino, ejecutada por la Administración del Ciberespacio de China (CAC). La primera reunión se llevó a cabo del 19 al 21 de noviembre de 2014 en la ciudad de Wuzhen, Zhejiang. Hasta diciembre 2017 se han ejecutado cuatro reuniones anuales de la WIC. Para más información de la WIC, se puede consultar el sitio oficial http://www.wuzhenwic.org

Asimismo, en julio de 2015, el Consejo de Estado dio a conocer el Plan de Acción para la ejecución de *Internet Plus*, que también tiene la intención de aumentar la presencia internacional de las empresas proveedoras de internet chinas (Aaronson S. A., 2016). Además, con el objeto de desarrollar un enfoque más holístico sobre el tratamiento de la ciberseguridad, en enero 2016, el gobierno chino anunció que realizaría una reforma profunda de los estándares de seguridad de la información que se habían establecido en 2002 en el Comité Técnico Nacional para la Estandarización de la Seguridad de la Información (NISSTC, por sus siglas en inglés) también llamado el Comité 260 (TC260) (Austin, 2018, pág. 16).

Para tal efecto, el régimen chino llevó a cabo la Reunión Nacional sobre Ciberseguridad e Informatización en 2016 (Xi, 2016) (SAC, 2016). Conjuntamente, en marzo de 2016 el gobierno chino estableció la Asociación China de Ciberseguridad (*Cybersecurity Association of China*) que comprende a 257 miembros entre instituciones académicas y de investigación, corporaciones e individuos que tiene como misión fomentar la auto-regulación de la industria, mejorar los estándares de operación, profundizar la investigación y ampliar la colaboración con contrapartes internacionales (Austin, 2018, pág. 11).

A su vez, a fines de 2016, la *Cyberspace Administration of China* (CAC) presentó una nueva estrategia para la ciberseguridad que incluye la advertencia de que, “el uso de internet con fines de traición, secesión, rebelión, subversión o robo o filtración de secretos de estado sería castigado" (Nagelhus Schia & Gjesvik, 2018a). Sobre el asunto, en diciembre de 2016, la CAC emitió la *National Cybersecurity Strategy* que provee la visión gubernamental china sobre el tema. Con referencia a esto, menciona lo siguiente:

> La seguridad del ciberespacio (de aquí en adelante llamada ciberseguridad) está relacionada con los intereses comunes de la humanidad, con cuestiones de desarrollo y paz global, así como con cuestiones de seguridad nacional de todos los países. Salvaguardar la ciberseguridad de nuestro país es una medida relevante para impulsar los acuerdos estratégicos integrales en la construcción de una sociedad moderadamente prospera, la profundización de las reformas, la gobernabilidad del país en conformidad con la ley y el ejercicio gubernamental coordinado como garantía para realizar el sueño chino del gran rejuvenecimiento de la nación china (CAC, 2016)

Conjuntamente, la CAC pretende analizar y supervisar los usos criminales e ilegales del ciberespacio relacionados con el “uso, recolección, almacenamiento y procesamiento de información de los usuarios y las prácticas injustas” (Austin, 2018, pág. 4). En síntesis, estas regulaciones enfatizan una prohibición de actividades que violan las "siete líneas de base" sobre el cumplimiento de leyes y regulaciones (el sistema socialista, el interés nacional, los derechos de los ciudadanos, los intereses legales de los ciudadanos, el orden público, la moral social y la veracidad de la información) (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018). En consecuencia, se está creando una “lista negra” de servicios y productos debido a que no aprueban los criterios de evaluación, lo que resulta en una proscripción de su uso por parte de agencias gubernamentales e industrias en sectores considerados estratégicos (Austin, 2018, pág. 4). Sobre la base de estas ideas, también se puede inferir que la estrategia gubernamental para la ciberseguridad es multidimensional, que involucra a diversos actores y altamente política (Austin, 2018, pág. 7). Asimismo, Greg Austin (2018, pág. 11) recalca que “estas regulaciones pretenden contribuir al objetivo gubernamental de convertirse un poder cibernético y de fortalecer la seguridad nacional”.

Asimismo, la *National Cybersecurity Strategy* de la CAC estableció nueve áreas prioritarias para la ejecución de este plan que se resumen en la tabla 4.2.

Tabla 4.2 Áreas prioritarias de la ciberseguridad en China

Áreas	**Funciones**
1. Defender la soberanía cibernética 2. Mantener la seguridad nacional	*Seguridad política*: protección del sistema de partido de amenazas políticas subversivas de carácter cibernético que se originen dentro y fuera de China
3. Proteger la infraestructura crítica de la información (CII)	*Seguridad interna*: asegurar la resiliencia de la economía digital y de los servicios esenciales en relación con ataques cibernéticos o fallas de sistemas que tengan impactos nacionales. Esta responsabilidad recae en los cuerpos policiales y servicios civiles de emergencia

4. Fortalecimiento de la cultura *online*	*Seguridad cultural*: manejar y proteger la información digital del comercio electrónico, contrarrestar rumores y el esparcimiento de noticias falsas, fomentar una cultura de internet e impulsar un comportamiento responsable en línea. Asimismo, asegurar un ecosistema de comunicaciones ordenado y regulado en el ciberespacio
5. Combate al crimen y terrorismo cibernético	*Política judicial*: proteger a las corporaciones, agencias gubernamentales y a las personas de crímenes no políticos que incluyen el robo de información, robo de identidad y ataques cibernéticos maliciosos
6. Mejoramiento de la gobernanza cibernética	*Política social*: creación de conceptos, aplicación de la investigación, desarrollo de sistemas, y buscar equilibrio entre innovación y seguridad entre diversos actores
7. Reforzamiento de los fundamentos de la ciberseguridad	*Política educativa y técnica*: edificar los cimientos para el desarrollo de ciencia y tecnología, educación digital, mejorar prácticas y estrategias en el manejo y monitoreo de riesgos, establecer políticas de *big data*, almacenamiento en nube e internet de las cosas.
8. Mejorar las capacidades de defensa cibernética	*Política de Defensa*: prevenir invasiones y conflictos en el ciberespacio, así como promoción de la paz digital.
9. Fortalecer la cooperación internacional	*Política exterior*: promoción de normas internacionales, construcción de capacidades a través de la asistencia mutua a nivel internacional

Fuente: (Austin, 2018, pág. 8) (CAC, 2016)

De la misma manera, en septiembre de 2016, como complemento a lo anterior, las autoridades chinas emitieron nuevas regulaciones que establecían explícitamente que los mensajes y comentarios sobre productos en redes sociales como *WeChat Moments* se pueden recopilar y utilizar como 'datos electrónicos' en procedimientos legales (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018; Marro, 2016). Aunado a

ello, en noviembre de 2016, el gobierno chino formuló *la Ley de Ciberseguridad*, que otorgaba prerrogativas para "monitorear, defender, y manejar amenazas y riesgos cibernéticos que se originen en fuentes dentro y fuera del país, además de proteger la infraestructura de información de ataques, intrusiones, interrupciones y daños" (Austin, 2018, pág. 11). Como resultado, en diciembre de 2016, la CAC publicó la *National Cyberspace Security Strategy*, una estrategia holística y multidimensional para abordar las cuestiones de seguridad en el ciberespacio en los niveles internacional, gubernamental, corporativo e individual (Austin, 2018).

Del mismo modo, en 2017, la CAC publicó cuatro regulaciones principales sobre la administración de Internet, que van desde el fortalecimiento en los requisitos de registro de nombres reales en los foros de Internet, los comentarios en línea, medidas sobre el uso de redes virtuales privadas (*virtual private networks* VPN)[75] y hasta la responsabilidad de las personas que albergan cuentas públicas, así como el contenido en las plataformas de grupos de chat políticamente moderados (China Digital Times, 2017) (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018) (Zheng S. , 2017). Esto puede ser evidencia de una intensificación de los esfuerzos por parte de las autoridades chinas para asegurar la correlación entre el registro de los usuarios con cuentas electrónicas y direcciones IP, además de una fuerte tendencia de prohibir el acceso anónimo al ciberespacio (Austin, 2018, pág. 90) (Xinhua, 2017b).

Con respecto a lo anterior, el 8 de febrero de 2017, el gobierno chino anuncio la creación de un Comité de Análisis sobre Ciberseguridad (*Cybersecurity Review Committee*), con prerrogativas amplias de supervisión sobre productos y servicios que tengan efectos sobre el interés público y la seguridad nacional (Austin, 2018, pág. 4) (China Daily, 2017). Asimismo, el 17 de febrero de 2017 el gobierno de la República Popular de China anunció la táctica de cercar el ciberespacio, como parte de una 'nueva perspectiva global sobre la protección de la infraestructura crítica de la información y establecer 'una valla' de ciberseguridad' (China.org, 2017). Por

[75] Las VPN son herramientas que utilizan los usuarios para acceder a contenido que ha sido prohibido o bloqueado por el gobierno chino. Funciona como un canal o conducto alterno para ingresar en internet, evitando o evadiendo los controles territoriales del contenido en línea.

consiguiente, en julio de 2017, el régimen chino anunció un plan para convertirse en líderes mundiales en inteligencia artificial (IA) para 2030 con el propósito de incrementar el valor de su industria para 2020 en alrededor de $22 mil millones de dólares estadounidenses y para 2025 en aproximadamente $59 mil millones de dólares estadounidenses (Gan, 2017). El plan está subdividido en tres fases: *1)* comprende mantener el desarrollo de aplicaciones tecnológica avanzadas en IA hasta 2020; *2)* para 2025 hacer los principales descubrimientos y; *3)* a partir de 2030 ser el líder indiscutible en el diseño, desarrollo y aplicación de IA (Lee A. , 2017).

En este sentido se comprende un fuerte incremento en el interés de las autoridades chinas en nuevas aplicaciones de inteligencia artificial, como reconocimiento facial en los lugares públicos, en el transporte público y en instalación de dispositivos de reconocimiento electrónico en documentos oficiales que tienen como objeto fortalecer la seguridad pública e identificar a personas que infrinjan diferentes tipos de reglamentaciones (Gan, 2017) (Li T. , 2017). Para tener una perspectiva del desarrollo de la inteligencia artificial en la República Popular de China y su posición mundial se puede observar la tabla 4.3.

Tabla 4.3 Inversión acumulada en los sectores de Inteligencia Artificial (2012-2016)

Posición con relación a la inversión	**País**	**Monto de inversión** (millones de dólares)	**Número de Compañías**
1	Estados Unidos	17.9 mil	2,905
2	República Popular de China	2.6 mil	709
3	Reino Unido	800	366
4	Canadá	640	228
5	Alemania	639	160
6	Israel	400	173
7	Japón	300	N/A**

8	Francia	280	136
9	España	250	132
10	Suiza	210	83

*India cuenta con alrededor 233 empresas, pero los montos de su inversión no están señalados.
**En el caso de Japón no se muestran el número de empresas dedicadas exclusivamente al desarrollo de Inteligencia Artificial. No obstante, otros reportes están muestran que estás equivalen al 2% de las compañías a nivel mundial (Neuromation, 2018)
Fuente: (Lee A. , 2017)

Por otra parte, en marzo de 2017, el gobierno solicitó a las compañías tecnológicas chinas (como Tencent, Weibo, Baidu) que cerraran los sitios web que alojaban discusiones sobre historia, asuntos internacionales y el ejército que fueran en contra de la postura oficialista (Segal A. , 2018, pág. 12). Unos meses más tarde, en el período previo al XIX Congreso del Partido Comunista Chino, Tencent, Weibo y Baidu fueron multados por albergar contenido considerado prohibido y por violar las nuevas leyes de ciberseguridad (Segal A. , 2018, pág. 12).[76]

De igual manera, el 9 de abril de 2018, el CAC ordenó a todas las tiendas de aplicaciones chinas eliminar las cuatro aplicaciones de noticias más populares durante semanas porque no lograron "mantener el orden legal sobre difusión de la información". (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018). Un día después (10 de abril de 2018), las autoridades exigieron a Toutiao (el principal sitio web de noticias de China) y a WeChat, cerrar permanentemente una cuenta que contenía parodias y bromas debido a la "publicación de contenido vulgar e impropio" (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018).

Con base en estas evidencias se puede aseverar que, la dirigencia china propone una visión sobre la ciberseguridad que se entrelaza profundamente con la seguridad interna y con acciones políticas y sociales que pongan en tela de juicio su legitimidad gubernamental. Es por esa razón, que la seguridad del contenido ha sido una prioridad en el manejo del ciberespacio (Austin, 2018). Con base en lo

[76] Tencent es una empresa proveedora de productos y servicios de internet, la segunda compañía digital más grande de la República Popular de China. Baidu es un motor de búsqueda, similar a Google. Por su parte, Weibo, es un sitio web de redes sociales.

anterior, el gobierno chino cree que el ciberespacio aún debe respetar la cultura, las costumbres y la gobernanza del espacio físico definido por las fronteras de un país (Burgman, 2016). Con la intención de lograr su objetivo, el régimen chino ha utilizado una combinación de controles sociales y técnicos para censurar el contenido y controlar las actividades en el ciberespacio que considere afectan la estabilidad política y social de la República Popular (Austin, 2014, pág. 65).

En este sentido, las autoridades políticas chinas consideran el ciberespacio como un campo de suma relevancia para el desarrollo económico a través de la innovación tecnológica. Visto de esta forma, algunos expertos destacan que la expresión por excelencia de esta posición es el desarrollo del sistema nacional de gestión de seguridad de la información (*National Information Security Management System*) también llamado Project 005 conocido como *The Great Firewall* (el Gran Muro de Fuego) (Klimburg, 2017, págs. 265-266).[77] Sobre el asunto, algunos especialistas recalcan que "China se está preparando para aprovechar la inteligencia artificial para usos militares, incluyendo drones autónomos, software que puede defenderse a sí mismo contra ciberataques y programas que extraen patrones de comportamiento en redes sociales para predecir movimientos políticos de disidentes del régimen" (Segal A. , 2018, pág. 14).

[77] En 1997 la revista *Wired* acuñó el término 'Great Firewall' como una analogía al constructo físico de la Gran Muralla (Barmé & Ye, 1997). En ese año el profesor y ex director de la Universidad de Correos y Telecomunicaciones de Beijing Fang Binxing entregó una propuesta para desarrollar una infraestructura digital al Ministerio de Industria y Tecnología de la Información de la República Popular de China. Es por ello, que se le considera el contribuidor principal en el desarrollo de la infraestructura de censura de contenido en el ciberespacio chino.
Un *firewall* es un dispositivo de seguridad de red que monitorea las entradas y salidas de contenido informático en una red, por consiguiente, decide que permitir o bloquear en el tráfico informativo basado en un conjunto de comandos predeterminados (Cisco, 2019). La idea es que está versión digital mantendrá alejados a aquellos visitantes indeseados del ciberespacio chino. La comparación se hace como una alusión a la Gran Muralla como una barrera que contenía a distintos grupos del espacio territorial controlado por las dinastías chinas. No obstante, esta barrera física en diversos periodos históricos no logró ese objetivo explícito (Spence, 1990). El *Great Firewall* de China fue operacional hasta el 2003, a partir de ese momento se ha actualizado y ajustado hasta ser una herramienta sumamente potente para el filtrado y el bloqueo en el acceso de contenido dentro de China. No obstante, su efectividad es discutida por especialistas en el campo y puesta a prueba por activistas y disidentes digitales a través de ingeniosas tácticas, juegos de palabras, sátira y humor, llamada *egao* 恶搞 (literalmente significa "trabajo malvado", referida como "parodia en línea) (Gong & Yang, 2010) (Leibold, 2011). Estas acciones tienen como propósito circumvalar los controles en el ciberespacio (China Digital Times, 2017) (Shih, 2015)

Asimismo, de estas evidencias, se puede destacar que la dirigencia china tiene un gran interés en fortalecer sus capacidades técnicas para controlar el contenido informativo del ciberespacio dentro de sus fronteras. Además, el régimen está buscando promover el desarrollo de su complejo industrial cibernético para dar solvencia a sus políticas internas de seguridad (Austin, 2018, pág. 27). Por tanto, se puede inferir que debido a la magnitud, alcance y variedad de las actividades cibernéticas ha obligado al gobierno chino a una reestructuración de su comportamiento, en aras de estar capacitado para abordar un fenómeno multidisciplinar, multidimensional y contingente.

4.4 Prácticas y narrativas de ciberseguridad china en el espacio digital

Cabe señalar que los gobernantes chinos no tienen una concepción singular del ciberespacio directamente análoga a la empleada por los teóricos militares y civiles en los Estados Unidos o en el conjunto gubernamental compuesto por la Unión Europea (Sheldon & McReynolds, 2015). El término ciberespacio, que a su vez se toma prestado de la ciencia ficción occidental y que tradicionalmente ha carecido de límites claramente definidos, se transcribe al chino como *wangluo kongjian* 网络空间 o *dianzi kongjian* 电子空间. Dentro de este orden de ideas, los analistas y estrategas de la República Popular de China consideran la existencia de un dominio de información que contiene una cantidad de subdominios claramente definidos, como el dominio de la red informática, el dominio electromagnético, el dominio psicológico y el dominio de inteligencia (Sheldon & McReynolds, 2015, pág. 197).

De este modo, esta visión puede ser una comprensión holística de los sistemas que componen el ciberespacio (ver capítulo 1), donde el gobierno chino robustece sus políticas para el control de cada uno de ellos. Por ejemplo, desde 2012, Beijing ha reforzado significativamente los controles en sitios web y redes sociales. De igual manera, con Xi Jinping como presidente, China ha tratado de dar forma a las instituciones y normas internacionales que rigen el ciberespacio (Segal A. , 2018, pág. 16). De acuerdo con el presidente chino, la soberanía cibernética representa “el derecho de cada país a elegir independientemente su propio camino

de desarrollo cibernético, su propio modelo de regulación cibernética y políticas públicas de Internet, y su participación en la gobernanza internacional del ciberespacio en igualdad de condiciones" (Segal A. , 2018, pág. 11).

Es por eso que, en la apertura de la 2ª Conferencia Mundial de Internet (*World Internet Conference*) en Wuzhen, China de 2015, el presidente Xi Jinping durante su discurso en la ceremonia de apertura, afirmó inequívocamente que todos los países tenían derecho a gobernar su ciberespacio (Xinhua, 2015). La idea de la "soberanía cibernética" ha sido aplicada por varios gobiernos durante muchos años, especialmente en países de la región de Medio Oriente, mediante la censura de contenido que se considera religiosamente inmoral o socialmente inaceptable (Burgman, 2016). No obstante, sólo recientemente es que una gran potencia ha respaldado la idea de soberanía cibernética al más alto nivel de gobierno (Nagelhus Schia & Gjesvik, 2018a) (Nagelhus Schia & Gvesvik, 2018b) (Burgman, 2016).

Por consiguiente, para el gobierno chino la soberanía cibernética es una nueva parte constitutiva de la soberanía, que debe ser protegida (Ye, 2015). Para comprender el concepto de soberanía cibernética, es útil contrastarlo con el método actual de gobernanza del ciberespacio y cómo ha evolucionado. Si bien la posición china es que el gobierno de una nación y las fuerzas armadas deben gobernar el terreno ciberespacial, el régimen actual, liderado principalmente por organizaciones no gubernamentales y apuntalado por el gobierno de Estados Unidos y algunos otros países socios, empresas y agencias gubernamentales estadounidenses, es interpretado por el régimen chino como un vehículo que da mucho espacio para la influencia de individuos y compañías privadas en la definición y protección de los activos digitales (Nagelhus Schia & Gvesvik, 2018b).

Dentro de esta perspectiva, en 2014, Lu Wei, el ex director de la *Cyberspace Administration of China* (Administración del Ciberespacio de China), escribió un artículo de opinión titulado "La soberanía cibernética debe gobernar Internet global", donde planteó una propuesta de respeto mutuo y cooperación en el ciberespacio entre los Estados Unidos y China (Lu W. , 2015) (Nagelhus Schia & Gvesvik, 2018b) (Burgman, 2016). Además, en la *International Strategy of Cooperation on Cyberspace* (Estrategia Internacional de Cooperación en el Ciberespacio), los

funcionarios chinos describieron el concepto “soberanía cibernética” de la siguiente manera:

> “Los países deben respetar el derecho de otro a elegir su propio camino de desarrollo cibernético, su propio modelo de regulación y políticas públicas de Internet, y participar en la gobernanza internacional del ciberespacio en una igualdad de condiciones. Ningún país deberá perseguir la hegemonía cibernética, interferir en los asuntos internos de otros países, o participar, aprobar o apoyar las actividades cibernéticas que socavan la seguridad nacional de otros países” (Xinhua, 2017).

En todo caso el concepto se refiere a la capacidad de los Estados para gobernar y controlar su ciberespacio, es decir, dentro de su territorio, asegurando que el espacio digital esté sujeto a las mismas reglas, normas y consideraciones culturales que el resto de la sociedad de un país (Nagelhus Schia & Gjesvik, 2018a). Para algunos funcionarios chinos “un país tiene derecho a establecer entradas de información (*information gateways*) para su frontera cibernética y de esa forma controlar la información que fluye hacia y desde sus límites cibernéticos” (Ye, 2015, pág. 133).

Por ejemplo, con base en la visión de sus máximos dirigentes, especialmente el presidente Xi Jinping (习近平), la ciberseguridad ha sido entendido de la siguiente manera: “*1)* la ciberseguridad es un tema holístico, en la ‘era de la información’, la ciberseguridad tiene una relación estrecha con varios aspectos de la *seguridad nacional*; *2)* la ciberseguridad es dinámica, pues la tecnología de la información cambia rápidamente, y las redes cada vez están más interconectadas e interdependientes. La fuente de amenazas y los medios de ataque se están desarrollando con mayor sofisticación. La idea de confiar en algunas cuantas piezas de equipo de seguridad y software de seguridad para mantener la resiliencia de las redes es obsoleta. Se necesita establecer un concepto de ciberseguridad dinámico e integral; *3)* la ciberseguridad es abierta, opera en múltiples niveles y únicamente se puede fortalecer si se establecen mecanismos de cooperación, intercambio e interacción para absorber tecnología avanzada; *4)* la ciberseguridad es relativa, ya que no existe seguridad absoluta, y debe considerar las condiciones nacionales, así

como tratar de evitar la seguridad a toda costa; *5)* la ciberseguridad es un lugar común, para las personas y se apoya en las personas, por ello, es responsabilidad de toda la sociedad y necesita la participación conjunta de gobierno, empresas, organizaciones sociales y de la totalidad de usuarios de la Red para construir una línea de defensa" (Xi, 2016).

Para algunos expertos como Greg Austin, esto dibuja una dirección general sobre el progreso de la ciberseguridad que enfatiza una relación íntima entre seguridad y desarrollo (Austin, 2018, pág. 6). Como resultado, el poder cibernético de la República Popular de China pretende anclarse en la intersección de cuatro prioridades nacionales: *1)* configurar un ciberespacio o 'internet armonioso'; *2)* la reducción de la dependencia externa en relación con equipos y componentes digitales y de comunicación, *3)* una mayor consciencia sobre el riesgo que representa los ataques cibernéticos en redes gubernamentales y privadas que podrían interrumpir servicios críticos, dañar el crecimiento económico y causar destrucción física y; *4)* la promoción del concepto de "soberanía cibernética" como el principio organizador para la gobernanza de Internet (Segal A. , 2018, págs. 10-11) (Zhang, 2016) (Zuo, 2016).[78]

En ese mismo tenor, se enfatiza que, para defender las fronteras cibernéticas, es necesario establecer defensas cibernéticas. Según el coronel del Ejército Popular de Liberación (EPL) Ye Zheng (2015, pág. 133) "las defensas cibernéticas se están convirtiendo en las nuevas murallas defensivas. Estas deben ser lideradas por el Estado e implementadas principalmente por los militares, con los esfuerzos combinados de la sociedad civil". Esto refleja lo que se mencionaba en los capítulos anteriores, como la securitización de un objeto social, o también puede interpretarse como la militarización de lo civil o la ciudadanización de los asuntos militares.

[78] El régimen de la República Popular de China ha buscado infundir la idea de que su presencia en el ciberespacio es omnipresente. Para ello, las autoridades chinas han desarrollado la representación de la soberanía cibernética, que tiene como propósito el ajuste de los flujos informáticos a una base territorial que cuente con una fuerte participación estatal. A su vez, el significado del concepto 'poder cibernético' no es tan nítido para la dirigencia china. No obstante, se enfatiza tanto en el ejercicio de control como en el desarrollo de capacidades económicas, científicas, técnicas y militares que apuntalan una superioridad en el ciberespacio (Austin, 2018, pág. 10).

Por consiguiente, para algunos funcionarios estadounidenses, “China está previendo un mundo de internet apegado a fronteras nacionales, con el control del gobierno justificado por los derechos soberanos de los Estados” (Segal A. , 2018, pág. 11). Debe recalcase que en muchos aspectos el funcionamiento del ciberespacio no ha estado desmarcado de las jurisdicciones nacionales o regionales, por lo cual los usuarios están sujetos a las condicionantes impuestas por el espacio físico cuando utilizan el espacio digital (Goldsmith & Wu, 2006). Con base en ello, para algunos funcionarios militares chinos “el ejercicio independiente de la autoridad de una nación sobre las actividades en el ciberespacio, incluidas las actividades políticas, económicas, culturales y tecnológicas, es un nuevo desarrollo en la era de la información” (Ye, 2015, pág. 132).

Es por eso que, en el documento llamado *International Strategy of Cooperation on Cyberspace* se menciona el concepto “soberanía cibernética” como una parte clave de una política cibernética china amplia, que se promueve desde los niveles políticos más altos. En otras palabras, el concepto de soberanía cibernética de China se basa en dos principios clave: *1)* prohibir la influencia no deseada en el ‘espacio de información’ de un país y; *2)* trasladar la gobernanza de Internet de los organismos actuales, a un foro internacional como las Naciones Unidas (Xinhua, 2017) (Nagelhus Schia & Gvesvik, 2018b).

En este sentido se comprende, lo que recalcan algunos especialistas acerca de que “los esfuerzos más visibles de China para escribir las reglas para el ciberespacio se han centrado en las Naciones Unidas y en el principio de soberanía cibernética” (Segal A. , 2018). Además, para Adam Segal, director del *Digital and Cyberspace Policy Program* del *Council on Foreign Relations* subraya que “los políticos chinos creen que tendrán una mayor participación en la regulación de la tecnología de la información y la definición de reglas globales para el ciberespacio si Naciones Unidas desempeña un papel más importante en la gobernanza del ciberespacio” (Segal A. , 2018, pág. 12).

En torno a esto, en junio de 2015, el gobierno de China aprobó la *Ley de Seguridad Nacional* con el propósito declarado de “salvaguardar la seguridad de China [sic]”, pero incluía amplias disposiciones que abordaban la política económica

e industrial (Aaronson S. A., 2016). A su vez, China también ha redactado leyes relacionadas con la lucha en contra del terrorismo y la ciberseguridad que, si se concretan en su forma actual, también impondrían restricciones comerciales de gran alcance y onerosas a los productos y servicios de TIC importados en China (Aaronson S. A., 2016). Por ejemplo, los borradores de la nueva *Ley de Ciberseguridad* (en vigor desde junio de 2017) se han distribuido desde julio de 2015, proporcionando indicadores de esta dirección que está tomando el gobierno chino en relación con este tema (Nagelhus Schia & Gjesvik, 2018a).

Asimismo, la nueva *Ley de Ciberseguridad* de China se puede entender como una función o un efecto del concepto de soberanía cibernética china. Es decir, a nivel nacional, el gobierno chino no muestra signos de desacelerar su régimen de censura de Internet, ya que ha elevado la importancia de su soberanía cibernética al mismo estatuto que su soberanía territorial física (Burgman, 2016). Es por ello que, el bloqueo abierto de los sitios web parece haber empeorado durante el 2015, con 8 de los 25 sitios web con mayor tráfico del mundo en la actualidad se bloqueados dentro de territorio chino (Aaronson S. A., 2016).

A razón de ello, se puede afirmar que una característica distintiva del concepto chino de seguridad de la información (信息安全 *xinxi anquan*) es que pone su énfasis tanto el contenido de la información que se transporta por el ciberespacio como el de la seguridad técnica de la red (网络安全 *wangluo anquan*), por el contrario, la noción de Estados Unidos sobre el concepto de ciberseguridad y en buena parte de Europa, destaca más la parte de las amenazas técnicas sobre la funcionalidad de los sistemas en red (Lindsay J. R., 2015b, pág. 11).

A su vez, se considera que, para los dirigentes chinos, todo el concepto del ciberespacio se sustenta en el control de la información a través de la censura, lo que se considera una visión completamente diferente de la de los gobernantes "occidentales" (Raud, 2016, pág. 6). Si bien la posición oficial china es que el gobierno de un Estado y las fuerzas armadas deben gobernar Internet, el ciberespacio, como se mencionó líneas arriba, se percibe tanto como una gran amenaza para la estabilidad de China, como necesario para los objetivos de desarrollo de China (Nagelhus Schia & Gjesvik, 2018a).

Por ello, una gran parte de las agencias gubernamentales, las empresas comerciales y las organizaciones sociales se benefician de la tecnología de la información y podrían verse perjudicados en cierta medida por su abuso o por un cierre parcial (Lindsay J. R., 2015b, pág. 6). Esto es un buen ejemplo de cómo los chinos entienden el elemento cibernético, como algo fuertemente integrado con la sociedad, y no lo separan del flujo general de gobernanza (Raud, 2016, pág. 5).

Naturalmente, China depende cada vez más de diversos actores cibernéticos y las autoridades chinas han reaccionaron en este tenor. Incluso, su concepto de soberanía cibernética se inscribe en esta perspectiva. Si bien es cierto que, esta idea está ligada con la subordinación del ciberespacio a los intereses y valores del Estado, el concepto no deja de lado la participación de actores no estatales en la configuración de la política cibernética. Como lo afirma Jon R. Lindsay, "la seguridad cibernética está conformada por la interacción estratégica de muchos actores con características diferentes y desafía cualquier interpretación simple" (2015b, pág. 6). Con ello, se puede atestiguar un creciente énfasis en las medidas de ciberseguridad, así como un aumento en la disposición del país para aprovechar las oportunidades que ofrece el entorno cibernético para responder a las amenazas hacia la seguridad nacional (Raud, 2016, pág. 5).

Por consiguiente, una de las principales formas en que la dirigencia china ha intentado equilibrar estas dos preocupaciones ha sido a través de la promoción de empresas nacionales de telecomunicaciones y de tecnología en los mercados bursátiles internacionales y, permitiéndoles una mayor participación en las decisiones gubernamentales (Nagelhus Schia & Gvesvik, 2018b). Conforme a algunos especialistas, "este es un enfoque holístico que no separa los desafíos de mantenimiento de una infraestructura ciberespacial del flujo de contenido y la información" (Nagelhus Schia & Gvesvik, 2018b).

Con base en lo revisado, se puede aseverar que las prácticas de *securitización* gubernamentales en el ciberespacio del régimen chino, tratan de legitimar y justificar sus acciones a través de referencias y testimonios que enfatizan la protección de valores culturales-nacionales y de la seguridad nacional. Aquí también se puede sostener lo que se mencionaba en el capítulo 2, acerca de que

los fundamentos físicos e infraestructuras que permiten el desarrollo del campo cibernético no tienen significado alguno sin la apropiación y usos que los agentes le otorguen, como en el caso del gobierno chino y su interpretación de lo que considera el sistema cibernético internacional y su relación con el concepto de ciberseguridad. Asimismo, se puede observar que las prácticas generadas por el gobierno chino en el ámbito digital le han dotado de una identidad cibernética única, que se encuentra ligada a la dinámica de la configuración de sus intereses por transformarse en una 'superpotencia tecnológica'.

Es por eso, que la conceptualización que China tiene sobre sí misma en el ámbito internacional es un reflejo que influye directamente de sus expectativas en el sistema internacional cibernético, las cuales son convertirse en un actor preponderante, que tenga voz y capacidad de decisión para (re)establecer las normas de conducta en el ciberespacio global. Como lo recalcaba Ted Hopf (1998) las identidades y los intereses de un actor conforman una variable que depende de los contextos histórico, cultural, político, social y espacial. En este caso, en todos los ámbitos el gobierno chino, bajo el liderazgo de Xi Jinping, puede decirse, como afirman algunos analistas "ha mostrado mayor confianza en su modelo político y económico y, sin duda un mayor interés en proyectar su influencia en otras partes del mundo" (Stenslie & Chen, 2016, pág. 121).

Además, se puede observar que la seguridad no ha sido un concepto estático, ni una condición social determinada para el gobierno chino, lo cual da mayor claridad a la no linealidad de su postura en el sistema internacional cibernético. También se ha podido constatar la dinámica de los procesos de securitización (*securitization*), donde ciertos temas, como el flujo de información en el ciberespacio pasan de ser 'asuntos ordinarios' a ser asuntos de seguridad nacional, enmarcado en las políticas gubernamentales y en la creación de instituciones para su manejo, el cual exige una mayor atención pública y la aceptación de políticas públicas urgentes (Buzan B. , 1991) (Buzan, Waever, & de Wilde, 1998) (Waever, 1995). Por tanto, bajo este sujeto de estudio se puede verificarla hipótesis de que los Estados están reconfigurando su comportamiento en el ciberespacio, que transita de la indiferencia a una inserción profundo en las

interacciones digitales. Esto se expresa en gran medida a través del desarrollo de normas y reglas para regular las acciones de ciberseguridad y con el afán de obtener una postura preeminente en el sistema internacional.

Capítulo 5. Origen y evolución de las estrategias estadounidenses de seguridad sobre el espacio digital

Introducción

La idea central de este capítulo es analizar el tema de la ciberseguridad como eje toral en las políticas internas y externas estadounidenses y su efecto sobre su conducta en el ciberespacio, esto con el objeto de contribuir al fortalecimiento de la hipótesis central de este trabajo. La ciberseguridad se ha vuelto un interés nacional de los Estados Unidos. Es por eso que, para el gobierno estadounidense, existen poderosas razones económicas, políticas y de seguridad para respaldar una internet segura y confiable, dada la cantidad de actividades que ahora se realizan en línea (Rovner & Moore, 2017, pág. 184). Asimismo, Estados Unidos de América tiene una fuerte apuesta en la ciberseguridad, dado el alcance y la complejidad de las comunicaciones entre las agencias civiles gubernamentales y las fuerzas militares a lo largo de la cadena de mando (Rovner & Moore, 2017, pág. 184).

Aunado a lo anterior, algunos autores consideran que la posición estadounidense en el ciberespacio es inherentemente predominante debido a que *de facto* es el lugar de nacimiento de Internet (Klimburg, 2017, pág. 136). Incluso, recalcan que el gobierno de Estados Unidos ha buscado tener una posición de preeminencia en esta área desde la década de 1980 (Joyner, 2012). Cabe resaltar que la meta de supremacía estadounidense no es únicamente una cuestión exclusiva para el ciberespacio. Por ejemplo, la Fuerza Área, la Marina y el Comando Espacial de los Estados Unidos en diferentes ocasiones han enfatizado el mismo propósito. No obstante, en esos dominios (tierra, aire, mar, espacio ulterior), a diferencia del ciberespacio, existen reglas explícitas e implícitas, leyes internacionales y normas de comportamiento comúnmente aceptadas que constriñen las acciones de los agentes (Klimburg, 2017, pág. 138).

Por otra parte, la gran mayoría de los actores de la industria cibernética en rubros como desarrollo de hardware, software y servicios digitales son estadounidenses o tienen su sede en los Estados Unidos (Klimburg, 2017, pág. 136). Por ello, comprender la estructura, la organización, las normas y prácticas que

dan forma a la arquitectura cibernética de los Estados Unidos de América no es una tarea sencilla. Asimismo, la ubicuidad de temas y traslapes del ciberespacio crean un entorno confuso y de incertidumbre, el cual se buscará esclarecer a lo largo de este capítulo. Para efectos de esta investigación se revisan la mayor cantidad de información abierta sobre el tema, así como en opiniones de especialistas reconocidos en el tema, a través de una comprobación cruzada de datos sensibles para corroborar su veracidad y autenticidad.

Con relación a lo anterior, completa la contrastación entre dos perspectivas gubernamentales sobre la ciberseguridad y el enfoque para participar en el espacio digital: específicamente a Estados Unidos como caso de estudio. En seguida, se muestran cuáles son las organizaciones que ejecutan algún aspecto de la política de ciberseguridad, cuáles son sus prerrogativas y las dinámicas institucionales para este tema específico. A partir de esto, se muestran las normas e iniciativas más significativas del enfoque gubernamental en relación con la ciberseguridad. Para efectos de esta investigación se realiza una revisión de la mayor cantidad de información abierta sobre el tema, así como en opiniones de especialistas reconocidos en el tema, a través de una comprobación cruzada. Finalmente, en la última sección de este capítulo se presenta narrativas significativas que solventan y brindan comprensión más profunda sobre el tipo de acciones en materia de ciberseguridad.

5.1 Estudio de la ciberseguridad en Estados Unidos

En la literatura especializada sobre ciberseguridad, existe un número no tan extenso de títulos que abordan profundamente y de forma holística a Estados Unidos como caso de estudio (Lord & Sharp, 2011; Owens, Dam, & Lin, 2009; Kamphausen, Li, & Scobell, 2009). Llama la atención este desarrollo, debido a la preponderancia que se le ha dado al fenómeno que se subrayaba en la parte introductoria. Sin embargo, la profusión sobre diversas temáticas relacionadas con la seguridad y el ciberespacio es amplia y diversa, cuestión que hace compleja la tarea de revisar toda la agrupación de análisis realizados.

Desde la década de 1990, existe un conjunto de investigaciones que han abordado a profundidad, el desarrollo y las implicaciones del conflicto cibernético o la guerra de información, el papel de las infraestructuras de información y los sistemas de comunicación en el campo militar (Libicki M. , 1995; Arquilla & Ronfeldt, 1993; Rattray, 2001; Mazanec & Thayer, 2015; Gary Sharp, 1999; Gompert, Lachow, & Perkins, 2006). Bajo este esquema, se han desarrollado diversos análisis que abordan la interrelación entre la información, el ciberespacio y la seguridad nacional (Denning D. , 1998; Reveron, 2012; Clarke & Knake, 2010; Libicki, 2009; Dunn Cavelty, 2008b; Miller & Lachow, 2007; Bayuk, y otros, 2012).

Por un lado, algunos estudios han buscado responder a cuáles son los efectos del ciberespacio sobre la geopolítica, la gobernanza global del ciberespacio o la competencia internacional digital (Powers & Jablonski, 2015; Buchanan, 2016) (Guiora, 2017; Segal, 2016). Por otro lado, otros análisis se han enfocado en cuestiones más precisas sobre los impactos de la cuestión cibernética en la sociedad, como la vigilancia estatal a través de la tecnología, el terrorismo cibernético, la ciberdelincuencia y el desarrollo de normas para combatirlo (Klein, 2015) (Weimann, 2005) (Lee N. , 2013) (Sanger D. , 2012).

Por lo que se refiere al tema en particular de la ciberseguridad en Estados Unidos, visto desde la perspectiva gubernamental, se han generado intensos debates de política pública sobre cómo responder a diferentes desafíos hacia la seguridad de la información, además, de cuál debe ser la mejor estrategia y cómo implementarla. No obstante, para algunos analistas, se está generando un enfoque basado en la preocupación y el desasosiego que está aumentando su prevalencia en relación con otras direcciones para abordar el fenómeno (Lawson, Yeo, Yu, & Greene, 2016).

Con base en esto, algunos observadores han destacado que, desde comienzos del siglo XXI, existe una tendencia entre estrategas políticos, expertos y medios de comunicación sobre la utilización de “escenarios cibernéticos aterradores” (*cyber-doom scenarios*) para describir la ciberseguridad y los efectos perjudiciales si no se protegen correctamente activos, infraestructuras y fundamentos técnicos que permiten el funcionamiento adecuado del ciberespacio

(Debrix, 2001) (Dunn Cavelty, 2008b) (Lawson S. , 2013). Por otra parte, algunos académicos recalcan que debido al apego a estas narrativas es probable que el gobierno de los Estados Unidos invierta más presupuesto y recursos organizacionales que el resto del mundo en tareas relacionadas con la ciberseguridad, incluido el espionaje y en el desarrollo de capacidades cibernéticas ofensivas y defensivas, (Klimburg, 2017, pág. 136) (White House, 2018) (White House, 2018b).[79]

A partir de estas evidencias, se hace necesario realizar un esfuerzo intelectual por construir un análisis holístico acerca del tratamiento de la ciberseguridad en Estados Unidos, en particular, desde la óptica gubernamental. A pesar de esta sugerencia e identificación de un problema epistemológico, no es la pretensión de esta investigación llenar este vacío, pues, este trabajo se enfoca principalmente en las acciones, conductas y percepciones que tienen los agentes estatales en el ámbito de la ciberseguridad, sin olvidar que interactúa con otras entidades y opera en diversos niveles para diseñar, implementar y ejecutar políticas para una cuestión multifacética, multinivel y compleja, pero deja de lado en buena medida las acciones de otros agentes.

5.2 Instituciones, estructura y organización encargadas de la política de ciberseguridad en Estados Unidos

Con el propósito de entender cómo el gobierno estadounidense maneja el fenómeno de la ciberseguridad, es necesario exponer cuáles son las principales instituciones encargadas de ejecutar la política de ciberseguridad, sus principales tareas y sus acciones en dicho ámbito. Con respecto a la estructura gubernamental de los Estados Unidos sobre quién gestiona y ejecuta la política de ciberseguridad, la

[79] Algunas estimaciones mencionan que solamente el presupuesto cibernético militar acumulado entre 2017-2022 será de aproximadamente $7 mil millones de dólares por año. Además, recalcan que eso podría ser únicamente una proporción del presupuesto general del Departamento de Defensa en temas de tecnologías de la información con un valor de $37 mil millones de dólares por año (Klimburg, 2017, pág. 136). E incluso, algunas estimaciones calculan que podría tener un presupuesto de entre $26 mil y $30 mil millones de dólares desde 2016 (White House, 2018b). Es complicado hacer una revisión cruzada de los datos debido a que existen pocos datos sobre las cifras asignadas para el ejercicio de la ciberseguridad gubernamental estadounidense.

organización es vasta y compleja, incluso, para algunos autores, esa complejidad se puede inferir desde el momento de determinar el número exacto de agencias, oficinas, departamentos y comisiones relacionadas con la temática (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 15).

En torno a esto, y debido a la complicación de coordinar una política transversal, multinivel y multifacética, en su momento, fue creado el Comité de Políticas Intergubernamentales de Infraestructura en Información y Comunicación del Consejo de Seguridad Nacional de la Casa Blanca (*National Security Council's Information and Communication Infrastructure Interagency Policy Committee*, por sus siglas, NSC-ICIIPC) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). Conviene subrayar que el Consejo de Seguridad Nacional (*National Security Council*) es un mecanismo en el que los miembros del Gabinete y los Asesores de Seguridad se reúnen con el representante del poder ejecutivo de los Estados Unidos para determinar las prioridades de la política nacional e internacional de dicho país.

Por su parte, el NSC-ICIIPC está co-presidido por el Consejo de Seguridad Interna (*Homeland Security Council*) y el Coordinador de Seguridad Cibernética (CSC, *Cyber Security Coordinator*,), que se localiza dentro de la Oficina de Seguridad Cibernética del Consejo de Seguridad Nacional (*National Security Council's Cyber Security Office*) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 15). Asimismo, el CSC lidera el desarrollo interinstitucional de la política de ciberseguridad, así como la implementación y supervisión de las estrategias realizadas por las distintas agencias gubernamentales (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 16).

Por otra parte, el Departamento de Seguridad Interna (*Department of Homeland Security*, DHS) es la principal institución responsable de la ciberseguridad dentro de las fronteras de los Estados Unidos, en particular, sobre las cuestiones no militares de la ciberseguridad, aunque para algunos expertos, "este tiene una responsabilidad legal muy limitada para la protección de los sistemas de información federales" (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 16)

(Klimburg, 2017, pág. 144).[80] No obstante, la cantidad de reglamentaciones y normas que dan facultades al DHS sobre la ciberseguridad y la protección de la infraestructura crítica es considerablemente abundante.

Por ejemplo, con el objeto de dotarle capacidad de implementación, en 2003, se emitió la *Directiva Presidencial de Seguridad Nacional No. 7* (*Homeland Security Presidential Directive 7*) que confirmaba la responsabilidad del DHS para coordinar los esfuerzos generales de protección de la infraestructura crítica y designaba al departamento como la agencia líder para fungir como enlace en el ejercicio de "compartir información sobre amenazas, evaluación de vulnerabilidades y desarrollo de medidas protección y planes de contingencia apropiados para los sectores de tecnología de la información y comunicaciones" (U.S. Department of Homeland Security, 2003).

Con base en esto, se le asignó al DHS la producción de un *Plan Nacional para la Protección de Infraestructura* (*National Infrastructure Protection Plan*, NIPP) que ponía los cimientos para "desarrollar criterios de asociación entre el gobierno federal y los propietarios y operadores de infraestructura crítica" (U.S. Department of Homeland Security, 2009).[81] De manera conjunta, en 2011, se implementó el plan *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* que perfilaba líneas estratégicas para el DHS, la Fundación Nacional de Ciencia (*National Science Foundation*) y el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*) sobre los

[80] Conforme a la Ley de Seguridad Interna de 2002 (*Homeland Securit Act*, 2002) fue creado dicho Departamento (*Department of Homeland* Security, DHS). Con respecto a la temática de la ciberseguridad, se le ha dado la prerrogativa de coordinar los esfuerzos nacionales relacionados con la protección de infraestructura crítica en los sectores de tecnología de la información y comunicaciones de carácter civil-gubernamental (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). Dentro del debate sobre sus funciones, se le imputa su poca capacidad técnica en comparación con otras agencias o departamentos federales, en especial, en relación con la NSA, USCYBERCOM y el Departamento de Defensa (Harris, 2014).

[81] De acuerdo con el *National Infrastructure Protection Plan* de 2009, el gobierno de los Estados Unidos considera que las infraestructuras críticas se componen por 16 diferentes sectores que incluyen: instalaciones químicas, instalaciones comerciales, comunicaciones, manufactura crítica, presas, base industrial de defensa, servicios de emergencia, sector energético, servicios financieros, sector de alimentos y agricultura, instalaciones gubernamentales, sector salud, reactores nucleares, sector de tecnología de la información, sistemas de transporte, sistema de agua y saneamiento y sector de materiales y residuos (U.S. Department of Homeland Security, 2009).

lineamientos en investigación y el aseguramiento de la infraestructura de comunicaciones (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 11).

En el mismo tenor a los documentos anteriores, en 2013 se emitió la *Orden Ejecutiva 13636: Mejoramiento de la Infraestructura Crìtica de Seguridad* (*Executive Order 13636*: *Improving Critical Infrastructure Cybersecurity*), que buscaba establecer un "intercambio más efectivo de información entre el gobierno federal y el sector privado, así como el establecimiento de requisitos mínimos para el mejoramiento de la seguridad en infraestructuras críticas" (U.S. Department of Homeland Security, 2013). Junto con la *EO 13636* se publicó la *Directiva Política Presidencial de Seguridad de la Infraestructura Crítica y Resiliencia* (*Presidential Policy Directive Critical Infrastructure Security and* Resilience, *PPD 21*) que exigía "una evaluación del modelo de asociación público-privado existente sobre el intercambio de información en materia de ciberseguridad, esclarecimiento de la identificación de datos de referencia y de los requisitos del sistema para un intercambio eficiente de información, junto con el desarrollo situacional de capacidades" (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 12).

Con objeto de la implementación de estas acciones, en 2014 el gobierno federal estadounidense desarrolló un Marco Voluntario de Ciberseguridad para la Protección de Infraestructura Crítica (*Framework for Improving Critical Infrastructure Cybersecurity*), el cual proveía de directrices, prácticas y estándares para que el sector privado se enfocara en la protección de la infraestructura crítica (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 12) (U.S. Department of Homeland Security, Office of Inspector General, 2014).[82] Conforme con las autoridades del DHS y el Departamento de Comercio, el marco estaba diseñado para ayudar a las organizaciones privadas a que iniciaran un programa de ciberseguridad o de mejoramiento de este (para los que ya contaran con algún plan), así como proporcionar un enfoque de gestión de riesgos en aras de fortalecer la ciberseguridad en los sectores de infraestructura críticos, sin embargo, su carácter

[82] El *marco* fue publicado por el *National Institute of Standards and Technology*, del Departamento de Comercio de los Estados Unidos (The National Institute of Standards and Technology, U.S. Deparment of Commerce, 2014)

no vinculante merma su ejecución (U.S. Chamber of Commerce, 2014) (Department of Homeland Security, 2013).

Con referencia a las ocupaciones del DHS, los documentos *Deparment of Homeland Security´s Blueprint for a Secure Cyber Future* de 2011 y *Quadrennial Homeland Security Review* de 2010 establecieron un plan de acción que delineaba dos áreas principales de responsabilidad para el DHS: *1)* proteger la infraestructura de información crítica y; *2)* fortalecer el ecosistema cibernético (U.S. Department of Homeland Security, 2011; U.S. Department of Homeland Security, 2014). De acuerdo con esto, sus tareas principales son: *a)* fortalecer y afianzar la resiliencia de la infraestructura crítica; *b)* apoyar a las agencias gubernamentales civiles con respecto a adquisiciones sobre ciberseguridad; *c)* promover la adopción de políticas comunes en atención a riesgos y promover el mejoramiento de las prácticas de ciberseguridad; *d)* fomentar la implementación de la normatividad; *e)* potenciar la capacidad de respuesta a incidentes de seguridad cibernéticos e, *f)* incentivar el reporte de capacidades y el aseguramiento del ecosistema cibernético (U.S. Department of Homeland Security, 2014). Para tal efecto, en 2013, el gobierno estadounidense legalizó el papel del DHS sobre la prevención y respuesta a incidentes de ciberseguridad y el establecimiento de una asociación de intercambio de información entre este y los propietarios-operadores de la infraestructura crítica, por medio de la *Ley Nacional de Ciberseguridad y Protección de Infraestructura Crítica* (*National Cybersecurity and Critical Infrastructure Protection Act*, NCCIP) (U.S. House Committee on Homeland Security, 2014).

Al mismo tiempo, en diciembre 2014, el presidente Barack Obama firmó la Ley Nacional de Protección en Ciberseguridad (*National Cybersecurity Protection Act*) que permitía al DHS: *a)* dar respuesta a incidentes cibernéticos; *b)* asistir a agencias federales y compañías privadas sobre incidentes cibernéticos y; *c)* recomendar medidas para la gestión de ciberseguridad (U.S. Congressional Budget Office, 2014). Por su parte, el *Quadrennial Homeland Security Review* del 2014 priorizaba la asignación de recursos en función de la protección ante las amenazas de ciberseguridad para aquellos que respaldaran el interés nacional (U.S. Department of Homeland Security, 2014).

Puesto que el DHS es el organismo encargado de la protección de infraestructura crítica entre los sectores gubernamentales civiles, el Departamento cuenta con varias unidades para la ejecución de la política de ciberseguridad tales como: la Dirección Nacional de Protección y Programas (*National Protection & Programs Directorate*, NPPD), la Oficina de Ciberseguridad y Comunicaciones (*Office of Cybersecurity and Communications*, (CS&C); que proporciona herramientas para la gestión de crisis, respuesta a incidentes y capacidades de defensa para la totalidad de la infraestructura de comunicación y el ciberespacio y; el Centro Nacional de Integración de Comunicaciones y Ciberseguridad (*National Cybersecurity & Communications Centre*, NCCIC); que coordina los aspectos de ciberseguridad en cuanto a la protección de infraestructura crítica junto con agentes privados dentro de la NPPD.

Además, dentro de sus actividades incluyen la concientización situacional sobre mitigación de vulnerabilidades, intrusiones, incidentes, así como acciones de recuperación de datos. (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, págs. 17-18) (U.S. Department of Homeland Security, 2014). No obstante, que la NCCIC trabaja estrechamente con operadores y propietarios de la infraestructura crítica, no tiene autoridad para hacer cumplir las medidas de ciberseguridad en el sector privado (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 18). Por último, en mayo de 2017 fue formulada la más reciente legislación sobre las facultades del DHS en cuestión de ciberseguridad, la *Executive Order 13800*, emitida por el presidente de los Estados Unidos Donald J. Trump para el fortalecimiento de las redes federales de comunicación y la infraestructura crítica (Department of Homeland Security, 2019).

Además del DHS, existen otras agencias gubernamentales con tareas particulares en relación con la ciberseguridad. Por ejemplo, el Departamento de Estado (*Department of* State, DoS) es la principal agencia para comunicar y coordinar la política de ciberseguridad de la rama ejecutiva a nivel internacional. Asimismo, el Departamento de Estado se ocupa de los aspectos cibernéticos relacionados con la seguridad internacional, los problemas económicos y asuntos como los derechos humanos digitales y el libre de acceso a Internet (Klimburg, 2017,

pág. 138). Para ello, dentro del Departamento de Estado, se encuentra la Oficina del Coordinador para Problemas Cibernéticos (*Office of the Coordinator for Cyber Issues*) que se encarga de coordinar los problemas cibernéticos al interior del departamento. Las responsabilidades de la oficina incluyen asesorar al secretario y a los subsecretarios en temas cibernéticos y actuar como enlace con la Casa Blanca, el ejecutivo estadounidense y entre distintos departamentos, agencias federales, así como con el sector privado (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016).

Igualmente, el Departamento de Estado tiene como asignatura impulsar una comprensión más amplia del derecho internacional cibernético, así como el desarrollo de normas de comportamiento en el ciberespacio. En relación con ello, ha instado por un uso más profundo de las herramientas internacionales existentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención sobre Ciberdelincuencia del Consejo de Europa (Convención de Budapest) (U.S. Government White House , 2018). Junto con eso busca fomentar la cooperación internacional en la investigación de actividades cibernéticas maliciosas, incluido el desarrollo de soluciones a posibles barreras para la recopilación e intercambio de información entre agencias gubernamentales (U.S. Government White House , 2018).

Conjuntamente, en cuanto a hacer cumplir las leyes y reglamentaciones relacionadas con la ciberseguridad, el Departamento de Justicia (*Department of* Justice, DoJ) es el gran responsable. Además, es el encargado de investigar, atribuir y procesar los delitos cibernéticos. Entre sus funciones se encuentra la recopilación, el análisis y la difusión de información sobre amenazas cibernéticas como fraude informático, delincuencia informática y vigilancia electrónica criminal. (U.S. Department of Justice, 2018). Para garantizar el combate efectivo hacia las amenazas cibernéticas sobre la seguridad nacional y brindarle al proceso un enfoque gubernamental global, la División de Seguridad Nacional del Departamento de Justicia (*National Security Division*) ha lanzado, en asociación con otros componentes del departamento, una Red Nacional de Especialistas Cibernéticos de Seguridad Nacional (*National Security Cyber Specialist Network*) con el objetivo de

tener un conocimiento profundo sobre las intrusiones y ataques cibernéticos realizados por otros Estados o por organizaciones no gubernamentales (U.S. Department of Justice, 2018). Además, en 2014 creó la Unidad de Ciberseguridad dentro la sección de Propiedad Intelectual y Crimen Informático para que funcione como un centro especializado en asesoría legal sobre violaciones cibernéticas. Junto con esa tarea, la Unidad de Ciberseguridad coadyuva a la conformación de la legislación especializada sobre ciberseguridad para proteger las redes nacionales e individuales informáticas (U.S. Department of Justice, 2018b).

Por otra parte, con respecto a los alcances del ciberespacio dentro del ámbito de seguridad nacional y de la esfera militar, el Departamento de Defensa (*Department of Defense,* DoD) es la agencia responsable de salvaguardar la infraestructura de información nacional de un ciberataque, así como la protección del dominio digital [.mil]. De igual manera, entre sus ocupaciones se encuentra recopilar información sobre amenazas cibernéticas extranjeras, garantizar la seguridad nacional y los sistemas militares, así como investigar los delitos cibernéticos bajo jurisdicción militar (U.S. Department of Defense , 2015). Con referencia a esto, para algunos especialistas, el gobierno de los Estados Unidos ha concebido el fenómeno cibernético como un problema de seguridad nacional con gran ímpetu (Joyner, 2012, pág. 159). Con relación a lo anterior, en 2006, fue emitida la Estrategia Nacional Militar para Operaciones en el Ciberespacio (*National Military Strategy for Cyberspace Operations*). Este documento brindaba una descripción general sobre el enfoque militar en relación con las operaciones del ciberespacio (The Joint Chiefs of Staff, 2006).[83]

Esta doctrina militar contiene el anuncio de la intención de explotar las operaciones de información como una herramienta para la política internacional separada de las operaciones del campo de batalla militar, en las cuales se incluye

[83] El Departamento de Defensa de los Estados Unidos ha cambiado el nombre de guerra de información (*information warfare* [IW] por sus siglas en inglés) como operaciones de información (*information operations* [IO] por sus siglas en inglés). Asimismo, la Organización del Tratado del Atlántico Norte también ha adoptado la misma definición para las (IO), las cuales son definidas como "las acciones tomadas para afectar la información del adversario y los sistemas de información mientras se defiende la información y sistemas de información propios" (Eriksson & Giacomello, 2006, pág. 237).

realizar espionaje informático y sabotaje informático[84], así como 'proyección de la verdad', es decir influir directamente en los medios de comunicación electrónicos en todo momento y así poder modificar la opinión pública (Dunn Cavelty & Brunner, 2007, pág. 10; U.S. Deparment of Defense, 2003). Además, en dicho texto, el ciberespacio se definía como "un dominio caracterizado por el uso del espectro electrónico y electromagnético para almacenar, modificar e intercambiar información a través de infraestructuras físicas y sistemas de información en red" (Kuehl, 2009, pág. 26)

Igualmente, en el 2006, se solicitó al Departamento de Defensa desarrollar una teoría sobre poder espacial y ciberespacial, encuadrada en el *Quadrennial Defense Review* (Department of Defense, 2006). De acuerdo con esa estrategia, "el ciberespacio era el entorno para lograr los objetivos nacionales militares en operaciones de inteligencia y en operaciones comerciales" (The Joint Chiefs of Staff, 2006). Llama la atención que en las operaciones militares de inteligencia se incluya una consideración comercial, aunque no se ahonda más sobre ello. Después, surgió la *National Military Strategy* de 2011, la cual reconocía que el "ciberespacio había emergido como un dominio de combate por derecho propio".[85]

Asimismo, subrayaba la utilidad de profundizar la participación gubernamental en el ciberespacio al decir que, "los Estados Unidos de América deben mejorar la disuasión en el aire, el espacio y el ciberespacio al poseer la capacidad de luchar en un entorno 'degradado' y así mejorar la capacidad para atribuir y derrotar ataques en los sistemas de infraestructura (U.S. Department of Defense, 2011). A su vez, en 2012, un documento titulado *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense* focalizaba los principales objetivos militares en el ciberespacio, como la defensa de las redes y la capacidad de resiliencia y recuperación de éstas (U.S. Department of Defense, 2012).

[84] Un programa de espionaje se define como una serie ordenada de actividades secretas o no, que están encaminadas a obtener información estratégica sobre un Estado, organismo o individuo, a fin de lograr un cambio en las interacciones con dichos actores (Arreola García, 2015, pág. 214)

[85] Para algunos especialistas, 2011 es el año que marca el inicio de una actividad estatal intensa en el ciberespacio, e incluso, lo señalan como el comienzo de la "militarización del ciberespacio" (Morozov, 2011) (Deibert, 2011)

Con respecto a las implicaciones multifacéticas y transversales de la ciberseguridad dentro del ámbito de la defensa, en 2010 fue creado el *US Cyber Command* (USCYBERCOM), que alcanzó capacidad operativa en el mismo año. Esta es una sub-unidad de comando bajo el *US Strategic Command* (USSTRATCOM) localizada en Fort Meade Maryland y co-localizada en las oficinas centrales de la Agencia de Seguridad Nacional de Estados Unidos (NSA, *National Security Agency*) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 20). La misión del USCYBERCOM es planificar, coordinar, integrar, sincronizar y conducir actividades de defensa de las redes de información específicas del Departamento de Defensa y, prepararse para dirigir operaciones militares dentro del ciberespacio (Singer & Friedman, 2014, pág. 133)

Asimismo, como parte de su misión, USCYBERCOM buscar crear y liderar tres tipos de gestiones cibernéticas: *a)* fuerzas de protección; *b)* misiones de combate y; *c)* fuerzas de misión nacional. Igualmente, dentro de esta rama militar, cada una tiene un componente encargado de cuestiones cibernéticas que reportan directamente a USCYBERCOM, por ejemplo: Comando Cibernético de la Armada (*Army Cyber Command*, ARCYBER), Décima Flota del Comando Cibernético de los Estados Unidos (*US Fleet Cyber Command 10th* (FCC/C10F), Fuerzas para el Ciberespacio del Cuerpo de Marina de EE.UU. (*US Marine Corps Forces Cyberspace*, MARFORCYBER), Vigesimocuarta Fuerza Área Cibernética (*24th Air Force Cyber*, AFCYBER), Comando Cibernético de la Guardia Costera (*Coast Guard Cyber Command*, CGCYBER) (U.S. Cyber Command, 2018).

Al mismo tiempo, USCYBERCOM tiene la responsabilidad principal del comando y control centralizado de las operaciones del ciberespacio en el ámbito de la defensa, incluida su sincronización, planificación y ejecución. Asimismo, lidera la defensa diaria y la protección de las redes de información del Departamento de Defensa[86]; coordina las operaciones que brindan apoyo a las misiones militares;

[86] Varias de las redes de información del Departamento de Defensa de EE.UU. no se encuentran conectadas a las redes informáticas globales. Igualmente, la mayoría de los ministerios de defensa del mudo operan de manera similar, bajo redes seguras y aisladas llamadas *air-gap systems*. No obstante, la preocupación de diversos gobiernos es que algunos incidentes han sucedido incluso dentro de este tipo sistemas informáticos aislados.

dirige las operaciones y la defensa de redes de información especificadas; y se prepara para llevar a cabo operaciones militares en el espectro completo del ciberespacio cuando se le indique (U.S. Cyber Command, 2018a) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 20).

Las actividades cibernéticas y las misiones del Departamento de Defensa quedaron sujetas en la estrategia de 2015, *Department of Defense Cyber Strategy*, que consideraba tres objetivos principales para el Departamento dentro del terreno cibernético: *1)* creación de capacidades operativas para la ciberseguridad y protección de redes internas, información y sistemas de información; *2)* defensa contra ataques cibernéticos de 'importancia significativa' y; *3)* apoyo a operaciones militares informáticas junto con la elaboración de planes de contingencia (U.S. Department of Defense , 2015).

Desde una perspectiva legal el Pentágono ha provisto al Departamento de Defensa con un *Manual Legal sobre la Guerra*, que incluye un capítulo que clarifica la interpretación legal de la aplicación de la ley y las interpretaciones de *jus in bello* –las prácticas aceptables mientras se está en guerra, sus disposiciones se aplican a todas las partes en conflicto-, independientemente de los motivos del conflicto y de la justicia de la causa- *ius ad bellum* – sobre las legítimas razones que un Estado tiene para entrar en guerra en el ciberespacio (U.S. Department of Defense, Office of General Counsel, 2015).[87] Por último, el documento *Joint Cyberspace Operations Document* (JP 3-12) de 2018 aborda el enfoque más reciente del gobierno de los Estados Unidos sobre cómo abordar las operaciones militares en el ciberespacio, además, de delinear las interrelaciones operativas y de comando relacionadas con el ciberespacio y la incorporación de las perspectivas operativas aprendidas (The Joint Chief of Staff, 2018).

En síntesis, las iniciativas estratégicas del Departamento de Defensa de los Estados Unidos para operar en el ciberespacio incluyen lo siguiente: *a)* abordar el ciberespacio como un dominio operacional para organización, entrenamiento y

[87] Para algunos académicos, este es uno de los aspectos más espinosos en cuanto al desarrollo de normas de comportamiento en el ciberespacio, puesto que genera un enfoque permisible para un entorno bélico, además de una participación gubernamental agresiva (Klimburg, 2017).

equipamiento para que el Departamento de Defensa pueda aprovechar al máximo su potencial; *b)* emplear nuevos conceptos operativos de defensa para proteger las redes y sistemas del Departamento de Defensa; *c)* asociarse con otros departamentos y agencias del gobierno de los Estados. Unidos, así como el sector privado, para permitir una estrategia gubernamental de ciberseguridad integral; *e)* construir relaciones sólidas con los aliados de Estados Unidos, así como con socios internacionales para fortalecer la ciberseguridad colectiva y; *f)* aprovechar el ingenio de la nación a través de una fuerza de trabajo cibernética excepcional y de rápida innovación tecnológica (U.S. Department of Defense, 2011).

Con el objetivo de aclarar las principales funciones que cada una de las agencias gubernamentales estadounidenses llevan a cabo en relación con la ciberseguridad, se puede observar la tabla 5.1.

Tabla 5.1 Instituciones gubernamentales involucradas en ciberseguridad dentro de Estados Unidos

Institución gubernamental	**Principales funciones**
Departamento de Defensa	• Abordar el ciberespacio como un dominio operacional como el resto de los dominios militares (terrestre, aéreo, marítimo y espacio ulterior).
Departamento de Justicia	• Investigar, atribuir y procesar los delitos cibernéticos • Recopilar, analizar y difundir información sobre amenazas cibernéticas • Hacer cumplir las leyes y reglamentaciones relacionadas con la ciberseguridad
Departamento de Comercio	• Ayudar a las organizaciones privadas a desarrollar sus propios programas de ciberseguridad • Generar normas para el buen funcionamiento de servicios relacionados con Internet

Departamento de Seguridad Interna	• Fortalecer y afianzar la resiliencia de la infraestructura crítica • Apoyar a otras agencias gubernamentales civiles con respecto a adquisiciones sobre ciberseguridad • Promover la adopción de políticas comunes en atención a riesgos y mejoramiento de las prácticas de ciberseguridad • Potenciar la capacidad de respuesta a incidentes de seguridad cibernéticos
Departamento de Estado	• Comunicar y coordinar la política de ciberseguridad de la rama ejecutiva a nivel internacional
USCYBERCOM	• Implementar nuevos conceptos de seguridad para tener éxito en ese ámbito. • Asociarse con otras agencias de seguridad y el sector privado cibernético • Desarrollar nuevos talentos para impulsar nuevas innovaciones sobre cómo los militares podrían luchar y ganar en este espacio.

Fuente: elaboración propia

Como se puede observar, para el caso de la política de ciberseguridad, todos los departamentos y agencias federales tienen la responsabilidad individual de proteger sus propios sistemas de tecnología de información y comunicación y, además, muchos tienen responsabilidades específicas sectoriales en relación con la ciberseguridad (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 15). Además, como consecuencia, para algunos analistas, estas evidencias muestran que "el Gobierno Federal pretende utilizar todos los medios disponibles para mantener a salvo su país de amenazas cibernéticas y proteger al pueblo estadounidense en el dominio digital" (Lynn, 2010; White House, 2018a). No obstante, cabría preguntarse si las acciones del gobierno de los Estados Unidos de América tienen como único objetivo la protección de sus ciudadanos o también la defensa en el dominio digital

sirve para ejercer un control más integral sobre su población y como una herramienta para mantener una posición preminente en el sistema internacional a través de aventajar a otros Estados en el terreno cibernético.

5.3 Normas e iniciativas gubernamentales elaboradas para la participación en el espacio digital

En cuanto al desarrollo de normatividades sobre la actuación y proceder en el entorno cibernético, el gobierno de los Estados Unidos ha sido pionero a nivel global. Por ejemplo, en 1963, se encargó a un grupo de expertos realizar una investigación sobre los sistemas de comunicaciones que se relacionaban con las necesidades de seguridad nacional y cómo se podían mejorar estas interacciones. A partir de ello, un comité interdepartamental gubernamental recomendó la formación de un sistema de comunicaciones unificado para apoyar las actividades del representante de la rama ejecutiva (Dunn Cavelty, 2008b, pág. 41). Por consiguiente, con el fin de brindar un mejor soporte a comunicaciones gubernamentales críticas durante procesos de emergencia, el presidente John F. Kennedy emitió un Memorando Presidencial el 21 de agosto de 1963 donde establecía el Sistema Nacional de Comunicaciones (Dunn Cavelty, 2008b, pág. 41). Después de eso, con el mismo propósito, en 1977 el presidente James E. Carter firmó la directiva presidencial *Presidential Directive/National Security Council-24* (PD/NSC-24) (Dunn Cavelty, 2008b).

De acuerdo con estos desarrollos, se estableció un primer vínculo entre las telecomunicaciones y la seguridad nacional en la década de 1960 y 1970, donde se enfatizaba que la comunicación era necesaria para garantizar la capacidad operativa del gobierno y, en especial, su capacidad para actuar de manera oportuna y efectiva en todo momento. Al mismo tiempo, la tecnología de la información durante la década de 1960 y 1970 estuvo vinculada estrechamente a la seguridad nacional, en especial, tras el debate sobre innovación tecnológica y guerra dentro del marco de la Guerra Fría (Dunn Cavelty, 2008b, pág. 42). Por lo tanto, el funcionamiento de los sistemas de comunicación fue visto como “un elemento vital

para garantizar la seguridad y el bienestar de la nación" (Dunn Cavelty, 2008b, pág. 42).

Por otra parte, fue durante los años sesenta y mediados de los setenta cuando los delitos cibernéticos comenzaron a despegar (Dunn Cavelty, 2008b, pág. 45). Asimismo, la discusión sobre el uso indebido de computadoras fue determinada por las nociones de delitos económicos relacionados con las computadoras. No obstante, el problema comenzó a tener una dimensión de seguridad nacional peculiar, puesto que la intrusión informática se vinculó con la amenaza de inteligencia extranjera, principalmente debido a un par de incidentes fuertemente publicitados que involucraron el robo de datos por parte de personas extranjeras (Dunn Cavelty, 2008b, pág. 45).[88]

Justamente, la discusión se enfocaba en cómo podría emplearse la tecnología de la información para ganar conflictos (Dunn Cavelty, 2008b, pág. 43)[89]. No obstante, para la especialista del ETH Zurich, Myriam Dunn Cavelty (2008b, pág. 42) los inicios del debate sobre las amenazas cibernéticas se pueden observar con mayor claridad desde la presidencia de Ronald Reagan (1981-1989). De acuerdo con su análisis, esto sirvió principalmente para el establecimiento de nuevos organismos, instituciones y normas para resolver la problemática, lo que indicaba que las viejas estructuras ya no eran suficientes para abordar el inconveniente (Dunn Cavelty, 2008b, pág. 59). Como muestra de ello, se pueden observar las siguientes normas desarrolladas solamente durante el mandato del presidente Ronald Reagan en relación con la temática:

[88] En relación con este tema, Myryam Dunn Cavelty (2008b) subraya que las primeras actividades calificadas como crimen cibernético no tenían una fuerte dimensión económica, sino que, principalmente eras acciones de inteligencia electrónica. En cuanto a la base comercial de los delitos cibernéticos, estos tienen un ascenso que se relaciona con el nacimiento de internet como plataforma comercial de alcance amplio.

[89] El especialista Alexander Kilmburg (2017) plantea como esta perspectiva ha influido fuertemente en la mentalidad de diversos cuerpos gubernamentales en relación con la seguridad nacional y la información, en especial, sobre la concepción que tiene el gobierno ruso sobre la utilidad de las operaciones de información y su alcance para influir en la toma de decisiones. Para ver un tratamiento más profundo, ver especialmente el capítulo noveno de su investigación.

- Orden Ejecutiva 12356 (EO-12356) (1982), *National Security Information*. Determinaba un sistema uniforme para clasificar, desclasificar y salvaguardar la información de seguridad nacional
- Orden Ejecutiva 12382 (EO-12382) (1982), *President's National Security Telecommunications Advisory Committee*
- *National Security Decision Directive 19* (NSDD-19) (1982), *Protection of Classified National Security Council and Intelligence Information*
- *National Security Decision Directive* (NSDD-84) (1983), *Safeguarding National Security Information*. Solamente la información cuya divulgación dañara los intereses de seguridad nacional de los Estados Unidos puede ser clasificada. Se debe hacer todo lo posible para desclasificar la información que ya no requiere protección en función del interés de la seguridad nacional
- Orden Ejecutiva 12472 (EO-12472) (1984) *Assignment of National Security and Emergency Preparedness Telecommunications Functions*.
- *National Security Decision Directive 145* (NSDD-145) (1984) *National Policy Telecommunications and Automated Information Systems Security*. Proporcionar objetivos, políticas y una estructura organizativa para orientar la dirección de las actividades nacionales dirigidas a salvaguardar los sistemas que procesan o comunican información sensible de explotación, el establecimiento de un mecanismo para el desarrollo de políticas y la asignación de responsabilidades para la implementación de estas. Su objetivo era asegurar la plena participación y cooperación entre los diversos centros tecnológicos del país a través del Poder Ejecutivo, promover una defensa coherente y coordinada contra la amenaza de inteligencia hostil contra sistemas informáticos y la promoción de un enfoque de asociación entre el gobierno y el sector privado en la consecución de estos objetivos.
- *National Security Decision Directive 196* (NSDD-196) (1985) *Counterintelligence/Countermeasure Implementations Task Force*. Requería el establecimiento de un grupo de trabajo para implementar una serie de decisiones políticas diseñadas para limitar la presencia de inteligencia hostil en los Estados Unidos

- *National Security Decision Directive 197* (NSDD-197) (1985) *Reporting Hostile Contacts and Security Awareness*. Mejorar los esfuerzos generales del gobierno para protegerse contra la adquisición ilegal o no autorizada de información y tecnología vitales para el interés nacional por servicios de inteligencia hostiles.
- *Computer Fraud and Abuse Act* (1986). Quien acceda a una computadora a sabiendas sin autorización o exceda el acceso autorizado, y por medio de tal conducta obtiene información que el gobierno de los Estados Unidos ha determinado que requiere protección contra la divulgación no autorizada por razones de defensa nacional o relaciones exteriores, o cualquier dato restringido con la intención o la razón para creer que dicha información así obtenida se usará para dañar a los Estados Unidos, o en beneficio de cualquier nación extranjera será castigada (Dunn Cavelty, 2008b, pág. 63).[90]
- *Computer Security Act* (1987). Tenía la intención de revertir la política ejecutiva que permitía a la comunidad de inteligencia expresar su opinión sobre el desarrollo de estándares técnicos de seguridad para sistemas y redes informáticos no gubernamentales y no clasificados. Asignaba la responsabilidad de desarrollar programas de capacitación de seguridad a nivel gubernamental a la *National Bureau of Standards* (NBS). (Dunn Cavelty, 2008b, pág. 51)

Con base en estas evidencias, se puede reconocer que el gobierno de Ronald Reagan hizo una referencia explícita a los vínculos entre la información y el poder económico y sobre el papel que la información y las nuevas tecnologías de la información debían jugar en el fortalecimiento de la economía estadounidense (Kuehl, 2009, pág. 39). Además, durante este período, la cantidad de atención prestada a los problemas de seguridad informática y las comunicaciones se incrementó en respuesta a los incidentes altamente publicitados, como los virus informáticos y las penetraciones de los sistemas informáticos en red (Dunn Cavelty, 2008b, pág. 54).

[90] Sigue siendo el principal mecanismo legal, a nivel federal, para procesas los delitos informáticos, en especial, los ataques cibernéticos de denegación de servicio (DDoS).

Por ejemplo, en uno de los primeros arrestos de hackers realizado en 1983, el FBI (*Federal Bureau of* Investigation) detuvo a un grupo llamado los '414' con sede en Milwaukee, que llevan el nombre del código telefónico del área local y que se dedicaban alterar códigos telefónicos (Dunn Cavelty, 2008b, pág. 46). Después, para 1988, un estudiante de la Universidad de Cornell, Robert T. Morris, desarrolló una herramienta automatizada de auto-replicación de ataques a la red (*Morris Worm*), que desató una explosión exponencial de copias en las computadoras en la red ARPANET (DeNardis, 2014, pág. 88).[91] Por último, en 1989, Clifford Stoll, un especialista en computación del Laboratorio Nacional Lawrence Berkeley, publicó un libro titulado *The Cuckoo's Egg* (1989), en el que describió un incidente de seguridad relacionado con la incipiente red informática internacional (Dunn Cavelty, 2008b, pág. 48).[92] Después de este incidente, el crimen cibernético virulento y la participación de servicios de inteligencia configuraron lo que se conoce como "la primera amenaza cibernética con implicaciones para la seguridad nacional" (Dunn Cavelty, 2008b, pág. 48). Además, como apunta la experta en gobernanza de infraestructura técnica, Laura DeNardis, "esto fue interpretado por las autoridades gubernamentales estadounidenses como un presagio del alcance y la trascendencia de amenazas técnicas sobre la funcionalidad de la Red" (DeNardis, 2014, pág. 89).[93]

---

[91] Para esa fecha, estaban conectados aproximadamente 60,000 dispositivos a Internet, de los cuales se estima que un diez por ciento fueron infectados. Además, Robert T. Morris fue acusado por haber violado la *Computer Fraud and Abuse Act* (CFAA) (DeNardis, 2014; Dunn Cavelty, 2008b). Este incidente dio gran visibilidad a la Red antes de su exposición comercial, puesto que en ese momento, gran parte de su uso se concentraba en universidades, centros de investigación y agencias gubernamentales estadounidenses. Al menos uno o dos *gusanos* informáticos aparecen cada año en la Red, con una mayor capacidad y velocidad de reproducción. Los más notorios han sido 'Melisa', 'I love you', 'Cod Red', 'Nimbda', 'Slammer', 'Blaster', 'My Doom', 'Stuxnet' y 'Flame'.

[92] Clifford Stoll pasó un año observando las actividades de un pirata informático, cuyo nombre en código era *Hunter*, quien utilizó diversas técnicas con el fin de implantar programas falsos y así poder penetrar en los sistemas informáticos estadounidenses, y de esta manera, obtener información estratégica (Dunn Cavelty, 2008b, pág.49).

[93] Sin embargo, ha quedo pendiente, y continúa siendo una problemática la definición de responsabilidades para prevenir, proteger y combatir los riesgos cibernéticos. Por ejemplo, las compañías de telecomunicación e industrias de la información son responsables de resguardar sus servicios y sus infraestructuras. Los bancos y los negocios comerciales son responsables de salvaguardar las transacciones de sus clientes. Asimismo, hay una responsabilidad individual al momento de proteger información personal. Esto hace que el ecosistema de seguridad del ciberespacio sea complejo e interrelacionado.

Por otra parte, en cuanto al ciberespacio como un ámbito gubernamental normativo resurge a partir de 1998, cuando el ex presidente de los Estados Unidos William Clinton firmó la *Decisión Presidencial Directiva 63* (*Presidential Decision Directive 63*), que establecía una estructura dentro de la Casa Blanca para coordinar acciones gubernamentales y privadas con el propósito de "eliminar cualquier vulnerabilidad significativa a ataques físicos y cibernéticos en infraestructuras críticas, incluyendo especialmente sus sistemas cibernéticos" (U.S. Government, 1998) (Reveron, 2012, págs. 8-9) (U.S. Government White House, 2009).[94] Bajo la administración de William Clinton se reconoció explícitamente el papel que la información tenía para asuntos diplomáticos, militares y económicos.

Dentro de este marco, uno de los primeros documentos que estructuró y organizó el abordaje de la cuestión cibernética en Estados Unidos fue la Ley Federal de Administración de la Seguridad de la Información (2002) (*Federal Information Security Management Act,* FISMA). Como parte de esto, se otorgaban las prerrogativas para la Ley de Gobierno Electrónico (*E-Governance Act*, 2002). Ésta última legislación, establecía un Oficial Federal de Información (*Federal Chief Information Officer*) dentro de la Oficina de Administración y Presupuesto (*Office of Management and Budget*, OMB), responsable de supervisar el uso de tecnología por parte del gobierno, tanto en términos de gasto como de estrategia (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 9). En otras palabras, el objetivo del gobierno estadounidense era estandarizar los procesos de ciberseguridad en todas las agencias gubernamentales de los Estados Unidos. Sin embargo, se han presentado críticas a este esquema debido "a la falta de métricas ampliamente aceptadas, variaciones en la interpretación de las agencias gubernamentales sobre las disposiciones, y la insuficiencia de mecanismos para hacer cumplir las obligaciones" (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 9).

En relación con lo anterior, se puede aseverar que el gobierno de los Estados Unidos ha buscado estar a la vanguardia en el desarrollo de políticas y estrategias de ciberseguridad. Para lograr esto, surgió la *Estrategia Nacional de Seguridad del*

[94] La directiva fue actualizada posteriormente por la Estrategia Nacional de Seguridad del Ciberespacio de 2003 (Reveron 2012).

Ciberespacio del 2003 (*National Strategy to Secure Cyberspace*) (Kuehl, 2009, pág. 25), la primera estrategia nacional integral de ciberseguridad (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 7). En este documento se definía al ciberespacio como "el sistema nervioso que controla los sistemas de una nación, compuesto de miles de computadoras, servidores, enrutadores, interruptores y cables de fibra óptica que permiten el correcto funcionamiento de infraestructuras críticas" (White House, 2003). Asimismo, la *Estrategia Nacional de Seguridad del Ciberespacio* (2003) establecía tres objetivos estratégicos para la seguridad nacional del ciberespacio: *1)* prevenir los ataques cibernéticos contra las infraestructuras críticas nacionales; *2)* reducir la vulnerabilidad nacional a los ciberataques y; *3)* minimizar el daño y el tiempo de recuperación de los ciberataques que ocurran (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). Aunado a ello, fue publicada en 2003 la *Estrategia Nacional para la Protección de Infraestructuras Crítica y Activos Claves* (*National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*) (U.S. Department of Homeland Security, 2009).

Dentro de esta perspectiva, en 2005, la *Estrategia de Defensa Nacional* (*National Defense Stategy*) identificó el ciberespacio como "un nuevo teatro de operaciones y evaluó las operaciones del ciberespacio como un desafío potencialmente disruptivo (Reveron, 2012, pág. 9). Por otra parte, cabe considerar que, para atajar las deficiencias en la coordinación e implementación de políticas de ciberseguridad, en el año 2008, durante el gobierno del presidente George W. Bush, se emitieron la *Directiva Presidencial de Seguridad Nacional 54* (*National Security Presidential Directive 54*) y la *Directiva Presidencial sobre Seguridad Interna 23* (*Homeland Security Presidential Directive 23*) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 10). Igualmente, fueron signadas la *Orden Ejecutiva 13355* en 2004, que buscaba el fortalecimiento de la comunidad de inteligencia y la *Orden Ejecutiva 13470* (2008), que buscaba brindar mayores atribuciones al Director Nacional de Inteligencia como herramientas para tener mayor control y vigilancia de las actividades en el ciberespacio (Dunn Cavelty, 2008b). Bajo estas directrices, en ese momento, el gobierno estadounidense consideraba al ciberespacio como "una red interdependiente de infraestructuras de tecnologías de la información, que incluye

Internet, redes de telecomunicaciones, sistemas computacionales, procesadores y controles de industrias críticas" (Kuehl, 2009, pág. 26), las cuales debían ser aseguradas y controladas por el gobierno estadounidense.

Cabe resaltar que, estas directivas autorizaban al Departamento de Seguridad Interna (*Department of Homeland Security*) junto con la Oficina de Administración y Presupuesto (OMB) desarrollar estándares mínimos de operación para la protección de las redes informáticas civiles de carácter gubernamental (U.S. Government White House, 2009) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 10). Asimismo, subrayaban el enfoque general del gobierno para garantizar la ciberseguridad, que posteriormente se incorporó en la *Iniciativa Nacional de Ciberseguridad Integral* (*Comprehensive National Cybersecurity* Initiative, CNCI) (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). (U.S. Government White House, 2009). Con base en esto, para algunos analistas "los documentos estratégicos que han conducido la política de ciberseguridad asignan papeles y responsabilidades de alto nivel a las entidades del gobierno federal, pero dejan los detalles de la implementación a discreción de las diversas agencias gubernamentales" (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 15), lo que ha generado problemas para la ejecución de las diversas estrategias.

Sin embargo, quizá la ley más controversial sobre las acciones gubernamentales en el ciberespacio ha sido la *Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act, PATRIOT Act* de 2001. Esta ley permitía el acceso sin restricciones a los cuerpos de inteligencia, sin intervención de las agencias de aplicación de la ley de los Estados Unidos, "indagar en registros telefónicos, financieros, e información electrónica sin una orden judicial, esto con el fin de proteger a la ciudadanía del terrorismo internacional o actividades de inteligencia clandestinas" (Arreola García, 2015, pág. 175). Debido a fuertes críticas nacionales e internacionales sobre las violaciones sistemáticas a derechos humanos sobre las atribuciones de esta legislación, se han hecho varias modificaciones y adecuaciones a su contenido (Arreola García, 2015, pág. 176).

Por otra parte, la administración del presidente Barack Obama convirtió la lucha contra el proteccionismo digital, el robo cibernético y el aumento de capacidades

ofensivas cibernéticas en una de sus prioridades gubernamentales (Aaronson S. A., 2016; Sanger D. , 2012). Durante su mandato, en el año 2009, se declaró el mes de octubre como el mes nacional de concientización sobre la ciberseguridad debido a "la creciente dependencia de la nación en las tecnologías cibernéticas y de la información, junto con la creciente amenaza de ataques cibernéticos maliciosos y la pérdida de privacidad" (White House, 2009).

En consecuencia, se ha presentado un desarrollo legislativo abundante. Por ejemplo, la *National Security Strategy* del 2010, que para algunos especialistas fue "la primera estrategia de seguridad nacional estadounidense" dedicó una atención sustancial a las amenazas informáticas (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 8). Esta ley, a su vez, representaba un cambio en la tipificación de las amenazas cibernéticas por el gobierno federal de los Estados Unidos de América, que ya no sólo enfatizaba las actividades terroristas digitales en el ámbito digital como la fuente más peligrosa para la seguridad nacional, sino que a aquellas actividades hechas por agentes estatales o por actores no estatales con el apoyo y patrocinio de un Estado nacional, con objetivos políticos y económicos de carácter internacional se tipificó como las más riesgosa (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). Es por ello que, a partir de ese momento, algunos analistas han considerado que "la ciberseguridad ha sido un tema complicado y en ocasiones espinoso en las relaciones bilaterales entre Estados Unidos y otros países durante y desde la administración de Barack Obama" (Lu C. , 2017).

Por ejemplo, en, 2011, la Casa Blanca lanzó la *Estrategia Internacional para el Ciberespacio* (*International Strategy for Cyberspace*) como un enfoque para relacionarse con otros socios internacionales y comunicar sus prioridades nacionales (Joyner, 2012). En dicho documento se enfatizaba que, "Estados Unidos trabajará internacionalmente para promover una infraestructura de información y comunicación abierta, interoperable, segura y confiable que respalde el comercio internacional, fortalezca la seguridad internacional y fomente la libre expresión y la innovación" (U.S. Government White House, 2011). A su vez, para la consecución de estos objetivos, se mencionaba que el gobierno estadounidense "construirá y mantendrá un entorno en el que las normas de comportamiento responsable guíen

las acciones del Estado, mantengan asociaciones y apoyen el estado de derecho en el ciberespacio" (U.S. Government White House, 2011).

Aunado a esto, otra de las normas representativas de la administración del presidente Barack Obama fue la emisión de la *Cyber Intellgence Sharing and Protection Act* en 2011 (U.S. House of Representatives, 2011). Bajo esta legislación la principal prerrogativa era el intercambio de información entre el gobierno y las empresas tecnológicas con motivos de inteligencia (U.S. House of Representatives, 2011) Asimismo, su propósito era garantizar la integridad, confidencialidad y disponibilidad redes informáticas bajo la identificación temprana de amenazas cibernéticas (U.S. House of Representatives, 2011). De la misma manera, para el 2011, la *National Defense Strategy* estimó que "la amenaza cibernética se ha expandido y se ha exacerbado por la falta de normas internacionales, las dificultades de atribución, las bajas barreras de entrada y la relativa facilidad para desarrollar capacidades ofensivas potentes" (Chairman of the Joint Chiefs of Staff, 2011). Resulta así mismo interesante que, en ese mismo año, la rama ejecutiva del gobierno de los Estados Unidos declaró que "un incidente cibernético se considera similar a un acto de guerra, punible a través de medios militares convencionales" (White House, 2011).

A razón de esto, en octubre de 2012, se emitió la Directiva de Política Presidencial 20 (*Presidential Policy Directive 20*), la cual autorizaba la ejecución de operaciones cibernéticas ofensivas bajo ciertas condiciones y únicamente después de una cuidadosa investigación interinstitucional (Valeriano & Jensen, 2019). En relación con lo anterior, algunos observadores como David E. Sanger y Kim Zetter han considerado ese año como el parteaguas para el desarrollo de armas cibernéticas, así como el presagio de una nueva forma de guerra y una prueba de que los ataques cibernéticos podrían causar un daño físico significativo (Sanger D. E., 2012; Zetter, 2014).

En ese mismo tenor, Kim Zetter considera que programas dañinos como Stuxnet o similares pudieran convertirse en armas de los 'débiles' contra los sistemas de

control industrial en las grandes economías industrializadas (Zetter, 2014).[95] Asimismo, después del surgimiento de Stuxnet, algunos analistas de seguridad han advertido que los ataques cibernéticos futuros podrían tener efectos de gran alcance, incluida una carrera de armas cibernéticas entre los Estados, inhibiendo el desarrollo de normas para contener las operaciones ofensivas del ciberespacio (Rovner & Moore, 2017, pág. 193; Landale & Meinrath, 2015). Sin embargo, algunos autores más escépticos señalan que muy pocos Estados y actores no estatales tienen recursos financieros y tecnológicos para orquestar un ataque tan complicado (Lindsay J. R., 2013).

En efecto, esto puede explicar por qué la guía de defensa estratégica de 2012 identificó que una de las misiones principales de las fuerzas armadas de los Estados Unidos debía ser la operación eficaz en el ciberespacio (Reveron, 2012, pág. 9). Además, para 2015, la *National Security Strategy* reconoció el peligro creciente de ataques cibernéticos perturbadores e incluso destructivos, y comunicó que la intención del gobierno de los Estados Unidos era "fortalecer la ciberseguridad de la infraestructura crítica, aumentar la inversión en capacidades cibernéticas e imponer altos costos a los actores cibernéticos maliciosos" (U.S. Government White House, 2015). Cabe señalar que el texto se enfocaba particularmente en el papel gubernamental estadounidense en la promoción de normas internacionales en el ciberespacio (U.S. Government White House, 2015).

A pesar de estos esfuerzos, es importante destacar que, desde el ámbito gubernamental estadounidense, en diferentes escalas y en diversos organismos existen aproximadamente más de 50 estatutos que abordan diversos aspectos de la ciberseguridad. No obstante, no existe una legislación general o una estrategia nacional de seguridad cibernética que sintetice estos documentos o describa exhaustivamente la estrategia del gobierno de los Estados Unidos de América (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 7).

[95] Cabe subrayar que partir de finales de 2009, durante aproximadamente dos meses, un programa supuestamente desarrollado por los cuerpos de inteligencia de Estados Unidos e Israel llamado 'Stuxnet' creó interrupciones y averías graves al funcionamiento de las centrífugas iraníes en la planta de enriquecimiento de uranio de Natanz. A su vez, el uso de Stuxnet provocó un ataque en forma de represalia por parte de Irán contra los bancos estadounidenses y la compañía petrolera Saudi Aramco (Rovner & Moore, 2017, pág. 191)

Sin embargo, como resultado este proceso, se ha emitido la *National Cyber Strategy* el 20 de septiembre de 2018, la primera estrategia cibernética totalmente articulada e integral para el gobierno de los Estados Unidos. Con ello, el aparato gubernamental estadounidense "reconoce el peligro que las amenazas cibernéticas representan para la economía e infraestructura pública […], a medida que estas amenazas continúan aumentado año con año, el gobierno federal sigue comprometido con reforzar las defensas cibernéticas de la nación y así fortalecer la seguridad nacional" (White House, 2018a).

No obstante, más que ser un plan detallado, el documento es una síntesis de algunas acciones que el Estado realiza en relación con las actividades cibernéticas de seguridad. Además, llama la atención que dada la 'complejidad' del fenómeno de ciberseguridad que se hace presente en la retórica de otras iniciativas, el documento hace poco detalle sobre las estrategias y tácticas para lograr sus objetivos. Más aún, para algunos especialistas, a pesar de lo cuantioso de estas iniciativas gubernamentales, "no existe un plan coherente para reducir la actividad maliciosa en el ciberespacio". (Reveron, 2012, pág. 9). Por otro lado, algunos expertos mencionan que la problemática reside en que "la mayoría de los documentos existentes abordan las prioridades nacionales de ciberseguridad desde áreas muy restringidas, lo que conduce a una variación en términos de prioridades y estructura" (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 7). Asimismo, también se recalca que, dadas las inquietudes legales sobre la privacidad, "no está totalmente claro qué papel pueden y deben desempeñar las diferentes dependencias y agencias gubernamentales en la defensa y protección de las redes informáticas" (Reveron, 2012, pág. 9).

Por otra parte, la estrategia reciente del gobierno de Donald J. Trump se basa en la creencia de que la ofensiva es una forma efectiva y fácil de evitar que los Estados rivales pueden *hackear* a Estados Unidos (Valeriano & Jensen, 2019). A razón de esto, en abril de 2018, el *U.S. Cyber Command* lanzó una nueva declaración que pide una acción perseverante para mantener la superioridad cibernética de los Estados Unidos (U.S. Cyber Command, 2018). De acuerdo con el documento *Achieve and Maintain Cyberspace Superiority: Command Vision for*

US Cyber Command, “ceder terreno digital a adversarios estatales y no estatales puede socavar no sólo el poder estadounidense, sino a la infraestructura digital global” (U.S. Cyber Command, 2018).

Asimismo, *U.S. Cyber Command* sostiene que Estados Unidos necesita una estrategia para el ciberespacio más agresiva, la cual prevé una nueva fase de acciones persistentes que busquen mantener la superioridad cibernética (Valeriano & Jensen, 2019). Además, menciona que las operaciones cibernéticas de los Estados Unidos “influirán en el cálculo de nuestros adversarios, desalentarán la agresión y aclararán la distinción entre comportamiento aceptable e inaceptable en el ciberespacio” y, como resultado, “mejorarán la seguridad y la estabilidad del ciberespacio” (U.S. Cyber Command, 2018).

A su vez, estas intenciones se vinculan estrechamente con la *Estrategia de Defensa Nacional* de 2018 (*National Defense Strategy*) (U.S. Department of Defense, 2018) y con la *Estrategia de Seguridad Nacional* de 2018 (*National Security Strategy*), la cual prevé una competencia constante entre las grandes potencias como la norma conductual en el siglo XXI. En este modelo, el ciberespacio se convierte en otro dominio en el que los Estados Unidos deben alcanzar el dominio de los bienes comunes para garantizar el orden internacional (Valeriano & Jensen, 2019). Como bien lo afirman los especialistas Brandon Valeriano y Benjamin Jensen (2019) “este enfoque ve cada vez más la preeminencia como el único camino viable hacia la seguridad”. Por último, este recuento del entorno jurídico estadounidense en relación con la ciberseguridad también muestra que la orientación gubernamental sobre este fenómeno incipiente busca ser cada vez más coordinada, condensada y centralizada. Sin embargo, bajo esta revisión queda poco claro si esta serie de instrumentos legales son efectivos al momento de reducir las amenazas cibernéticas y/o brindar la seguridad nacional en el ciberespacio.

5.4 Prácticas y narrativas de ciberseguridad estadounidenses en el espacio digital

Cabe señalar que los gobernantes estadounidenses cuentan una concepción regularmente similar sobre el ciberespacio a diferencia de la empleada por los

teóricos militares y civiles en la República Popular de China. Por ejemplo, en 2006, Michael Wynne, el entonces secretario de la Fuerza Aérea de los Estados Unidos declaró "el ciberespacio es un dominio en el que la Fuerza Aérea vuela y lucha" (Rid, 2012, pág. 6). Del mismo modo, en 2008, la Estrategia de Defensa Nacional (*National Defense Strategy*) exploró las implicaciones que pueden tener pequeños grupos o individuos sobre el ciberespacio. De acuerdo con este documento, estos "pueden atacar puntos vulnerables en el ciberespacio e interrumpir el comercio y la vida cotidiana, causando daños económicos, comprometiendo información y materiales confidenciales e interrumpiendo servicios críticos como las redes de energía e información (U.S. Department of Defense, 2008).

Por su parte, en 2009, el Consejo Nacional de Investigación (*National Research Council*) realizó un estudio para delimitar y definir lo que se consideraba como un ataque cibernético (Singer & Friedman, 2014, pág. 68). Dentro de este documento, se les definía como "acciones deliberadas para alterar, interrumpir, engañar, degradar o destruir sistemas informáticos o redes o la información y programas residentes o en tránsito por estos sistemas o redes" (Owens, Dam, & Lin, 2009; U.S. House of Representatives, 2011). Además, recalcaba que "en la competencia cibernética, aquella entidad que domine las capacidades ofensivas tendrá ventajas sobre sus competidores" (Owens, Dam, & Lin, 2009).

Como consecuencia, esta suposición es lo que "ha favorecido un impulso hacia un aumento en el gasto presupuestal para el desarrollo de capacidades cibernéticas ofensivas militares" (Singer & Friedman, 2014, pág. 154). A su vez, este pensamiento detrás de la ventaja ofensiva es que "será más barato y más fácil atacar los sistemas de información que detectar y defenderse contra los ataques" (Owens, Dam, & Lin, 2009).[96] Por otra parte, en 2010, en un artículo de opinión en la revista *Foreign Affairs*, el secretario adjunto de Defensa de los Estados Unidos de aquel momento, William J. Lynn, mencionó que "aunque el ciberespacio es un

[96] Supuestamente, bajo esta perspectiva, los atacantes tienen la iniciativa y la ventaja de poder elegir la hora y el lugar de su ataque, mientras que el defensor debe estar alerta de manera constante.

dominio hecho por el humano, se ha vuelto tan crítico para las operaciones militares como la tierra, el mar, el aire, y el espacio exterior" (Lynn, 2010, pág. 101).

Asimismo, en febrero de 2011, el entonces director de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés, *Central Intelligence Agency*, Leon Panetta advirtió al *House of Permanent Select Committee on Intelligence* que "el próximo Pearl Harbor podría ser un ataque cibernético" (Rid, 2012, pág. 6). Su antecesor, también ex director de la CIA y de la NSA (*National Security Agency*), Michael Hayden subrayaba que "rara vez algo tan importante ha sido discutido con tan poca claridad y comprensión que lo cibernético" (Hayden, 2011, pág. 3).

Dentro de esa tendencia, el ex director del Departamento de Seguridad Nacional Tom Ridge mencionó que "los terroristas pueden sentarse en una computadora conectada a una red y crear un caos en el mundo, no necesariamente necesitan bombas o explosivos para paralizar un sector de la economía o cerrar una red eléctrica" (Ridge, 2002). Incluso, otros ex funcionarios como Richard Clarke, antiguo asesor cibernético de la Casa Blanca, ha anunciado calamidades relacionadas con el ciberespacio "que podrían hacer palidecer a otras anteriores como el 9/11" (Rid, 2012, pág. 6) (Clarke & Knake, 2010, pág. 261).

Sin embargo, para un enfoque analítico, quizá el mayor problema sobre la narrativa y la estrategia cibernética del gobierno de los Estados Unidos es si pone demasiado énfasis en la táctica ofensiva (Owens, Dam, & Lin, 2009; Klimburg, 2017). En buena medida, esta tendencia reside en el atractivo intrínseco que tienen conceptos como "guerra cibernética", "explotación de software", "catástrofe digital" o "guerreros cibernéticos" sobre los cuerpos militares, puesto que estos son más convenientes para realizar el proceso de securitización y, que no pueden reducirse a una simple retórica, sino que implican la posibilidad de una amplia movilización de recursos para apoyar dicha narrativa y que sea apoyada y aceptada por la sociedad (Bigo, 1994) (Huysmans, 1998).

Además, así como sucedió a finales de la década de 1980, varios incidentes cibernéticos de alto perfil han centrado la atención de los medios de comunicación y los responsables políticos de la ciberseguridad sobre posibles escenarios catastróficos. Estos han incluido dos ataques cibernéticos a gran escala atribuidos

a Rusia: uno contra Estonia en 2007 (Davis, 2007; Blank, 2008); y uno contra Georgia que coincidió con una invasión terrestre en 2008 (Danchev, 2008); en enero de 2010 las acusaciones hechas por Google sobre ataques cibernéticos chinos en su contra desencadenaron una respuesta del más alto nivel gubernamental estadounidense, representado por el discurso de la entonces Secretaria del Departamento Estado Hillary R. Clinton sobre la libertad en Internet (Clinton, 2010).

Después, en el 2012, el desarrollo de códigos maliciosos persistentes como *Stuxnet*, que causó daños a las centrífugas iraníes en la planta de enriquecimiento de uranio de Natanz (Sanger D. E., 2012; Zetter, 2014). Luego, en 2013 vinieron las revelaciones de Edward Snowden sobre los programas de inteligencia como PRISM que ayudaban a las agencias como la NSA y el FBI a recopilar datos encriptados de los usuarios de compañías como Google, Microsoft, Facebook, Yahoo!, y que además les obligaban a adoptar protocolos de cifrados débiles.[97] Además, en 2016, 3 mil millones de cuentas de la empresa Yahoo! fueron comprometidas, calificadas como una de las transgresiones de seguridad informática más grande de la historia (Oath, 2017). A su vez, en 2016, la empresa Uber reportó que los datos de 57 millones de conductores y usuarios fueron robados (Khosrowshahi, 2017). Por último, en 2017, los datos personales de 147 millones de consumidores manejados por la compañía de análisis Equifax fueron robados (Equifax, 2018). En la tabla 5.2 se pueden observar algunos de los sucesos de ciberseguridad empresarial más grande en relación con la cantidad de usuarios comprometidos.

Tabla. 5.2 Mayores sucesos de ciberseguridad empresarial por la cantidad de usuarios comprometidos

Empresa	**Cantidad de usuarios comprometidos**	**Año**
1. Yahoo!	3 mil millones	2013
2. Marriot	500 millones	2014-2018

[97] PRISM es un programa que busca apoderarse de toda la información guardada y enviada a través de dispositivos digitales, lo que se llama en el argot informático *data mining* (minado de datos).

3. Adult FriendFinder	412 millones	2016
4. MySpace	360 millones	2016
5. Under Armor	150 millones	2018
6. Equifax	145 millones	2017
7. eBay	145 millones	2014
8. Target	110 millones	2013
9. Heartland Payment Systems	100 millones	2018
10. LinkedIn	100 millones	2012

Fuente: (CISCO/Cybersecurity Ventures, 2019)

Por otro lado, los supuestos defensivos como “ingeniería de seguridad”, “cifrado apropiado” y “protección de cadenas de suministro”, difícilmente generarían un proceso de securitización, en el cual, los agentes gubernamentales, tendrían una complejidad mayor para justificar la aplicación de medidas excepcionales y la aceptación de éstas por parte de la ciudadanía (Buzan, Waever, & de Wilde, 1998, pág. 24). Como muestra, en 2016, el gobierno estadounidense se volvió mucho más específico en sus preocupaciones sobre las políticas digitales de otros gobiernos, poniendo especial énfasis en las acciones desempeñadas por la República Popular de China, señalando que éste usa argumentos de seguridad nacional (lo que China denomina soberanía de la información o soberanía cibernética) para justificar la censura, las políticas industriales, el robo cibernético y el proteccionismo comercial.

Sobre el asunto, algunos expertos mencionan que no únicamente el gobierno chino realiza actividades que obstaculizan el ciberespacio como mecanismo de control a través de diversas justificaciones (Deibert R. , Palfrey, Rohozinski, & Zittrain, 2010), sino que el sistema de inteligencia/espionaje estadounidense “también es una ‘herramienta’ que permite resguardar la seguridad nacional y, al mismo tiempo, preservar el dominio y la hegemonía de los Estados Unidos en el ámbito internacional” (Arreola García, 2015, pág. 9). Con base en lo revisado, se puede aseverar que en las prácticas de *securitización* del acceso al espacio digital,

el gobierno estadounidense legitima y justifica sus acciones a través de referencias y testimonios que enfatizan la protección de activos relacionados con la seguridad nacional

Otros analistas identifican que los gobiernos de Estados Unidos y China están ingresando en una competencia creciente, tal vez al borde del conflicto, donde el punto focal no es la fuerza militar o la expansión territorial, sino que este conflicto es “sobre el control de las palancas modernas del poder: normas e instituciones globales, estándares relacionado con el comercio y tecnología” (Lewis, 2018; Segal A. , 2018). No obstante, “Estados Unidos tiene ventajas innatas en cualquier carrera tecnológica, ya que cuenta con la base de investigación más sólida del mundo, empresas líderes en tecnología y una cultura innovadora difícil de igualar” (Lewis, 2018).

De igual manera, en el caso del gobierno de los Estados Unidos, hay analistas que identifican cinco prioridades nacionales para alcanzar el objetivo de la seguridad nacional en el espacio cibernético: *1)* asegurar las redes y los sistemas informáticos federales; *2)* desarrollar un sistema de respuesta; *3)* establecer un programa de reducción de amenazas y vulnerabilidad; *4)* iniciar un programa de concientización y capacitación en seguridad cibernética; *5)* desarrollar un sistema de cooperación internacional. (Aaronson S. A., 2016). Es por eso, que la conceptualización que Estados Unidos tenga sobre sí mismo en el ámbito internacional es un reflejo que influye directamente de sus expectativas en el sistema internacional cibernético, las cuales son ser un actor preponderante, que tenga voz y capacidad de decisión para (re)establecer las normas de conducta en el ciberespacio global.

Además, como se ha podido constatar, estos actos discursivos de los dirigentes estadounidenses no se han reducido a acciones verbales o retóricas, sino que han sido acompañadas por la implementación y ejecución de actividades institucionales y presupuestarias para su realización. Con base en ello, el gobierno estadounidense ha tratado de presentar a la sociedad el fenómeno de la ciberseguridad como un *riesgo*, para de esta manera justificar la emisión de leyes, normas y presupuestos para contener dicho peligro, incluso si este conjunto jurídico

transgrede otras normatividades nacionales e internacionales. Por tanto, así como en el caso de la República Popular de China, para el gobierno de Estados Unidos la ciberseguridad tiene un efecto directo en su comportamiento internacional, a través de una restructuración de funciones gubernamentales, el desarrollo de legislaciones y normatividades específicas para el tratamiento del tema, lo cual verifica la hipótesis de este trabajo de investigación.

Capítulo 6. La competencia en el ámbito de la ciberseguridad entre China y Estados Unidos

Introducción

Como se puede observar en los capítulos precedentes, la ciberseguridad se ha convertido en una prioridad estatal a partir de la primera década del siglo XXI. Junto con este desarrollo, también se ha presentado una vinculación estrecha con temáticas de seguridad nacional. Este proceso se ha hecho evidente a través de dos mecanismos. Primeramente, las acciones gubernamentales se han justificado debido a la ubicuidad de puntos que pueden ser vulnerables a un ataque cibernético, lo que se ha traducido en la necesidad de proteger y salvaguardar la funcionalidad de los sistemas de información global. En segundo lugar, la narrativa estatal se ha abocado a encumbrar el alza de incidentes ofensivos/agresivos cibernéticos, lo que genera que sus acciones sean un imperativo para tratar de combatirlos y disminuirlos. No obstante, algunos datos sobre las acciones cibernéticas demuestran que la cantidad de ataques cibernéticos no es tan elevada como lo señala el discurso gubernamental.

Si bien es cierto que las cifras y la metodología de medición de éstos se encuentra bajo debate, algunas aproximaciones pueden dar luz sobre la dimensión y superficie que ocupa el fenómeno de la ciberseguridad en su escala global. Por ejemplo, los investigadores Ryan C. Maness, Brandon Valeriano y Benjamin Jensen han documentado que, de 2000 a 2016 se han registrado 272 operaciones cibernéticas entre entidades estatales (Maness, Valeriano, & Jensen, 2017). Estos ataques los han clasificado con base en los mecanismos utilizados y la pretensión de objetivos de cada uno de los entes gubernamentales. Por un lado, el 32.7% fueron incidentes que buscaban interrumpir, alterar o perturbar un sistema o red para conseguir una posición temporal de ventaja estratégica (89 incidentes). Por otro lado, el 54.4% fueron actividades relacionadas con espionaje, éstas buscan alterar el balance de información u obtener alguna información sensible para poseer recursos de negociación diplomática (148 incidentes). Por último, el 12.9% fueron actos que buscaban degradar, arruinar o destruir algún aspecto de las redes,

sistemas o funciones de información de un adversario (35 incidentes) (Maness, Valeriano, & Jensen, 2017).

Bajo este esquema, el *Council on Foreign Relations* también ha desarrollado una herramienta para indagar sobre el desarrollo de acciones cibernéticas, llamada *Cyber Operation Tracker*. De acuerdo con este instrumento, de 2005 a 2016, se han perpetrado 200 ataques cibernéticos, los cuales involucran la participación de al menos 16 Estados diferentes (Council on Foreign Relations, 2019). Con base en estas evidencias, Maness, Valeriano y Jensen concluyen que "el ciberespacio es un dominio restringido, con pocos ataques agresivos que buscan un impacto dramático y decisivo" (Maness, Valeriano, & Jensen, 2017). Entonces, surge la interrogante, ¿con qué fin los Estados utilizan las actividades cibernéticas? De acuerdo con lo observado a lo largo de este trabajo, los Estados utilizan la ciberseguridad como una herramienta para proyectar una posición de dominio en una competencia intermodal a largo plazo. Además, han identificado a la ciberseguridad como un medio para recuperar espacios de acción e influencia en la cual los gobiernos habían perdido preponderancia en relación con otros agentes.

A razón de lo anterior, este capítulo realiza un tratamiento comparativo de los esquemas gubernamentales de ciberseguridad abordados con anterioridad en otros capítulos, con el objeto de conocer qué efectos tienen las actividades cibernéticas sobre la concepción de la seguridad nacional. En seguida, se presentan algunas delimitaciones conceptuales sobre la competencia internacional, basadas en la concepción de una disputa hegemónica dentro de un contexto trans-histórico particular y, qué función tiene la ciberseguridad en esta apuesta competitiva. En seguida, se desmenuzan brevemente los proyectos de ciberseguridad chinos y estadounidenses como herramientas de este ciclo competitivo, lo que a la postre se traduce en un tipo particular de reglas, normas y principios que enarbola cada programa ciberespacial. Con base en esto, se describe la manera en la que buscan establecer y configurar la agenda internacional del fenómeno bajo ideas y estrategias específicas. Para finalizar, en la última sección de este capítulo se presentan los principales hallazgos y limitantes que enfrentó este trabajo de investigación.

6.1 El papel de la ciberseguridad sobre visiones del orden internacional en competencia

Como se ha podido constatar en los capítulos precursores, la principal diferencia entre la República Popular de China y los Estados Unidos de América es su apreciación del concepto de ciberseguridad. Para el gobierno chino, la ciberseguridad involucra aspectos que pueden fortalecer su ejercicio gubernamental y, a su vez, permitan el desarrollo y el bienestar general de su conjunto social. Asimismo, pretenden utilizar la ciberseguridad como herramienta para la disminución de en un alto porcentaje de puntos de riesgo que puedan vulnerar la legitimidad y margen de acción política de su dirigencia. Es por ello, el enfoque gubernamental chino de ciberseguridad se califica como un programa de ciberseguridad nacional enfocado en aspectos socio-políticos más que en aspectos técnicos.

Por su parte, los funcionarios estadounidenses, también lo consideran como un dispositivo en el robustecimiento de su ejercicio gubernamental. No obstante, los funcionarios públicos de Estados Unidos han centrado su atención en fortalecer una concepción de la ciberseguridad bajo un lente más técnico. Esto se debe a que poseen los recursos y capacidades para realizarlo. Además, el gobierno estadounidense busca tener una mejor coordinación intragubernamental a través de una mejora en los preceptos técnicos de la seguridad de la información, lo que indirectamente beneficia a su población en general.

A pesar de las diferencias enunciadas anteriormente, se puede deducir que ambos proyectos también tienen elementos que comparten. Por ejemplo, tanto el enfoque chino como estadounidense de ciberseguridad tienen en común la premisa de que el mantenimiento de ésta es de suma importancia para el desarrollo y estabilidad de sus sociedades. Además, sus enfoques estratégicos se cimientan en la satisfacción de sus intereses nacionales, los cuales ponen un fuerte acento en la preeminencia digital. Con base en esto, ambos gobiernos enarbolan sus estrategias digitales de seguridad como el arquetipo a emular por otras entidades

gubernamentales a nivel internacional. Sin embargo, ambos casos también pueden clasificarse como particularidades de programas de ciberseguridad a nivel global.

En primer lugar, porque los gobiernos chino y estadounidense cuentan con una imbricación amplia entre sectores de operación en la implementación y ejecución de una política de ciberseguridad comprehensiva y de largo alcance. En segundo lugar, las acciones estatales sino-estadounidenses en materia de ciberseguridad pretenden posicionarse como *primus inter pares*, algo que difícilmente otros pueden alcanzar, salvo algunas pequeñas excepciones. En ambos casos, distintos agentes no gubernamentales ayudan a apuntalar esas visiones que buscan mantener o alcanzar una posición de privilegio en el desarrollo tecnológico. Por último, cabe señalar que las diferencias entre la perspectiva china y estadounidense en el marco de la ciberseguridad radican en las formas y medios de lograr su cometido.

Cabe resaltar que estos dos ejemplos gubernamentales no son los únicos que están conduciendo estrategias de ciberseguridad basadas en alguno de los enfoques enarbolados tanto por Estados Unidos de América como por la República Popular de China. Por ejemplo, países como Reino Unido, Alemania, Australia y algunos gobiernos de la Unión Europea han buscado mantener el *statu quo* en la gestión y gobernanza del ciberespacio, especialmente a lo que se refiere a los procedimientos y protocolos de seguridad de la información. Además, cada uno de estos Estados ha emitido estrategias de ciberseguridad nacional, creando cuerpos institucionales para realizar procedimientos de seguridad de la información eficaces dentro de sus respectivas jurisdicciones, y han invertido cuantiosos recursos para desarrollar herramientas de ciberseguridad sofisticadas a través del desarrollo de enfoques propios sobre la importancia de la funcionalidad del sistema cibernético global.

Aunado a lo anterior, esos Estados apoyan la perspectiva estadounidense sobre un enfoque de gobernabilidad de la ciberseguridad que pone el peso de la implementación y ejecución de tareas y responsabilidades bajo un esquema de múltiples partes interesadas (*multistakeholder approach*), entre agentes gubernamentales, privados, civiles y militares. No obstante, la divergencia de estos

gobiernos con su contraparte estadounidense radica en cuanto las instituciones participantes, la compresión de áreas prioritarias y los mecanismos para gestionar los riesgos cibernéticos de seguridad.

Es importante subrayar que no sólo la República Popular de China es el único país que apuesta por un proyecto de seguridad cibernética basado en una concepción apegada a una mayor intervención estatal. Algunos países, como Brasil, India, Rusia, Corea del Sur, e Israel conciben que la mejor manera de afrontar la vasta cantidad de problemas de ciberseguridad es a través de la creación de jurisdicciones, normas y reglamentaciones soberanas sobre el flujo de información y contenido en el ciberespacio (*cyber-sovereignty*). No obstante, la diferencia en este bloque de Estados es sobre qué debe ser regulado y, bajo que estándares y preceptos.

Con base en esto, se seleccionó a los Estados Unidos de América y a la República Popular de China como sujetos de estudio, pues representan formas paradigmáticas de dos visiones que están fungiendo como un faro orientador para las acciones de otros Estados soberanos sobre la participación y el tratamiento del fenómeno de ciberseguridad a nivel global. De cierta forma, estas visiones se han envuelto bajo un debate sobre la gestión de los protocolos de seguridad que permiten el funcionamiento adecuado de la estructura ciberespacial, y que solventan la mayoría de interacciones de una sociedad que es más propensa y dependiente de las tecnologías de información y comunicación.

A su vez, esto refleja la situación de dos cuestiones de carácter estructural a nivel internacional: primero, la conformación de un orden internacional complejo, confuso e impreciso producido por una intensa competencia ideacional y material y; segundo, el papel que la tecnología juega en las interacciones sociales, políticas, estratégicas y económicas que generan un desarrollo de prácticas y los valores particulares que sirven para recrear un ámbito social particular (Escobar, 1994). Históricamente, en la mayoría de las sociedades es posible encontrar conjuntos de ideas en competencia, pero en pro de una acción efectiva suele tratar de dominar una ortodoxia en la jerarquía de tales conjuntos (Legro, 2000, pág. 258).

Cabe recalcar que las ideas colectivas son intersubjetivas y distintas de las creencias individuales; típicamente se encarnan en símbolos, discursos e instituciones (Legro, 2000, pág. 258). Éstas son fundamentales pues "no sólo revisten psicológica, simbólica y moralmente la participación de los actores en su lucha por el poder" (Morgenthau, 1948), "sino que son una fuente de poder por sí mismas pues configuran discursos específicos que contribuyen a un orden particular" (Morales, 2018, pág. 458). Los agentes (individuales o grupales) y sus interacciones influyen sobre las ideas colectivas, pero también tienen que confrontar esas ideas como "hechos" (Legro, 2000, pág. 258).

Ese cambio, se puede presentar en dos etapas: primero, los actores sociales deben de alguna manera coincidir, explícita o tácitamente, en que la antigua estructura ideacional es inadecuada, provocando así su colapso; segundo, los actores tienen que consolidar algún conjunto de ideas nuevo que sirva de reemplazo (Legro, 2000, pág. 255). En la escala internacional, las ideologías se materializan en normas, regímenes e instituciones, normalmente encabezadas por un Estado hegemónico (Morales, 2018). Sin embargo, como lo apunta el académico Daniel Morales Ruvalcaba, "la humanidad ha entrado en un momento poco común en la historia, caracterizado por la ausencia de una potencia hegemónica" (Morales Ruvalcaba, 2018). Esta fase se conoce como interregno hegemónico y se distingue por una intensa competencia interestatal, interempresarial, conflictos sociales y la reconfiguración de la estructura internacional (Morales, 2018, pág. 482; Morales, 2018b).

Para ilustrar estas concepciones, por un lado, se localiza la incertidumbre y el debate que ha crecido a medida que el gobierno de la República Popular de China, encabezado por Xi Jinping, ha adoptado políticas y comportamientos exteriores más asertivos. Por ejemplo, el énfasis del presidente chino Xi Jinping y de sus contrapartes en el 'rejuvenecimiento nacional' sugiere la existencia de un vínculo entre su doctrina del "sueño chino" (*zhonguo meng* 中国梦) y una gran estrategia de convertirse en la superpotencia dominante del mundo con una economía fuerte y un ejército poderoso (Xi, 2014, págs. 315-320).

Con base en esto, se están desarrollando los esquemas del "Cinturón Económico de la Ruta de la Seda" (*Silk Road Economic Belt*) y "la Ruta Marítima de la Seda del siglo XXI" (*Twenty First Century Maritime Silk Road*), hechas públicas en septiembre y octubre de 2013 respectivamente, los cuales son pilares fundamentales para el gobierno chino en su búsqueda por tener un mayor impacto en la configuración del orden internacional (Berger, 2014).[98] Al extender el alcance del proyecto de China, Xi Jinping pretende aprovechar el auge económico que su país ha acumulado durante décadas para aumentar el peso regional y global chino. Además, para fortalecer los proyectos mencionados se han establecido una serie de ambiciosas iniciativas de financiamiento, que incluyen la formación del Banco Asiático de Inversión en Infraestructura (*Asian Infrastructure Investment Bank*, AIIB), el Fondo de la Ruta de la Seda (*Silk Road Fund*) y la propuesta de un Área de Libre Comercio de Asia-Pacífico (*Free Trade Area of the Asia-Pacific*) (Miller T. , 2017).

En general, estas acciones desean crear un espacio de interconexión y de cooperación a través de la construcción de infraestructura, como lo son vías férreas, caminos, puertos, minas y diversos servicios públicos relacionados. En gran medida, este desarrollo apuesta a tener una mayor participación china en el escenario mundial y desempeñar un papel significativo en su configuración. Para ello, los dirigentes chinos consideran que las tecnologías de la información y la comunicación juegan un papel trascendental. Debido a ese corolario, la ciberseguridad se convierte en un pilar fundamental para la consecución de sus objetivos por medio de la edificación de cables de fibra óptica, redes de comunicación, centros de procesamientos de datos y establecimiento de ciudades inteligentes.

Por otro lado, el gobierno de Estados Unidos considera que la funcionalidad y operatividad de la red de información global debe robustecerse. Bajo esta idea, se pretende involucrar efectivamente a una mayor cantidad de agencias gubernamentales en un ecosistema digital más diverso y complejo. Para ello, los

[98] A estos planes también se les conoce como la Iniciativa de la Franja y la Ruta (*yidai yilu* 一带一路) que busca construir una extensa infraestructura de comunicaciones que conecte a la República Popular de China con el océano Índico, el Golfo Pérsico y una buena proporción de Europa.

dirigentes estadounidenses se apoyan no sólo en su aparato gubernamental sino también en el respaldo y experiencia que brindan diversas empresas tecnológicas de alcance global. En su estrategia, radica aprovechar la posición estadounidense en relación con el liderazgo sobre la evolución y el desarrollo del ciberespacio (Segal A. , 2018), que se ha subrayado con suma claridad en documentos oficiales recientes (U.S. Government White House , 2018). En otras palabras, el enfoque es mantener la estructura de gobernabilidad del ciberespacio, en particular, en sus aspectos de seguridad, sin grandes modificaciones, en la cual, precisamente, el gobierno estadounidense cuenta con una gran capacidad de influencia y negociación debido a su impronta en el diseño temprano del ciberespacio. Además de lo anterior, el gobierno estadounidense ha buscado limitar la inversión extranjera en empresas tecnológicas y de telecomunicaciones, bloqueado servicios de comunicación brindados por empresas extranjeras que considera pueden afectar la seguridad nacional y, a su vez, ha prohibido la venta de equipamiento y servicios tecnológicos en 'sectores críticos', como parte de sus acciones por mantener la preeminencia en espacios tecnológicos que considera sensibles.

No obstante, ambos proyectos públicos de ciberseguridad han generado suspicacias entre entes gubernamentales y no gubernamentales. Por un lado, los gobiernos francamente abiertos a una mayor participación gubernamental en el ciberespacio, como India, Brasil, Rusia, Corea del Sur, Israel, quienes buscan involucrarse directamente en el establecimiento de normas de comportamiento del Estado, no perciben en el enfoque chino un atractivo completo, debido a diversos factores, especialmente en el tratamiento de datos y lo infranqueable de algunos de sus planes de defensa cibernética, así como en el manejo de contenido digital a través de aplicaciones sociales.

Por otra parte, también distintos actores estatales observan con cautela el enfoque gubernamental estadounidense de ciberseguridad, principalmente, en lo que se refiere a las acciones emprendidas por sus agencias de inteligencia y sus instituciones militares. Precisamente, consideran que las acciones estadounidenses en el ciberespacio están teniendo un efecto contraproducente en la estabilidad y funcionalidad de la estructura digital global. Es decir, a medida que el gobierno de

los Estados Unidos desarrolla más y mejores capacidades ofensivas y defensivas en el ciberespacio, a la par se produce un proceso que busca minar y vulnerar esas operaciones, lo cual se traduce en una orientación hacia la militarización de los asuntos cibernéticos.

En relación con los agentes no estatales, la preocupación es que, tanto la visión gubernamental china como la estadounidense, sienten un precedente de intervención constante en los sistemas informáticos, que puedan entorpecer el adecuado funcionamiento de las redes globales. Otro de los aspectos que genera desasosiego, es que el ámbito de acciones estatales tenga una capacidad de intervención ubicua en relación con las actividades de sus conciudadanos, minando por ende diversas libertades. En muchos casos, los gobiernos están utilizando las tecnologías de información y comunicación para desplegar un mayor alcance de la censura, profundizar la vigilancia y desarrollar de nuevas formas de control y manipulación social de manera sofisticada, lo que limita derechos y libertadas en general. Esto genera contra respuestas que rebasan el alcance de esta investigación, pero que pueden ser temas de investigación pertinentes y relevantes en un futuro.

6.2 Enfoques de ciberseguridad de China y Estados Unidos

La relación bilateral sino-estadounidense está entrelazada en diversos ámbitos: estratégicamente, diplomáticamente, económicamente, socialmente, culturalmente y políticamente. Además, opera en diversos niveles de acción: globalmente, regionalmente, nacionalmente y localmente (Shambaugh D. , 2012).[99] De esta manera, la importancia de sus interacciones radica en la dimensión y alcance de ésta. Por ejemplo, ambos cuentan con las dos economías más grandes del mundo, los presupuestos militares más altos, son los dos principales consumidores de

[99] Por ejemplo, hay alrededor de 38 acuerdos de hermanamiento entre alguna provincia china y un estado estadounidense. Además, existen aproximadamente 169 acuerdos vinculantes de cooperación entre ciudades, muestra de la relación interdependiente entre China y Estados Unidos (Shambaugh, 2013, pág. 73).

energéticos en el orbe, los principales emisores de gases de efecto invernadero y, a su vez, quienes más invierten en investigación y desarrollo en energías renovables, los países con mayor número de patentes, cuentan con empresas tecnológicas de carácter global, y con una posición relevante en mecanismos como las Naciones Unidas, la Organización Mundial de Comercio o el G-20. Estas y otras condiciones les permiten tener una posición relevante para encaminar la agenda internacional en diversas temáticas, incluyendo en el ciberespacio.

No obstante, a estas posiciones interdependientes o convergentes, la relación sino-estadounidense comienza a mostrar más signos de competencia que de colaboración, principalmente desde 2009-2010. Diversas perspectivas consideran que, a partir de este momento, la dirigencia china obtuvo gran confianza por su manejo en la crisis financiera global combinado con un papel errático estadounidense durante esta situación, lo que ha acelerado el declive de su posición hegemonía internacional (Morales, 2018) (deLisle & Goldstein, 2017) (Helleiner & Kirshner, 2014) (Shambaugh D. , 2013).

Además, la divergencia de intereses, enfoques y políticas es cada vez más evidente en el entorno económico, ideológico, normativo, geopolítico y de seguridad (Shambaugh, 2013, pág. 74). Por ejemplo, David Shambaugh (2012, pág. 75), los esfuerzos bilaterales y multilaterales, se han convertido más en foros para discutir y manejar los impulsos competitivos, que para forjar una cooperación real. Para Kenneth Liberthal y Wang Jisi (2012), esto responde a que ambos gobiernos desconfían plenamente de los motivos reales de su contraparte, produciendo un ‘déficit de confianza estratégica’, lo que genera una dinámica de acción-reacción, donde cada dirigencia sobre interpreta y sobredimensiona las acciones y la narrativa del otro.

Con base en esta situación, y para las circunstancias que atañen a esta investigación, tanto la República Popular de China como los Estados Unidos de América han desarrollado un conjunto de leyes, reglas y normas de acción para salvaguardar la información de los sistemas reticulares gubernamentales y privados y han buscado la implementación procesos de innovación tecnológica interna y han buscado un mayor protagonismo en la gobernabilidad de estándares globales para

el funcionamiento del terreno ciberespacial. En este tenor, ambos gobiernos pretenden dar respuesta a incidentes de ciberseguridad, disminuir las vulnerabilidades en los sistemas informáticos, proteger la infraestructura de información crítica e involucrar a una vasta cantidad de agencias gubernamentales en el esfuerzo. Ciertamente, esto último, es para ambos gobiernos uno de los obstáculos más complejos de sortear, puesto que la interpretación y aplicación de estas políticas en los distintos niveles gubernamentales merma la eficacia de la implementación y ejecución de medidas de seguridad.

Además, bajo la voluntad de apuntalar las medidas de ciberseguridad, ambos gobiernos han promovido principios organizacionales para la gobernanza del ciberespacio, que en apariencia son diametralmente opuestos. Por un lado, el gobierno chino pretende que organismos internacionales intergubernamentales como las Naciones Unidas, en particular, la Unión Internacional de Telecomunicaciones, tengan un papel más relevante en los procesos de gestión del ciberespacio. Por otro lado, el gobierno estadounidense apuesta por mantener el actual funcionamiento, donde organismos descentralizados como ICANN, IETF, World Wide Web Consortium y los equipos CERT sean los encargados de desarrollar los estándares de la arquitectura global del ciberespacio, determinen los sistemas de nombre de dominio y sean quienes den respuesta a los incidentes cibernéticos que se presenten.

De la misma manera, ambos gobiernos han puesto a trabajar a diferentes dispositivos gubernamentales para la implementación de una estrategia de ciberseguridad integral. Al interior de sus jurisdicciones esto se ha traducido en el establecimiento de organizaciones centrales que puedan sortear el problema de colaboración interdepartamental al momento de un incidente cibernético o de otorgar mayores prerrogativas y funciones a cuerpos gubernamentales existentes en relación con temáticas de seguridad cibernética.

Por un lado, el gobierno chino ha creado la Administración para el Ciberespacio de China (CAC, por sus siglas en inglés) con el objeto de coordinar y ejecutar sus planes de ampliación de la soberanía cibernética. Por otra parte, el gobierno de los Estados Unidos ha creado el Comando Cibernético (USCYBERCOM), el cual busca

implementar conceptos de seguridad en el ciberespacio y crear asociaciones con el sector privado cibernético y otras agencias gubernamentales para una apuesta centrada en la seguridad nacional.

La creación de estos mecanismos centralizados no implica otros aparatos gubernamentales jueguen un papel en la ejecución de programas y políticas de ciberseguridad. Por ejemplo, para ambos casos, se involucran los máximos organismos militares, la Comisión Militar Central y el Departamento de Defensa; los mecanismos de procuración de justicia, Ministerio de Seguridad Pública y el Departamento de Justica; órganos encargados de seguridad, Ministerio de Seguridad del Estado y el Departamento de Seguridad Interna; agencias de inteligencia, 3º y 4º Departamento del Ejército Popular de Liberación y por otro lado, la Agencia de Seguridad Nacional (NSA), el FBI y la CIA; departamentos de investigación y desarrollo en materias de innovación y tecnología como el Ministerio de Industria y Tecnología de la Información o como la Fundación Nacional de Ciencia y el Instituto Nacional de Estándares y Tecnología. Esto da muestra de la importancia de la ciberseguridad en las acciones estatales y la fuerte valoración que está obteniendo la ciberseguridad para China y Estados Unidos. En la tabla 6.1 se puede ver de forma esquemática lo descrito en líneas anteriores.

Tabla 6.1 Departamentos gubernamentales en la implementación de la ciberseguridad

Rubros	**Agencias de la República Popular de China**	**Agencias de los Estados Unidos de América**
Militar y Defensa	Comisión Militar Central 3º y 4º Departamento del EPL	USCYBERCOM Departamento de Defensa
Procuración de Justicia	Ministerio de Seguridad Pública	Departamento de Justicia
Seguridad y Aspectos Judiciales	Ministerio de Seguridad del Estado Ministerio de Seguridad Pública CAC	Departamento de Seguridad Interna FBI

Inteligencia	3º y 4º Departamento del EPL CAC	NSA CIA FBI
Investigación y Desarrollo	Ministerio de Industria y Tecnología de la Información	Fundación Nacional de Ciencia Instituto Nacional de Estándares y Tecnología

Fuente: elaboración propia

Como se observa en el capítulo 4 y 5, la cantidad y la diversidad de oficinas, ministerios y departamentos gubernamentales que participan en la política de ciberseguridad, permite aseverar que la ponderación otorgada para esta área rubro es significativa. Con base en esto, se puede aseverar que el proceso de securitización de un objeto referentes, expresada por un desarrollo institucional ingente, asignación de recursos y narrativas se cumple tanto para la República Popular de China como para Estados Unidos de América.

Junto con ello, el gobierno chino y el gobierno estadounidense han desarrollado una amplia cantidad normas y regulaciones especializadas para contener la actividad maliciosa en el ciberespacio, y planes nacionales de ciberseguridad. Sin embargo, difieren en la identificación de elementos que pueden provocar vulnerabilidades y socavar sus tácticas de defensa cibernética. Asimismo, ambos Estados han considerado que la superficie digital que tienen que defender se acrecienta, y que el robustecimiento de la ciberseguridad se dará conforme la innovación tecnológica se apuntale. De esta manera, se puede entender la fuerte competencia comercial y estatal en rubros como el desarrollo e implementación de la tecnología 5G, la evolución de la inteligencia artificial y el posicionamiento de empresas nacionales de tecnología de información en diversos rubros como se expresa de forma sintética en la tabla 6.2.

Tabla 6.2 Comparación de proyectos de ciberseguridad gubernamental

Rubros	**República Popular de China**	**Estados Unidos de América**
No. de usuarios de internet	829 millones de personas	293 millones de personas

Porcentaje de la población con acceso a internet	60%	89%
No. de patentes en el desarrollo de tecnología 5G	3,400	1,368
No. de empresas involucradas en el desarrollo de inteligencia artificial	709	2,905
Porcentaje global de investigación en inteligencia artificial	28%	36%
Principal institución para abordar temas de ciberseguridad	CAC	USCYBERCOM
Ponderación de la ciberseguridad para objetivos de desarrollo	Muy alta	Muy alta
Enfoque de gestión de ciberseguridad	• Soberanía cibernética • Participación de organismos intergubernamentales internacionales	• Enfoque múltiples partes interesadas • Participación de organismos descentralizados
Tipo de participación gubernamental en relación con la ciberseguridad	Multi-ministerial	Multi-agencia

Fuente: elaboración propia con datos de (South China Morning Post; Abacus; Edith Yeung, 2019)

No obstante, esas diferencias aparentes obstaculizan la apreciación de las características de similitud entre ambas. Por ejemplo, en esta investigación se puede observar que la postura estadounidense de un proyecto de gestión sobre operatividad ciberespacial, pretende mantener un esquema funcional que ha sido co-dirigido y co-desarrollado preminentemente por su gobierno. Con base en esto, se han empujado ciertos preceptos que benefician y fortalecen su situación. Por otra parte, el gobierno chino ha buscado desarrollar un programa que lo convierta en una 'superpotencia cibernética' y busca tener una mayor injerencia en la gobernabilidad y operatividad de las redes informáticas globales.

Dentro de estos planes para posicionarse como guías conductuales, se ha brindado un fuerte apoyo al diseño, desarrollo, y posicionamiento de empresas tecnológicas, en ámbitos como el comercio electrónico, la clasificación de información, la transmisión de contenido audiovisual, el desarrollo de servicios musicales digitales, de transporte, de geolocalización, de almacenamiento en nube y juegos digitales. En la tabla 6.3 se puede observar algunas de las compañías más relevantes en cada sector, para ambos países.

Tabla 6.3 Principales compañías tecnológicas por sector

Rubros	**República Popular de China**	**Estados Unidos de América**
Búsqueda en la Red	Baidu	Google
Compras en línea	JD.com Tmall Taobao Pinduodudo	Amazon eBay
Transferencias y Pagos en líneas	Alipay WeChat Pay	Venmo PayPal iPay
Transmisión de contenido audiovisual	Tencent Video Youku iQiyi	YouTube Hulu Netflix Prime Video
Servicios musicales	QQMusic KuGou Music KuWo Music	Spotify iTunes
Servicios de mensajería	QQ WeChat	Whatsapp iMessage Groupme
Redes sociales	WeChat Weibo	Facebook Twitter Instagram
Servicios de citas	Tantan Momo	Tinder
Servicios de geolocalización	Autonavi	Google Maps
Servicios de transportación	DiDi	Uber Lyft
Servicios de renta de alojamiento	Xiaozhu	Airbnb
Servicios de reservación turística	Ctrip	Expedia Booking.com

Desarrollo de juegos digitales	NetEase Games Tencent Games	Activision Blizzard XBOX Game Studios Apple
Servicios de almacenamiento en nube	Alibaba Cloud Tencent Cloud	Amazon Web Services Google Cloud Platform

Fuente: (South China Morning Post; Abacus; Edith Yeung, 2019)

Con base en esto, algunos sectores comerciales estadounidenses, atribuyen que este amplio desarrollo tecnológico chino se debe a una actividad incesante de espionaje industrial y de robo de secretos comerciales, que les ha ayudado a acortar distancia en relación con la innovación industrial (Hannas, Mulvenon, & Puglisi, 2013). A menudo, esta postura asume que el espionaje cibernético es un atajo barato y efectivo para mejorar la innovación industrial. Sin embargo, los países adquirentes de tecnología externa han enfrentado desafíos para absorber la experiencia extranjera relevante y aplicarla (Andreas, 2014).

De igual manera, Jon R. Lindsay y Tai Ming Cheung (2015, págs. 66-67) han expuesto en su investigación que, los pasos necesarios que tiene que cumplir la República Popular de China para convertir la tecnología extranjera obtenida a través del espionaje cibernético en una variante doméstica rehecha son bastante complejos. Asimismo, señalan que el espionaje es una pequeña parte de un esfuerzo chino mucho mayor para adquirir, absorber y reconfigurar la experiencia tecnológica extranjera (Lindsay & Cheung, 2015, pág. 53). Además, cabe apuntar que la variante cibernética de espionaje industrial es sólo la manifestación más reciente de una tradición de siglos de antigüedad practicada por los principales países del sistema internacional en aras de subir los peldaños de la escalera tecnológica lo más rápido posible (Harris J. R., 1998; Bruland, 1989). Por lo cual, en este aspecto, la República Popular de China no representa una novedad en cuanto a sus esfuerzos de impulso industrial-tecnológico (Steinfeld E. S., 2017). Por último, para la República Popular de China la avalancha de datos digitales puede complicar aún más el problema de adquisición de información vía inteligencia y su consiguiente conversión en innovación autóctona (Lindsay & Cheung, 2015).

Por un lado, hay quienes resaltan que este enfoque basado en la competencia industrial-tecnológica obstaculiza la visualización de los puntos de convergencia y cooperación entre agentes tecnológicos de ambos países. Por ejemplo, el

académico Edward S. Steinfeld destaca que un énfasis excesivo en la rivalidad económica interestatal, oscurece la identificación de patrones de intensa colaboración comercial, desarrollo de empresas conjuntas y aprendizaje mutuo en el sector de tecnologías de información (Steinfeld E. S., 2017). Además, la estrategia basada en la competencia interestatal frena los impulsos sinérgicos necesarios para continuar apuntalando el desarrollo científico-tecnológico.

Por otro lado, a pesar de algunos contactos entre el gobierno de China y de los Estados Unidos por disipar visiones divergentes, no se han discutido oficialmente temas de ciberseguridad desde mayo de 2014. En ese momento, China suspendió su participación en el Grupo de Trabajo Cibernético Estados Unidos-China (*U.S.-China Cyber Working Group*), después de que el Departamento de Justicia de los Estados Unidos acusara a cinco miembros de la Ejército Popular de Liberación de llevar a cabo actividades maliciosas en el ciberespacio (Gady, 2016).[100]

No obstante, han existido algunos mecanismos de diálogo cibernético entre los dos países desde 2013 para resolver sus diferendos (Lu C. , 2017). El primero, fue el *US-China Cyber Working Group*. El objetivo de este grupo de trabajo era establecer un mecanismo de diálogo integral para abordar temas como el robo y el espionaje cibernético, así como para generar confianza estratégica entre sus cuerpos militares (Lu C. , 2017). En una segunda etapa, destaca el establecimiento del *China-US High-Level Joint Dialogue on Cybercrime and Related Issues*. Durante la segunda etapa, se resolvieron algunos problemas de robo cibernético de secretos comerciales, pero se avanzó poco en otros temas relacionados con el ciberespacio (Lu C. , 2017). Por último, en octubre de 2017 se presentó oficialmente el mecanismo *China-US Law Enforcement and Cybersecurity Dialogue*, uno de los cuatro mecanismos bilaterales establecidos después de la Cumbre de Mar-a-Lago entre el presidente Donald J. Trump y el presidente Xi Jinping en abril de 2017.

A pesar de ello, algunos analistas consideran que “China y Estados Unidos aún deben abordar más enérgicamente los problemas de ciberseguridad, incluida

[100] En mayo de 2014, el Departamento de Justicia condenó a los oficiales militares de la República Popular de China, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu y Gu Chunhui por hurtar información comercial propiedad de la compañía alemana de tecnología fotovoltaica SolarWorld y de la empresa proveedora de energía nuclear Westinghouse.

la cooperación para mecanismos de cumplimiento de la ley, la elaboración de normas internacionales en el ciberespacio, reglas sobre el acceso al mercado digital y pautas de entendimiento y confianza entre sus militares" (Gady, 2016; Li Z. , 2016; Lu C. , 2017).

Sin embargo, a pesar de estas proposiciones, las acciones gubernamentales sino-estadounidenses en materia de ciberseguridad parecen encaminarse en sentido opuesto. Por ejemplo, una de las estrategias gubernamentales estadounidenses ha sido comunicar y advertir a diferentes países sobre el riesgo en el uso de equipos y dispositivos electrónicos de empresas tecnológicas chinas, para sus comunicaciones internas, en especial, de la compañía Huawei (Toca, 2019).[101] Asimismo, el presidente de los Estados Unidos de América, Donald J. Trump, ha hecho explícito, a través de una orden ejecutiva, un estado de emergencia en las telecomunicaciones, la cual le brinda facultades y competencias al gobierno federal para prohibir a cualquier empresa adquirir servicios o productos con proveedores extranjeros. (Guimón, 2019; Muñoz, 2019).

Por una parte, esta medida representa un bloqueo directo contra la compañía china Huawei, así como, una nueva fase en la competencia hegemónica global contra la República Popular de China (Guimón, 2019; Toca, 2019).[102] Por un lado, la firma china vendió 202.9 millones de móviles en todo el mundo en el 2018, y tuvo un incremento de ventas de un 34.8%, lo que lo coloca el tercer fabricante mundial de móviles detrás de Apple y Samsung (Muñoz, 2019; Vida Liy & Mars, 2019). Bajo este marco analítico, algunos investigadores comentan que "el gobierno de EE. UU. parece haber decidido que es demasiado arriesgado que una empresa tecnológica china controle una parte sustanciosa de la infraestructura 5G" (Knight, 2019).[103]

---

[101] Algunos países que han impuesto restricciones (o han considerado hacerlo) a los equipos y dispositivos tecnológicos chinos son: Alemania, Australia, Canadá, Gran Bretaña, Japón y Nueva Zelandia (Knight, 2019).

[102] El temor expresado por las autoridades estadounidense en relación con las empresas tecnológicas chinas se funda en la estrecha relación que estas tienen con la cúpula política china. No obstante, grandes consorcios tecnológicos estadounidenses han trabajado codo a codo el gobierno de su país en el intercambiado de información sensible y en tareas de espionaje (Harris, 2014). Asimismo, la compañía Huawei se ha convertido en el mayor proveedor de equipos de redes, segundo mayor fabricante de teléfonos inteligentes en el mundo

[103] La red 5G es un sistema que permitiría la interconexión de dispositivos, aparatos, equipos mobiliarios e inmobiliarios enlazarse de manera simultánea, a una velocidad de ancho de banda de

Con base en esto, se ha comentado que la estrategia de detener la expansión de la compañía puede tener un efecto positivo para sus competidores, pues les permitiría emparejarse en la carrera comercial y técnica, en especial, las compañías tecnológicas estadounidenses (Knight, 2019; Vida Liy & Mars, 2019). Por otro lado, refleja claramente una competencia global por el liderazgo sobre el desarrollo e implementación de la próxima generación de tecnología de la comunicación, así como también, en el impulso de la computación cuántica y la inteligencia artificial.

No obstante, se mantiene incierto en qué medida las visiones sino-estadounidenses, en su afán competitivo, puedan ayudar a aminorar los riesgos y las vulnerabilidades a la seguridad cibernética. Tampoco está claro si estas perspectivas en apariencia divergentes producen un efecto estabilizador o colaboren para formar un esquema de ciberseguridad menos seguro y más incierto. Por último, tampoco se puede anticipar si la discrepancia sino-estadounidense puede generar una espiral de fragmentación y escisión del ciberespacio en jurisdicciones nacionales que, por ende, transforme completamente la estructura digital tradicional. Hasta el momento, solamente se puede aducir que la tendencia apunta hacia la continuación de un proceso de competencia intensa por el predominio o la preponderancia en el terreno ciberespacial; e implica que ambos Estados se perciben mutuamente como amenazas en el ciberespacio.

6.3 Conclusiones Generales

Este proyecto de investigación surgió de una pregunta muy simple: ¿por qué las actividades cibernéticas han tenido un efecto directo en la comprensión de la seguridad nacional? Al indagar sobre el tema, se encontró que no era una inquietud necesariamente nueva, pues como se ha demostrado a lo largo de este trabajo, la existencia de una vasta cantidad de artículos de investigación, libros, reportes y

20 gigas por segundo, lo que representa un aumento de entre el 25% y el 50% en comparación con las redes 3G y 4G respectivamente. De acuerdo con algunos reportes, la investigación para la implementación de las redes 5G en la República Popular de China comenzó en el año 2013. Además, desde el año 2016, se han realizado pruebas técnicas relacionadas con esta tecnología, por lo cual se afirma que está a la vanguardia para la implementación de dicha tecnología (Woyke, 2019).

opiniones abocados al estudio del fenómeno de las actividades cibernéticas de seguridad, sobre todo en lo que se refiere a las acciones gubernamentales, en especial, sobre sus efectos en el ramo de la seguridad nacional queda de manifiesto.

Bajo la revisión de la literatura, se puede aseverar que la novedad de este texto no radica en la interrogante, sino en el tipo de respuesta que ofrece, basándose en un enfoque multidisciplinar, donde se utilizan diversos modelos explicativos y conceptuales provenientes de áreas como la Comunicación, las Relaciones Internacionales, los Estudios de Seguridad Internacional, la Política Internacional y la Informática. Precisamente, la dinámica de la ciberseguridad comprende una serie de actividades transversales en diversos campos que difícilmente pueden analizarse bajo un solo lente analítico y que obligan a repensar sus implicaciones en diferentes frentes.

Para demostrar la hipótesis de este trabajo, en el capítulo 1, se presentó la definición de la problemática, los componentes esenciales de las acciones de los sujetos de estudio, cómo y qué conforman la estructura y el espacio de interacciones globales cibernéticas y las perspectivas de estudio en la relación entre tecnología y desarrollo que se traduce en ciertas prácticas que permiten la reconfiguración de escenarios y dinámicas socio-políticas. Por un lado, la revisión de la literatura, permitió demostrar que había un vacío epistemológico al momento de analizar la interacción entre acciones cibernéticas y sus efectos en las relaciones internacionales, en especial, sobre las consecuencias prácticas y sistémicas del fenómeno de la ciberseguridad en los asuntos internacionales.

Por otro lado, permitió distinguir entre un enfoque que pretende la incorporación de los asuntos tecnológicos y sus impactos en cuestiones estratégicas, políticas, diplomáticas, económicas y sociales y, otro que prefiere mantener una distancia considerable en relación a la relevancia que las actividades cibernéticas tienen como elemento de cambio y transformación del orden internacional. De esta manera, se ilustra un fuerte debate, que se mantiene vigente, sobre los efectos que tienen los espacios tecnológicos, en qué medida afectan las acciones de seguridad, políticas, económicas y sociales de diversos actores, así

como las acciones emprendidas por diversos agentes para asegurarse un predominio y control por encima de otros.

De igual manera, se buscó trazar una cronología sobre el desarrollo cibernético global, que fungiera como un puente teórico y empírico para comprender las mecánicas de cooperación y competencia entre diversos agentes en relación con la ciberseguridad, en especial, la inserción de los actores estatales y las formas en cómo lo han llevado a cabo. Asimismo, esta temporalización fue útil para tratar de comprender tendencias de más larga duración, que reconocen la conformación de la agenda de ciberseguridad contemporánea.

Por otra parte, en el capítulo 2 se buscó problematizar la concepción de seguridad, en especial, en su vertiente cibernética, desde la perspectiva de las Relaciones Internacionales. Ciertamente, dentro de la literatura del área informática, existen extensos análisis y sumamente precisos que circunscriben el problema de la seguridad cibernética y sus efectos sobre sistemas tecnológicos, pero no permiten observar que implicaciones tiene más allá de este reducido entorno. Por ello, se recurrió a concepciones teóricas que brindaran una explicación y comprensión profunda del fenómeno de seguridad y su interpretación por los agentes estatales, así como las respuestas que genera.

Al momento de conformar el sustento teórico de este trabajo de investigación, una dificultad encontrada reiteradamente en otros análisis que preceden a éste, es que había pocas acciones cibernéticas realizadas por los agentes estatales que hayan tenido efectos cinéticos de gran calado o qué tuvieran efectos sobre la seguridad global. Esto obstaculiza la refinación de los preceptos teórico-conceptuales por la escasez de situaciones empíricas que puedan ayudar a comprobar y contrastar las proposiciones. Aunque dicha cuestión se fue perfilando desde la revisión de la literatura en el primer capítulo de esta tesis, se hizo palpable en este apartado.

No obstante, bajo estas evidencias, y en aras de brindar una aportación teórico-metodológica, esta investigación se dio a la tarea de analizar la forma en cómo se enmarcaban las actividades de seguridad cibernética a través de elementos observables como el desarrollo de regulaciones gubernamentales. Como

se señaló, a falta de casos empíricos y debido a lo incipiente del fenómeno, se buscó, en aras de refinar, depurar y consolidar un esquema teórico-conceptual comprender cómo los agentes conceptualizan un fenómeno como una amenaza, que, por ende, se vuelve una problemática de seguridad y debido a este conduce a reconfiguraciones discursivas, simbólicas e institucionales. Para la consecución de este propósito se recurrió primordialmente a dos perspectivas analíticas.

Por un lado, se hizo uso de concepciones constructivistas de Relaciones Internacionales como una forma de palanca que permitiera entender cuestiones como la constitución mutua entre agencia y estructura, constituida por elementos cognitivos, recursos materiales y prácticas. En este caso particular, los agentes estatales, la conformación estructural tecnológica y las acciones realizadas para participar dentro de ésta, observables a través de un desarrollo institucional constante, donde establecen un proceso de interacción que genera nuevos ámbitos y alteraciones en las acciones cibernéticas de carácter sistémico. Con base en ello, se manifiesta una base sólida para entender efectos estructurales que suceden a nivel unitario, como se muestra en los capítulos 4 y 5.

Además, el constructivismo dio la oportunidad de problematizar el cambio de prácticas de los agentes conforme a sus intereses, situación que se pudo observar tenuemente desde el capítulo 1 y que se demostró en el capítulo 3. En este caso, se buscó identificar por qué los agentes estatales realizaban ciertas acciones en el ciberespacio que anteriormente no habían ejecutado. En este orden de ideas, también los elementos constructivistas brindaban la oportunidad de plantear tres elementos de un mismo proceso que realizan los agentes como guía de acción para enmarcar la forma de interactuar con otros *1)* señalamiento; *2)* interpretación; y *3)* respuesta. Sin embargo, a pesar de esta base explicativa sólida, únicamente se proveía de una explicación parcial sobre la injerencia estatal en la conformación de la estructura digital.

Con base en esto, se escudriñó sobre el uso, apreciación e interpretación del concepto de seguridad por los agentes estatales y cómo sirve de mapa para el diseño de políticas destinadas a disminuir riesgos y amenazas. Por ello, se acudió a la subdisciplina de Estudios de Seguridad Internacional, que ha problematizado

sobre la concepción de la seguridad, sus dimensiones y los medios utilizados para implementarla. Primordialmente, hubo un énfasis en la interpretación que hacen la Escuela de Copenhague y de París, dos perspectivas que tratan de explicar cómo el enmarcado del riesgo y la amenaza determina el significado de las acciones de los agentes. Esta acción la denominan como el proceso de securitización, en otras palabras, cuando los asuntos públicos se convierten en un problema de seguridad no necesariamente porque existe una amenaza existencial real, sino porque el problema se presenta y establece con éxito por agentes clave como una amenaza.

Ciertamente, este ejercicio analítico muestra limitantes, pues no explora como la presentación de ciertos fenómenos expresados como asuntos de seguridad son aceptadas por la atención pública, en qué medida y por cuánto tiempo permanece la aceptación. No obstante, esto puede fungir como una línea de investigación futura, que trascienda de los agentes estatales hacia la recepción social sobre la existencia de ciertas amenazas y el despliegue de medidas de respuesta y contra respuesta. Puesto que los sujetos de estudio seleccionados para esta investigación son casos paradigmáticos, la indagación en estos puede aportar elementos para la profundización de esta problemática. De la misma manera, esta propuesta metodológica puede traslaparse para estudiar agentes estatales como Rusia, Israel, Alemania, Estonia, Irán o el caso de México que cuentan con andamiajes y desarrollos cibernéticos interesantes, lo cual hace relevante y pertinente esta propuesta de investigación.

Para dar continuidad con este hilo conductor, sobre cómo están ligados los procesos de securitización a elementos discursivos convencionales y al uso de recursos materiales e institucionales que los agentes despliegan en el espacio digital y corroborar qué efectos tienen sobre la reestructuración del carácter en las actividades dentro del ciberespacio, en el capítulo 3, se enfatizó, primeramente, en una construcción ontológica de la problemática, para entender lo que se ha considerado como el espectro de ciberseguridad. Bajo estas circunstancias, se hizo una breve presentación de cómo se fue gestando y evolucionando la administración del ciberespacio y cómo ha ido conformándose.

Este ejercicio era necesario para la comprensión del tipo de actividades que generan vulnerabilidad en los sistemas informáticos, en cómo se buscan solucionar y en qué medida brindan una justificación para acciones estatales más agresivas en el entorno digital. Un hallazgo al contrastar las aproximaciones de agentes estatales y no estatales en la forma de regir las acciones de seguridad cibernética es que indirectamente las acciones estatales generan una respuesta contraproducente en el mantenimiento de la estabilidad, funcionalidad y resiliencia del entorno ciberespacial. Esto se debe a que las herramientas, dispositivos y disposiciones institucionales gubernamentales en ocasiones fungen más como una fuente de vulnerabilidad o como un catalizador de riesgo que como una solución en la mecánica funcional de seguridad en el ciberespacio.

Además, las acciones de los Estados cuentan con un enfoque que prima la competencia y la fragmentación del ciberespacio, en el cual la seguridad informática es una herramienta que busca, a través del control y regulación, consolidar posiciones estratégicas y de poder, antes que aspectos organizacionales como la administración y la gestión. A partir de ello, la operatividad global del ciberespacio entremezcla tanto estándares técnicos como medios formales e informales de autoridad y jurisdicción. Como se ha podido observar, este es sólo un pequeño conjunto de un ámbito más amplio de investigación que se centra en las implicaciones creadas por el ciberespacio.

Por un lado, esta investigación se concentró en analizar cuál es el papel del Estado en la conformación de la arquitectura técnica del ciberespacio y cuáles son las iniciativas institucionales y normativas que producen para crear una línea administrativa que pueda ajustarse a sus intereses. Con base en ello, se encontraron dos vertientes principales para gestionar la operatividad de la estructura digital global. Aunque, si bien es cierto, estos dos esquemas no son enarbolados únicamente por los sujetos de estudio presentados en los capítulos 4 y 5, sí representan las versiones más asertivas y paradigmáticas a nivel internacional.

Por otro lado, el análisis permitió perfilar que la conformación de principios, normas y reglas que garantizan la interoperabilidad del sistema informático

internacional está generando cismas y escisiones que pueden afectar el funcionamiento de la estructura global ciberespacial. Además, esta tesis ha dejado de manifiesto que las acciones estatales comprenden la ciberseguridad como un área importante para la competencia por la preeminencia de poder global. Sin embargo, como hallazgo de esta investigación, se pudo observar que la capacidad de influencia de los gobiernos en la ejecución funcional del ciberespacio se encuentra aún limitada, aunque, decididamente buscan modificar esta circunstancia, que se constata en su forma de participación y en la profundidad de sus acciones.

Cabe resaltar que, una limitante del enfoque estato-céntrico abrazado en gran medida por esta investigación en relación con el estudio de las actividades cibernéticas de seguridad, es que deja fuera las percepciones y acciones de otros actores relevantes, que comúnmente son quienes perfilan en buena medida la estructura de seguridad del ciberespacio. No obstante, uno de los objetivos de este trabajo era conocer cómo los agentes estatales pueden modificar el funcionamiento de la arquitectura ciberespacial a través de su injerencia, lo cual brindaba una cara de la explicación para un fenómeno multi-agencia. No obstante, antes que representar un obstáculo, esto puede verse como una oportunidad que abre pautas para líneas de investigación futura, como por ejemplo saber el papel que las empresas, grupos de interés y organizaciones no gubernamentales juegan al formar y modelar las opciones de los agentes estatales en el ámbito tecnológico y, así realizar una comparación de enfoques sobre la gobernanza de ciberseguridad.

Para brindar base empírica de lo anterior, los capítulos 4 y 5 permitieron observar una comparación entre dos enfoques de acercamiento hacia el fenómeno de la ciberseguridad, acción que se ha hecho de forma escasa, por lo cual se identifica como una fortaleza de esta propuesta de investigación, presentada sucintamente en este último apartado. Con ello, salta a la vista la necesidad de seguir profundizando en este tipo de análisis. Bajo estas circunstancias, al contrastar las distintas aproximaciones del fenómeno de los sujetos de estudio, se identificó que en ambos casos se ha desarrollado una cantidad considerable de

estrategias, tácticas y recursos utilizados para hacer frente a los riesgos y vulnerabilidades de seguridad cibernética.

De igual manera, se observó que la capacidad, contexto, estructuras institucionales y mecanismos de acercamiento proporcionan como consecuencia acciones y respuestas particularmente distintivas para abordar la temática de ciberseguridad. No obstante, como se trató de demostrar, en ambos casos los sujetos de estudio llevaron a cabo respuestas institucionales que pueden generar una dinámica de inestabilidad para la funcionalidad de la estructura ciberespacial debido a que premian la superioridad y la competencia como móviles en sus estrategias.

Finalmente, a través de esta investigación se puede identificar la importancia, relevancia y pertinencia para las Relaciones Internacionales y otras ramas de estudio la necesidad de continuar analizando y abordando temáticas no tradicionales o incipientes, que, aunque complejas de enmarcar, acotar o delimitar y que complejizan la tarea de investigar, también permiten tener un mayor alcance y trascendencia explicativa, la cual facilita la comprensión holística de fenómenos transversales como la ciberseguridad u otras problemáticas globales que cuentan con características similares. Además, este trabajo de investigación pone de manifiesto que las intersecciones epistemológicas se convierten en un factor de enriquecimiento y beneficio para el conocimiento humano.

Bibliografía

Aaronson, S. A. (26 de septiembre de 2016). *The Great Moderation? China and the U.S. in Cyberspace.* Recuperado el 2 de septiembre de 2018, de China U.S. Focus: https://www.chinausfocus.com/peace-security/the-great-moderation-china-and-the-us-in-cyberspace

Accenture & Polemon Institutte. (2017). *2017. Cost of Cyberecrime Study: insights on the Security Investments that Make a Difference*. Recuperado el 21 de junio de 2019, de Accenture: https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

Acharya, A. (2014). *The End of American World Order.* Cambridge: Polity.

Adler, E. (1992). The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the idea of Nuclear Arms Control. *International Organization, 46*(1), 101-145.

Adler, E. (1997). Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations, 3*(3), 319-363.

Adee, S. (13 de junio de 2019). *Por qué los esfuerzos de Rusia y China para poner fronteras a internet suponen el fin de la red tal y como la conocemos*. Recuperado el 14 de junio de 2019, de BBC: https://www.bbc.com/mundo/vert-fut-48618084

Allison, G. T., & Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis* (2a. edición ed.). New York: Longman.

Allison, G., & Treverton, G. T. (1992). *Rethinking America's Security: Beyond Cold War to New World Order.* Nueva York: W. W. Norton.

Alsabah, N. (15 de septiembre de 2016). *Information Control 2.0: The Cyberspace Administration of China tames the Internet.* Recuperado el 16 de febrero de 2019, de Mercator Institute for China Studies: https://www.merics.org/sites/default/files/2017-09/China_Monitor_32_Information_control20_EN_0.pdf

Andreas, P. (2014). *Smuggler Nation.* Nueva York: Oxford University Press.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy, 12*(2), 141-165.

Arreola García, A. (2015). *Ciberespionaje: la puerta al mundo virtual de los estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos.* México: Siglo XXI.

Austin, G. (2014). *Cyber Policy in China.* Cambridge: Polity.

Austin, G. (2018). *Cybersecurity in China. The Next Wave.* Cham, Suiza: Springer.

Blank, S. (2008). Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy, 27*(3), 227-247.

Baldwin, D. (1996). Security Studies and the End of the Cold War. *World Politics, 48*(1), 117-141.

Baldwin, D. (1997). The Concept of Security. *Review of International Studies, 23*(1), 5-26.

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace.* Recuperado el 8 de agosto de 2018, de Electronic Frontier Foundation: https://www.eff.org/

Barnett, A. D. (1985). *The Making of Foreign Policy in China: Structure and Process.* Boulder: Westview Press.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook.* New Jersey: Wiley.

Beckley, M. (2011). China's Century? Why America's Edge Will Endure. *International Security, 36*(3), 41-78.

Beck, U. (1992). *Risk Society.* Londres: Sage Publications.

Beck, U. (1999). *World Risk Society.* Londres: Polity.

Bendrath, R. (2003). The American Cyber-Angst and the Real World- Any Link? En R. Latham, *Bombs and Bandwidth: The Emerging Relationship Between IT and Security.* New York: New Press.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven: Yale University Press.

Berger, S. (09 de noviembre de 2014). *Xi Offers Vision of China-Driven 'Asia-Pacific' Dream.* Obtenido de Jakarta Globe: http://jakartaglobe.id/international/xi-offers-vision-china-driven-asia-pacific-dream/

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed. *Journal of Strategic Studies, 35*(5), 689-711.

Bi, R. (11 de enero de 2018). *Is America's Post-Net Neutrality Internet Sinocizing?* Recuperado el 02 de mayo de 2019, de China-US Focus: https://www.chinausfocus.com/peace-security/is-americas-post-net-neutrality-internet-sinocizing

Bigo, D. (1994). The European internal security field: stakes and rivalries in a newly developing area of police intervention. En M. Anderson, & M. den Boer, *Policing Across National Boundaries* (págs. 161-173). Londres: Pinter.

Bonner, R. (24 de mayo de 2011). *Rebekka's Bonner Blog.* Obtenido de Information Society Project, Yale Law School.

Booth, K. (1994). *A Security Regimen in Southern Africa: Theoretical Considerations.* University of the Western Cape. Sudáfrica: Centre for Southern African Studies.

Borg, S. (2005). Economically Complex Cyberattacks. *IEEE Security and Privacy Magazine, 3*(6), 64-67.

Borgmann, A. (1999). *Holding on to Reality: The Nature of Information at the Turn of the Millennium.* Chicago: University of Chicago Press.

Bravo, J. (2017). La relación política sinoestadounidense en Asia del Este: lucha por el poder o divergencias resultantes de la percepción de amenaza. *Foro Internacional, 57*(4), 870-914.

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* Nueva York: Penguin.

Brito, J., & Watkins, T. (2011). *Loving the cyber bomb? The dangers of threat inflation.* Arlington, VA: George Mason University.

Broeders, D. (2015). *The Public Core of the Internet: An International Agenda for Internet Governance.* Amsterdam: Amsterdam University Press.

Bruland, K. (1989). *British Technology and European Industrialization.* Cambridge: Cambridge University Press.

Buchanan, B. (2016). *The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations.* Oxford: Oxford University Press.

Bukovansky, M. (1997). American Identity and Neutral Rights from Independence War of 1812. *International Organization, 51*(2), 209-243.

Bukovansky, M. (1999). The Altered State of Nature: The French Revolution and International Politics. *Review of International Studies, 25*(2), 197-216.

Burgman, P. R. (18 de mayo de 2016). *Securing Cyberspace: China Leading the Way in Cyber Sovereignty.* Recuperado el 29 de agosto de 2018, de The Diplomat: https://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/

Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies.* Londres: Lynne Rienner.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis.* Londres: Lynne Rienner.

CAC. (27 de diciembre de 2016). *国家网络空间安全战略 [China's National Cybersecurity Strategy]*. Recuperado el 7 de noviembre de 2018, de Cyberspace Administration of China: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

Camilleri, J. A., & Falk, J. (1992). *The End of Sovereignty? The Politics of a Shrinking and Fragmenting World.* Aldershot: Edward Elgar.

Campbell, J. L. (1998). Institutional Analysis and the Role of the Ideas in Political Economy. *Theory and Society, 27*(3), 377-409.

Castells, M. (1989). *The Informational City: Information Technology, Economic Restructuring, and the Urban-Regional Process.* Oxford: Blackwell.

Castells, M. (1996). *The Information Age: Economy, Society, and Culture, Vol.1: The Rise of the Network Society.* Malden, MA: Blackwell.

Castells, M. (1997). *The Information Age: Economy, Society, and Culture, Vol. 2: The Power of Identity.* Malden, MA: Blackwell.

Castells, M. (1998). *The Information Age: Economy, Society, and Culture, Vol. 3: End of Millenium.* Malden, MA: Blackwell.

Castells, M. (2009). *Comunicación y poder.* Madrid: Alianza Editorial.

Chairman of the Joint Chiefs of Staff. (2011). *National Military Strategy of the United States.* Washington: U.S. Deparment of Defense.

Chappell, B. (13 de febrero de 2015). *Obama: Cyberspace Is the New Wild West.* Recuperado el 21 de noviembre de 2018, de NPR: https://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats

Chen, Z. (2009). International Responsibiltiy and China's Foreign Policy. En M. Iida, *China's Shift: Global Strategy of the Rising Power* (págs. 7-28). Tokyo: The National Institute for Defense Studies.

Cheng, L. (2016). *Chinese Politics in the Xi Jinping Era: Reassesing Collective Leadership.* Washington, DC: Brookings Institution.

Cheng, D. (2017). *Cyber Dragon. Inside China's Information Warfare and Cyber Opertions.* Santa Barbara: Praeger.

Chernov, A. (2004). Global Information Society. *International Affairs, 6*, 8-22.

Cheung, T. M. (2009). *Fortifying China: The Struggle to Build a Modern Defensa Economy.* Ithaca, NY: Cornell University Press.

China Daily. (07 de febrero de 2017). *China to introduce rewiee commision on cybersecurity.* Recuperado el 31 de enero de 2019, de China Daily: http://www.chinadaily.com.cn/business/tech/2017-02/08/content_28135358.htm

China Digital Times. (2017 de enero de 2017). *China reinforces great firewall with new VPN rules.* Recuperado el 30 de enero de 2019, de https://chinadigitaltimes.net/2017/01/china-reinforces-great-firewall-new-vpn-rules/

China.org. (18 de febrero de 2017). *Xi calls for global vision in China's national security work*. Recuperado el 9 de febrero de 2019, de China.org: http://www.china.org.cn/video/2017-02/18/content_40313020.htm

Choucri, N. (2012). *Cyberpolitics in International Relations.* Londres: MIT Press.

Christensen, T. (2015). *The China Challenge: Shaping the Choices of a Rising Power.* Nueva York: Norton.

CISCO/Cybersecurity Ventures. (6 de febrero de 2019). *2019 Cybersecurity Almanc: 100 Facts, Figures, Predictions and Statistics*. Recuperado el 21 de junio de 2019, de Cybersecurity Ventures & CISCO: https://cybersecurityventures.com/cybersecurity-almanac-2019/

Clark, D. D. (2010). *Characterizing Cyberspace: past, presente and future.* Cambridge: MIT Press.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat* . Nueva York: Ecco.

Clinton, H. R. (2010). *Remarks on Internet Freedom.* Washington, DC: U.S. Department of State.

Collins, A. R. (2007). *Contemporary Security Studies.* Oxford: Oxford University Press.

Council on Foreign Relations. (2019). *Cyber Operations Tracker.* Recuperado el 2019, de CFR: https://www.cfr.org/interactive/cyber-operations#CyberOperations

Craig, A. J., & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. En D. Orsi, J. R. Avgustin, & M. Nurnus, *Realism in Practice: An Appraisal* (págs. 85-101). Bristol, Reino Unido: E-International Relations Publishing.

Crosset, V., & Dupont, B. (2018). Internet et propagande jihadiste: la régulation polycentrique du cyberespace. *Critique Internationale, 78*(1), 107-125.

Danchev, D. (11 de agosto de 2008). *Coordinated Russia vs Georgia Cyber Attack in Progress*. Recuperado el 11 de agosto de 2018, de ZDNet: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Davis, J. (22 de agosto de 2007). *Hackers Take Down the Most Wired Country in Europe*. Recuperado el 23 de agosto de 2018, de Wired: https://www.wired.com/2007/08/ff-estonia/

deLisle, J., & Goldstein, A. (2017). *China's Global Engagement: Cooperation, Competition and Influence in the 21st Century.* Washington: Brookings Institution Press.

Debrix, F. (2001). Cyberterror and media-induced fears: the production of emergency culture. *Strategies, 14*(1), 149-168.

Deibert, R. (2011). *Tracking the Emerging Arms Race in Cyberspace.* Bulletin of Atomic Scientists.

Deibert, R. J. (1997). *Parchment, Printing, and Hypermedia.* Nueva York: Columbia University Press.

Deibert, R. J. (1997). *Parchment, Printing, and Hypermedia.* New York: Columbia University Press.

Deibert, R. J. (1997). *Parchment, Printing, and Hypermedia: Communication in World Order Transformation.* Nueva York: Columbia University Press.

Deibert, R. J. (2003). Black code: censorship, surveillance, and militarization of cyberspace. *Millennium, 32*(2), 501-530.

Deibert, R. J. (2013). *Black code: surveillance, privacy, and the dark side of the internet.* Toronto: McClelland & Stewart.

Deibert, R. J. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto: McClelland & Stewart.

Deibert, R. J., & Gross Stein, J. (2003). Social and Electronic Networks in the War on Terror. En R. Latham, *Bombs and Bandwidth: The Emerging Relationshio Between Information Technology and Security* (págs. 157-174). New York: New Press.

Deibert, R. J., & Rohozinsky, R. (2010). Liberation vs Control in Cyberspace. *Journal of Democracy, 21*(4), 43-57.

Deibert, R. J., & Rohozinsky, R. (2010). Liberationn vs Control in Cyberspace. *Journal of Democracy, 21*(4), 43-57.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Deibert, R., Palfrrey, J., Rohozinski, R., & Zittrain. (2008). *Access Denied: the Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

Demchak, C. C. (2011). *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security.* Athens: University of Georgia Press.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance.* Cambridge, Massachusetts: MIT Press.

DeNardis, L. (2014). *The Global War for Internet Governance.* New Haven: Yale University Press.

Denning, D. (1998). *Information Warfare and Security.* Reading: Addison-Wesley.

Denning, D. E. (2001). Activims, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy. En J. Arquilla, & R. D. J., *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica, MA: Rand.

Department of Defense. (2006). *Quadrennial Defense Review.* Washington: Department of Defense.

Department of Homeland Security. (marzo de 2013). *Executive Order (EO) 13636, Improving Critical Infraestructure Cybersecurity.* Obtenido de Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf

Department of Homeland Security. (20 de mayo de 2019). *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Recuperado el 20 de mayo de 2019, de Department of Homeland Security: https://www.dhs.gov/cisa/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

Desjardins, J. (13 de marzo de 2019). *What Happens in an Internet Minute in 2019*. Recuperado el 13 de marzo de 2019, de Visual Capitalist: https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

Deudney, D., & Matthews, R. (1999). *Contested Grounds Security and Conflict: The New Environmental Politics.* Albany: State University of York Press.

Deutsch, K. (1963). *The Nerves of the Government: Models of Political Communications and Control.* Nueva York: Glencoe.

Dobbins, J. (2012). War with China. *Survival, 54*(4), 7-24.

Dobbins, J. (2012). War with China. *Survival, 54*(4), 7-24.

Drezner, D. W. (2009). Bad Debts Assesing China's Influence in Great Power Politics. *International Security, 34*(2), 7-45.

Dunn Cavelty, M. (2007). Is Anything Ever New? En M. Dunn Cavelty, V. Mauer, S. Krishna-Hensel, & (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (págs. 19-44). Londres: MPG Books.

Dunn Cavelty, M. (2008b). *Cyber-Security and Threats Politics: U.S. Efforts to Secure the Information Age.* Nueva York: Routledge.

Dunn Cavelty, M. (2008b). Cyber-terror, looming threat or phantom menace: the framing of the US cyber-threat debate. *Journal of Information & Technology Politics, 4*(1), 19-36.

Dunn Cavelty, M., & Brunner, E. M. (2007). Introduction: Information, Power and Security: An Outline of Debates and Implications. En M. Dunn Cavelty, V. Mauer, S. Krishna-Hensel, & (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.* Londres: MPG Books.

Dutton, W. H. (1999). *Society on the Line: Information Politics in the Digital Age.* Oxford: Oxford University Press.

Ebert, H., & Maurer, T. (2014). Revendications sur le cyberespace et puissances émergentes. *Hérodote, 152-153*(1), 276-295.

Edde, R. (2018). Le droit? Un outil de régulation du cyberespace? Le cas du droit à l'oubil numérique. *Homme et la Societe, 206*(1), 69-94.

Embajada de la República Popular de China en Estados Unidos de América. (11 de mayo de 2006). *China Maps Out Informatization Development Strategy.* Recuperado el 20 de abril de 2018, de People's Republic of China Embassy: http://www.china-embassy.org/eng/xw/t251756.htm

Equifax. (1 de marzo de 2018). *Equifax Releases Updated Information on 2017 Cybersecurity Incident.* Recuperado el 21 de junio de 2019, de https://www.equifaxsecurity2017.com/2018/03/01/equifax-releases-updated-information-2017-cybersecurity-incident/

Eriksson, J., & Giacomello, G. (. (2007). *International Relations and Security in the Digital Age.* Londres, Nueva York: Routledge.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security and international relations: the (IR) relevant theory? *International Political Science Review, 27*(3), 221-244.

Escobar, A. (junio de 1994). Welcome to cyberia: notes on the anthology of cyberculture. *Current Anthropology, 35*(3), 211-231.

Everard, J. (2000). *Virtual States: The Internet and the Boundaries of the Nation-State.* Londres, Routledge.

Executive Office of the President of the United States of America. (diciembre de 2017). *National Security Strategy of the United States of America*. Obtenido de U.S. White House: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Flournoy, M., & Sulmeyer, M. (2018). Battlefield Internet: A Plan for Securing Cyberspace. *Foreign Affairs, 97*(5), 40-46.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival, 53*(1), 23-40.

Fearon, J. D., & Wendt, A. (2002). Realism v. Constructivism: A Skeptical View. En *Handbook of International Relations.* Londres: Sage Publications.

Feigenbaum, E. A. (2003). *China's Techno Warriors: National Securirty and Strategic Competition.* Stanford , CA: Stanford University Pres.

Ferguson, N. (2017). The False Prophecy of Hyperconnection. *Foreing Affairs, 96*(5).

Finnemore, M. (2011). Cultivating International Cyber Norms. En K. M. Lord, & T. Shard, *America's Cyber Future: Security and Prosperity in the Information Age, vol.1.* Washington, DC: Center for a New American Security.

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization, 52*(4), 887-917.

Foot, R., & Walter, A. (2010). *China, the United States, and the Global Order.* Nueva York: Oxford University Press.

Foot, R., & Walter, A. (2011). *China, the United States, and Global Order.* Nueva York: Cambridge University Pres.

Fountain, J. E. (2001). *Building the Virtual State: Information Technology and Institutional Change.* Washington, DC: Brookings Institution.

Franda, M. F. (2001). *Governing the Internet: The Emergence of an International Regime.* Boulder, CO: Lynne Rienner.

Freeman, C., & Louca, F. (2002). *As Times Goes By: From the Industrial Revolutions to the Information Revolution.* Oxford: Oxford University Press.

Friedberg, A. L. (2011). *A Contest for Supremacy: China, America and the Struggle for Mastery in Asia.* Nueva York: W.W. Norton.

Friedberg, A. L. (2011). *A Contest for Supremacy: China, America and the Struggle for Mastery in Asia.* Nueva York: W.W. Norton.

Friis, K., & Ringsmose, J. (s.f.). *Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives.* Londres: Routledge.

Fu, D. (2017). *Mobilizing Without the Masses. Control and Contention in China.* Cambridge: Cambridge University Press.

Glaser, C. L. (2004). When Are Arms Races Dangerous? Rational versus Suboptimal Arming. *International Security, 28*(4), 44-84.

Glaser, B., & Medeiro, E. (2007). The Changing Ecology of Foreign Policy-Making in China: The Ascension and Demise of the Theory of 'Peaceful Rise'. *The China Quarterly, 190*, 291-310.

Gady, F.-S. (28 de enero de 2016). *What Does 2016 Hold for U.S.-China Relations in Cyberspace?* Recuperado el 15 de noviembre de 2018, de China-US Focus: https://www.chinausfocus.com/peace-security/what-does-the-year-2016-hold-for-china-u-s-relations-in-cyberspace/

Gan, N. (21 de septiembre de 2017). *China's Security chief calls for greater use of AI to predict terrorism, social unrest.* Recuperado el 14 de febrero de 2019, de South China Morning Post: https://www.scmp.com/news/china/policies-politics/article/2112203/china-security-chief-calls-greater-use-ai-predict

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41-73.
Gary Sharp, W. (1999). *Cyberspace and the Use of Force.* Falls Church: Aegis Research.
Gilpin, R. (1981). *War and Change in World Politics .* Cambridge: Cambridge University Press.
Gilpin, R. (1986). The Richness of the Tradition of Political Realism. En R. Keohane, *Neorealism and Its Critics.* New York: Columbia University Press.
Gilping, R. (1987). *The Political Economy of International Relations.* Princeton, NJ: Princeton University Press.
Giacomello, G. (2005). *National Governments and Control of the Internet: A Digital Challenge.* Londres: Routledge.
Gibson, W. (1984). *Neuromancer.* Nueva York: Ace.
Goldman, E., & Mahnken, T. G. (2004). *The Information Revolution in Military Affairs in Asia.* New York: Palgrave Macmillan.
Goldsmith, J. L., & Wu, T. (2006). *Who Controls the Internet: Illusions of a Borderless World.* Oxford: Oxford University Press.
Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World.* New York: Oxford University Press.
Goldstein, L. (2015). *Meeting China Halfway.* Washington, DC: Georgetown University Press.
Gompert, D. C., Lachow, I., & Perkins, J. (2006). *Battle-Wise: Seeking Time-Information Superiority in Networked Warfare.* Washington: National Defense University Press.
Gourevitch, P. (1978). The Second Image Reversed: The International Sources of Domestic Politics. *International Organization, 32*(4), 881-912.
Greenwald, G., & MacAskill, E. (7 de junio de 2013). *Obama Orders US to Draw Uo Overseas Target List for Cyber-Attacks*. Recuperado el 12 de marzo de 2018, de The Guardian: https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas
Guimón, P. (16 de mayo de 2019). *Trump blinda las telecomunicaciones de EE UU contra Huawei en una nueva ofensiva contra China.* Recuperado el 16 de mayo de 2019, de El País: https://elpais.com/internacional/2019/05/15/estados_unidos/1557957202_172429.html
Guiora, A. N. (2017). *Cybersecurity: Geopolitics, Law, and Policy .* Nueva York : Routledge.
Han, R. (2018). *Contesting Cyberspace in China: Online Expression and Authoritarian Resilience.* New York: Columbia University Press.
Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage: Technology Acquisition and Military Modernization.* Nueva York: Routledge.
Hansen, L. (2000). The Little Mermaid's Salient Security Dilemma: The Absence of Gender in the Copenhagen School. *International Studies, 29*(2), 285-306.
Hansen, L., & Nissenbaum, H. (2009). Digital disaster: cyber security, and the Copenhagen School. *International Studies Quarterly*(4), 1155-1175.
Hao, Y., & Su, L. (2005). *China's Foreign Policy Making: Societal Force and Chinese American Policy.* Burlington, VT: Ashgate.

Haro Navejas, F. J. (2005). Política exterior china en Asia Central: construcción del institucionalismo regional. En X. Ríos, *Política exterior de China. La diplomacia de una potencia emergente* (págs. 191-217). Barcelona: Bellaterra.

Harris, J. R. (1998). *Industrial Espionage and Technology Transfer: Britain and Francein the Eighteenth Centrury.* Londres: Ashgate.

Harris, S. (2014). *@War: The Rise of the Military-Internet Complex.* Londres: Houghton Mifflin Harcourt.

Hart, J. A., & Kim, S. (2000). Power in the Information Age. En J. V. Ciprut, *Of Fears and Foes: Security and Insecurity in an Evolving Global Political Economy* (págs. 35-58). Westport, CT: Praeger.

Hay Newman, L. (22 de junio de 2018). *China Escalates Hacks against the US as Trade Tensions Rise*. Recuperado el 24 de junio de 2018, de Wired: https://www.wired.com/story/china-hacks-against-united-states/

Hayden, M. V. (2011). The Future of Things Cyber. *Strategic Studies Quarterly, 5*(1), 3-7.

Helleiner, E., & Kirshner, J. (2014). *The Great Wall of Money: Power and Politics in China's International Monetary Relations.* Ithaca: Cornell University Press.

Herz, M. (2013). Seguridad. En T. Legler, A. Santa Cruz, L. Zamudio, & (eds.), *Introducción a las Relaciones Internacionales: América Latina y la política global* (págs. 123-133). México: Oxford University Press.

Hobart, M., & Schiffman, Z. (2000). *Information Ages: Literacy, Numeracy and the Computer Revolution.* Washington: Johns Hopkins University Press.

Hopf, T. (1998). The Promise of Constructivism in International Relations. *International Security, 23*, 171-200.

Hsü, I. C. (2000). *The Rise of Modern China .* Nueva York : Oxford University Press.

Hu, W., Chan, G., & Zha, D. (2000). Understanding China's Behavior in World Politics: An Introduction. En W. Hu, G. Chan, & D. Zha, *China's International Relations in the 21st Century: Dynamics of Paradigm Shifts* (págs. 1-14). Lamham, Maryland: University Press of America.

Huysmans, J. (1995). Migrants as a Security Problem: Dangers of 'Securitizing' Societal Issues. En R. Miles, & D. Thranhardt, *Migration and European Integration: The Dynamics of Inclusion and Exclusion.* Londres: Pinter Publishers.

Huysmans, J. (1998). The question of the limit: desecuritization and the aesthetics of terrorism in political realism. *Millenium, 27*(3), 569-589.

Huysmans, J. (2006). *The Politics of Insecurity: Fear, Migration and Asylum in the EU.* Nueva York: Routledge.

Ikenberry, J. (2009). Liberal Internationalism 3.0: America and the Dilemmas of World Order. *Perspectives on Politics, 7*(1), 71-87.

Inkster, N. (2013). *China's Cyber Power.* Londres: International Institute for Strategic Studies.

Inkster, N. (2013). Chinese Intelligence in the Cyber Age. *Survival: Global Politics and Strategy, 55*(1), 45-66.

Inkster, N. (2015). The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and*

Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (págs. 29-50). New York: Oxford University Press.

Inkster, N. (2015). The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* New York: Oxford University Press.

Jacques, M. (2009). *When China Rules the World. The End of the Western World and the Birth of a New Global Order.* Nueva York: Penguin.

Jacques, M. (2009). *When China Rules the World: The End of the Western World and the Birth of a New Global Order.* Nueva York: Penguin.

Jakobson, L. (2016). Domestic Actors and the Fragmentation of China's Foreign Policy. En R. S. Ross, & J. I. Bekkevold, *China in the Era of Xi Jinping. Domestic and Foreign Policy Challenges* (págs. 137-164). Washington, DC: Georgetown University Press.

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics, 31*(2), 289-324.

Jiang, W. (27 de febrero de 2014). The Central Internet Security and Information Leading Small Group Established [中央网络安全和信息化领导小组成立：从网络大国迈向网络强国. *Xinhua*.

Johnston, A. I. (2013). How New and Assertive is China's New Assertiveness? *International Security, 37*(4), 7-48.

Joyner, J. (2012). Competing Transatlantic Visions of Cybersecurity. En D. S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (págs. 159-172). Washington: Georgetown University Press.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. *Journal of Strategic Studies, 36*(1), 125-133.

Klein, J. J. (2015). Deterring and Dissuading Cyberterrorism. *Journal of Strategic Security, 8*(4), 23-38.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* New York: Penguin Press.

Klotz, A., & Lynch, C. (2007). *Strategies and Research in Constructivism in International Relations.* Armonk, NY: M. E. Sharpe.

Kaldor, M. (2007). *Human Security.* Cambridge: Polity Press.

Kahin, B., & Nesson, C. (1997). *Borders in Cyberspace.* Cambridge, MA: MIT Press.

Kamphausen, R., Li, D., & Scobell, A. (2009). *Beyond the Strait: PLA Missions Othen than Taiwan.* Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute.

Kang, D. C. (2009). *China Rising: Peace, Power, and Order in East Asia.* Nueva York: Columbia University Press.

Karpf, D. (2012). *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy.* Oxford: Oxford University Press.

Katzenstein, P. (1985). *Small States in World Markets: Industrial Policy in Europe.* Ithaca, NY: Cornell University Press.

Kello, L. (2013). The meaning of cyber revolution: perils to theory and statecraft. *International Security, 38*(2), 7-40.

Kennedy, P. (1987). *The Rise and Fall of Great Powers.* Nueva York: Random House.

Keohane, R. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton: Princeton University Press.
Keohane, R. O., & Nye, J. S. (1977). *Power and Interdependence: World Politics.* Boston: Little Brown.
Keohane, R., & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs , 77*(5), 81-94.
Khanna, P. (2016). *Connectography: mapping the future of global civilization.* Nueva York: Random House.
Khosrowshahi, D. (21 de noviembre de 2017). *2016 Data Security Incident.* Recuperado el 21 de junio de 2019, de Uber Newsroom: https://www.uber.com/newsroom/2016-data-incident/
Kirshner, J. (2010). The Tragedy of Offensive Realism: Classical Realism and the Rise of China. *European Journal of International Relations, 18*(1), 53-75.
Kirshner, J. (2010). The Tragedy of Offensive Realism: Classical Realism and the Rise of China. *European Journal of International Relations, 18*(1), 53-75.
Kissinger, H. (2011). *On China.* Nueva York: Penguin.
Knight, W. (13 de febrero de 2019). *Claves para entender por qué EE.UU. teme que Huawei domine el 5G.* Recuperado el 21 de mayo de 2019, de MIT Technology Review : https://www.technologyreview.es/s/10935/claves-para-entender-por-que-ee-uu-teme-que-huawei-domine-el-5g?fbclid=IwAR0_jtOi_pIlz09ivuyKqBWpBeIl8KsvvIkHZFvyIP51o311fV8rd9vwe0Q
Knockel, J., Ruan, L., Crete-Nishihata, M., & Deibert, R. (14 de agosto de 2018). *(Can't) Picture This: An Analysis of Image Filtering on WeChat Moments.* Recuperado el 5 de octubre de 2018, de The Citizen Lab: https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments/
Kramer, F. D., Starr, S. H., Wentz, L. K., & (eds.). (2009). *Cyberpower and National Security.* Washington, DC: Potomac.
Kramer, F. D., Starr, S. H., Wentz, L. K., & (eds.). (2009). *Cyberpower and National Security.* Washington, DC: Potomac Books.
Kratochwil, F. (1993). The Embarrassment of Changes. *Review of International Studies, 19*, 63-80.
Kratochwil, F., & Ruggie, J. G. (1986). International Organization: A State of the Art on an Art State. *International Organization, 40*(4), 753-775.
Krauthamer, C. (31 de julio de 1995). Why We Must Contain China. *Time*.
Krauthammer, C. (31 de julio de 1995). Why We Must Contain China. *Time*.
Krebs, B. (2014). *Spam Nation: The Inside Story of Organized Cybercrime.* Naperville: Sourcebooks.
Kreiss, D. (2012). *Taking Our Country Back: The Crafting of Networked Politics from Howard Dean to Barack Obama.* Oxford: Oxford University Press.
Krishna-Hensel, S. F. (2007). Preface. Cybersecurity: Perspectives on the Challenges of the Information Revolution. En M. Dunn Cavelty, V. Mauer, S. F. Krishna-Hensel, & (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.* Londres: MPG Books.
Krutskikh, A. (1999). Information Challenges to Security. *International Affairs, 45*(2), 29-37.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. En F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (págs. 24-42). Washington: Potomac Books.

Kupchan, C. (2012). *No One's World. The West, The Rising, and the Coming Global Turn.* Nueva York: Oxford University Press.

Kupchan, C. (2012). *No One's World: the West, the Rising Rest, and the Coming Global Turn.* New York: Oxford University Press.

Kurlantzick, J. (2007). *Charm Offensive. How China's Soft Power Is Transforming the World.* New Haven: Yale University Press.

Kwalwasser, H. (2009). Internet Governance. En F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (págs. 491-524). Washington: Potomac Books.

Lai, H. (2010). *The Domestic Sources of China's Foreign Policy: Regimes, Leadership, Priorities, and Process.* Londres: Routledge.

Lampton, D. M. (2001). *The Making of Chinese Foreign and Security Policy in the Era of Reform.* Stanford: Stanford University Press.

Lampton, D. M. (2008). *The Three Faces of Chinese Power: Might, Money, and Minds.* Berkeley, California: University of California Press.

Landale, J., & Meinrath, S. (4 de noviembre de 2015). *Opinion: The Troubling Stuxnet Effect.* Recuperado el 30 de mayo de 2019, de Christian Science Monitor: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1104/Opinion-The-troubling-Stuxnet-effect

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). *The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate.* Tallinn: 8th International Conference on Cyber Conflict, NATO CCD COE Publications.

Lawson, S. (2013). Beyond cyber doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics , 10*(1), 86-103.

Layne, C. (2006). The Unipolar Illusion Revisited: the Coming End of the United States 'Unipolar Moment'. *International Security, 31*(2), 7-41.

Layne, C. (2009). The Waning of U.S. Hegemony: Myth or Reality? A Review Essay. *International Security, 34*(1), 147-172.

Lee, A. (21 de julio de 2017). *World dominance in three steps: China sets out road map to lead in artificial intelligence.* Recuperado el 14 de febrero de 2019, de South China Morning Post: https://www.scmp.com/tech/enterprises/article/2103568/world-dominance-three-steps-china-sets-out-road-map-lead-artificial

Lee, N. (2013). *Counterterrorism and Cybersecurity. Total Information Awareness.* Nueva York: Springer.

Legro, J. W. (2000). Whence American Internationalism. *International Organization, 54*(2), 253-289.

Lessig, L. (2006). *Code and Other Laws of Cyberspace.* Nueva York: Basic Books.

Levy, S. (2010). *Hackers.* Sebastopol: O'Reilly Media.

Lewis, J. A. (30 de noviembre de 2018). *Technologial Competition and China.* Recuperado el 22 de enero de 2019, de Center for Strategic & International Studies: https://www.csis.org/analysis/technological-competition-and-china

Li, A., & Xu, A. (2015). China's Cybersecurity Situation and the Potential for International Cooperation. En J. R. Lindsay, T. M. Cheung, & D. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Age.* Nueva York: Oxford University Press.

Li, M. (2009). *Soft Power: China's Emerging Strategy in International Politics.* Lanham, Maryland: Lexington.

Li, R. (2009). *A Rising China and Security in East Asia: Identity Construction and Security Discourse.* Londres: Routledge.

Li, T. (22 de noviembre de 2017). *Chinese facial recognition start-up eyes global opportunities beyond public security.* Recuperado el 15 de febrero de 2019, de South China Morning Post: https://www.scmp.com/tech/start-ups/article/2121100/chinese-facial-recognition-start-eyes-global-opportunities-beyond

Li, Y., & Xu, L. (2015). China's Cybersecurity Situation and the Potentional for International Cooperation. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain* (págs. 225-241). New York: Oxford University Press.

Li, Z. (16 de enero de 2016). *Different Values but Similar Visions for Cyberspace.* Recuperado el 17 de enero de 2016, de China-US Focus: https://www.chinausfocus.com/peace-security/different-values-but-similar-visions-for-cyberspace

Libicki, M. (1995). *What Is Information Warfare?* Washington: National Defense University.

Libicki, M. C. (2007). *Conquest in cyberspace: national security and information warfare.* Nueva York: Cambridge University Press.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica: RAND.

Lieberthal, K., & Wang, J. (2012). *Addressing U.S.-China Strategic Distrust .* Washington, Beijing: John L. Thornton China Center, Beijing University Center for International and Strategic Studies.

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *The Journal of Strategic Studies, 35*(3), 401-428.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404.

Lindsay, J. R. (2015). Introduction. China and Cybersecurity: Controversy and Context. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (págs. 1-26). New York: Oxford University Press.

Lindsay, J. R. (2015a). The impact of China cybersecurity: fiction and friction. *International Security, 39*(3), 7-47.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* New York: Oxford University Press.

Lindsay, J. R., & Cheung, T. M. (2015). From Exploitation to Innovation: Adquistion, Absorption, and Application. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China*

and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (págs. 51-86). New York: Oxford University Press.

Loader, B. D. (1997). The Governance of Cyberspace: Politics, Technology, and Global Restructuring. En B. Loader, & (ed.), *The Governance of Cyberspace.* Londres, Nueva York: Routledge.

López, J. (2015). *Influencia de abajo hacia arriba. El cabildeo de los estados y las diásporas en Estados Unidos.* Guadalajara: Universidad de Guadalajara.

Lord, K. M., & Sharp, T. (2011). *America's Cyber Future. Security and Prosperity in the Information Age.* Washington: Center for a New American Security.

Lu, C. (29 de diciembre de 2017). *China-US Cyberspace Relations in the Trump Era.* Recuperado el 29 de diciembre de 2018, de China-US Focus: https://www.chinausfocus.com/peace-security/china-us-cyberspace-relations-in-the-trump-era

Lu, N. (2000). *The Dynamics of Foreign-Policy Decision Making in China.* Boulder: Westview Press.

Lu, W. (15 de diciembre de 2015). *Cyber Sovereignty Must Rule Global Internet.* Recuperado el 30 de agosto de 2018, de Huffington Post: https://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs, 89*(5), 97-108.

Madrigal, A. C. (01 de mayo de 2019). *The End of Cyberspace.* Recuperado el 02 de mayo de 2019, de The Atlantic: https://www.theatlantic.com/technology/archive/2019/05/the-end-of-cyberspace/588340/

Maness, R. C., Valeriano, B., & Jensen, B. (2017). *The Dyadic Cyber Incident and Dispute Dataset*. Recuperado el 8 de julio de 2019, de http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf

Marro, N. (5 de diciembre de 2016). *The five levels of cybersecurity in China*. Recuperado el 9 de febrero de 2019, de China Business Review : http://www.chinabusinessreview.com/the-5-levels-of-information-security-in-china/

Mattelart, A. (2007). *Historia de la sociedad de la información.* Barcelona: Paidós.

Mazanec, B. M., & Thayer, B. A. (2015). *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace.* Nueva York: Palgrave Macmillan.

McLuhan, M. (1964). *Understanding Media.* Nueva York: New American Library.

McEvoy, M. M. (2010). From global village to virtual battlespace: the colonizing of the internet and the extension of realpolitik. *International Studies Quarterly, 54*(2), 381-401.

McPherson, S. H., & Zimmerman, G. (2010). Cyberspace Control. En S. Jasper, *Securing Freedom in the Global Commons* (págs. 83-98). Stanford: Stanford University Press.

Meritalk. (7 de septiembre de 2018). *Gen. Nakasone Lays Out Vision for '5th Chapter' of US Cyber Command*. Recuperado el 17 de septiembre de 2018, de Meritalk: https://www.meritalk.com/articles/nakasone-cyber-command-vision/

Mesa, L. (2009). *El debate sobre la seguridad nacional en la República Islámica de Irán. Estudio del primer mandato del presidente hojateleslam Seyed Mohammed Khatami (1997-2001).* México: El Colegio de México.

Miller, A. L. (2008). The CCP Central Committee's Leading Small Groups. *China Leadership Monitor*(26).

Miller, R. A., & Lachow, I. (2007). *Strategic Fragility: Infrastucture Protection and National Security in the Information Age.* Washington: Center for Technology and National Security Policy.

Miller, T. (2017). *China's Asian Dream.* Londres: Zed Books.

Microsoft News Center. (26 de septiembre de 2003). *China Information Technology Security Certification Center Source Code Review.* Recuperado el 28 de agosto de 2018, de Microsoft: https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/

Ministry of Foreign Affairs of the People's Republic of China. (29 de noviembre de 2014). *The Central Conference on Work Relating to Foreign Affairs Was Held in Beijing*. Obtenido de Ministry of Foreign Affairs of the People's Republic of China: https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1215680.shtml

Mitrany, D. (1948). The Functional Approach to World Organization. *International Affairs, 24*(3), 350-363.

Morales Ruvalcaba, D. (5 de marzo de 2018b). *Interregno hegemónico y competencia interestatal.* Recuperado el 8 de julio de 2019, de Foreign Affairs Latinoamérica: http://revistafal.com/interregno-hegemonico-y-competencia-interestatal/

Morales, D. (2018). Ciclos políticos hegemónicos: implicaciones para la gobernanza internacional. *Brazilian Journal of International Relations, 7*(3), 452-493.

Moravcsik, A. (1998). *Centralization or Fragmentation? Europe Facing Challenges of Deepening, Diversity, and Democracy.* New York: Council on Foreign Relations.

Moravcsik, A. (1999). *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht.* Londres: UCL Press.

Morgan, S. (20 de noviembre de 2017). *Cybersecurity Business Report* . Recuperado el 21 de junio de 2019, de CSO: https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html

Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace.* New York: McGraw Hill.

Morozov, E. (2009). Cyber-scare: the exaggerated fear over digital warfare. *Boston Review, 34*(4).

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom.* Nueva York: Public Affairs.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus, 140*(4), 70-92.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance.* Cambridge, MA: MIT Press.

Mueller, M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace.* Cambridge: MIT Press.

Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance, 13*(2), 237-254.

Muñoz, R. (20 de mayo de 2019). *Google rompe con Huawei, cuyos móviles se quedarían sin sus 'apps' y actualizaciones.* Recuperado el 20 de mayo de 2019, de El País: https://elpais.com/economia/2019/05/19/actualidad/1558294622_546268.html

Nagelhus Schia, N., & Gjesvik, L. (7 de septiembre de 2018a). *The Chinese Cyber Sovereignty Concept (part 1).* Recuperado el 7 de septiembre de 2018, de The Asia Dialogue: http://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/

Nagelhus Schia, N., & Gvesvik, L. (7 de septiembre de 2018b). *The Chinese Cyber Sovereignty Concept (part 2).* Recuperado el 8 de septiembre de 2018, de The Asia Dialogue: http://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-2/

Naím, M. (2014). *El fin del poder.* (M. L. Tapia., Trad.) México: Debate.

Nathan, A. J. (2016). China's Rise and International Regimes. Does China Seek to Overthrow Global Norms. En R. S. Ross, & J. I. Bekkevold, *China in the Era of Xi Jinping. Domestic and Foreign Policy Challenges* (págs. 165-195). Washington , DC: Georgetown University Press.

Nathan, A. J. (2016). China's Rise and International Regimes. Does China Seek to Overthrow Global Norms? En R. S. Ross, J. I. Bekkevold, & (eds.), *China in the Era of Xi Jinping: Domestic and Foreign Policy Challenges* (págs. 165-195). Washington, DC: Georgetown Univerisity Press.

Naughton, B. (2014). China's Economy: Complacency, Crisis and the Challenge of Reform. *Daedalus, 143*(2), 14-25.

Neuromation. (06 de abril de 2018). *Artificial Intelligence in Japan (R&D, Market and Industry Analysis).* Recuperado el 16 de febrero de 2019, de Neuromation: https://medium.com/neuromation-blog/artificial-intelligence-in-japan-r-d-market-and-industry-analysis-e086a38639ec

Newitz, A. (16 de septiembre de 2013). *The Bizarre Evolution of the Word 'Cyber'.* Recuperado el 12 de noviembre de 2018, de Gizmodo: https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487

Norris, P. (2001). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide.* Cambridge: Cambridge University Press.

Nye, J. (2010). *Cyber Power.* Belfer Center for Science and International Affairs, Harvard Kennedy School. Cambridge: Harvard University.

Nye, J. S. (2004a). *Soft Power: The Means to Success in World Politics.* New York: Public Affairs.

Nye, J. S. (2004b). *Power in the Global Information Age: From Realism to Globalization.* Londres: Routledge.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly, 5*(4), 18-38.

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly, 5*(4), 18-36.

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly, 5*(4), 18-38.

Nye, J. S. (9 de marzo de 2018). *How Will New Cybersecurity Norms Develop?* Recuperado el 4 de junio de 2018, de China-US Focus: https://www.chinausfocus.com/peace-security/how-will-new-cybersecurity-norms-develop

Nye, J. S., & Owens, W. A. (1996). America's Information Edge. *Foreign Affairs*, 20-36.

Oath. (03 de octubre de 2017). *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft.* Recuperado el 21 de junio de 2019, de Oath: https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

O'Day, A. (2004). *Cyberterrorism.* Aldershot: Ashgate.

Ohm, P. (2008). The Myth of the Superuser: Fear, Risk, and Harm Online. *Univeristy of California Davis Law Review, 41*(4), 1327-1402.

Owens, W. A., Dam, K. W., Lin, H. S., & (eds.). (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Adquisition and Use of Cyberattack Capabilities.* Washington, DC: National Academies Press.

Owens, W., Dam, K., & Lin, H. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: National Research Council, National Academies Press.

Palfrey, J. (2010). Four phases of internet regulation. *Social Research, 77*(3), 981-996.

Papp, D., Alberts, D., & Tuyahov, A. (1997). Historical Impacts of Information Technologies: An Overview. En D. Alberts, & D. Papp, *The Information Age: An Anthology of Its Impacts and Consequences* (págs. 13-35). Washington: National Defense University.

Pariser, E. (2011). *The Filter Bubble. What the Internet is Hiding from You.* Nueva York: Penguin Press.

Perloff, R. M. (2014). *The Dynamics of Political Communication. Media and Politics in a Digital Age.* Nueva York, Londres: Routledge.

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: United States.* Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Perrit, H. H. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strenghtening National and Global Governance. *Indiana Journal of Global Studies, 5*(2), 423-442.

Perry, S., & Roda, C. (2017). *Human Rights and Technology: Digital Tightrope.* Londres: Palgrave Macmillan.

Peterson, T. L. (2011). *Nightwork. A History of Hacks and Pranks at MIT.* Cambridge: MIT Press.

Petterson, D. (2013). Offensive Cyber Weapons: Construction, Development, Employment. *Journal of Strategic Studies, 36*(1), 120-124.

Pillsbury, M. (2015). *The Hundred Year Marathon: China's Secret Strategy to Replace America as the Global Superpower.* Nueva York: Henry Holt.
Pillsbury, M. (2015). *The Hundred Year Marathon: China's Secret Strategy to Replace America's as the Global Superpower.* Nueva York: Henry Holt.
Pollpeter, K. (2015). Chinese Writings on Cyberwarfare and Coercion. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (págs. 138-162). New York: Oxford University Press.
Ponemon Institute. (junio de 2017). *2017 Cost of Data Breach Study*. Recuperado el 21 de junio de 2019, de IBM: https://www.ibm.com/downloads/cas/ZYKLN2E3
Posen, B. (2014). *Restraint: A New Foundation for US Grand Strategy.* Ithaca: Cornell University Press.
Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internte Freedom.* Urbana, Chicago, Springfield: University of Illinois Press.
Qu, W. (2010). *China's Path to Informatization.* Singapur: Cengage Learning Asia.
Rachman, G. (1996). Containing China. *Washington Quarterly, 19*(1), 129-140.
Rattray, G. J. (2001). *Strategic Warfare in Cyberspace.* Cambridge: MIT Press.
Raud, M. (2016). *China and Cyber: Attitudes, Strategies, Organisation.* Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence.
Reardon, R., & Nazli, C. (2012). *The Role of Cyberspace in International Relations.* San Diego, CA: ISA Annual Convention.
Reveron, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington, DC: Georgetown University Press.
Reveron, D. S. (2012). An Introduction to National Security and Cyberspace. En D. S. Reveron, *Cyberspace and National Security: Threats, Oppotunities, and Power in a Virtual World* (págs. 3-20). Washington, DC: Geogetown University Press.
Reveron, D. S., & (eds.). (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington, DC: Georgetown University Press.
Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 523-544.
Ridge, T. (23 de abril de 2002). Remarks by Homeland Security Director Tom Ridge to the Electronics Industry Alliance. (W. H. Secretary, Entrevistador)
Riordan, S. (2019). *Cyberdiplomacy: Managing Security and Governance.* Cambridge: Polity Press.
Riquelme, R., & Martinez, L. A. (29 de mayo de 2018). *Glosario mínimo de términos de ciberseguridad.* Recuperado el 31 de mayo de 2018, de El Economista: https://www.eleconomista.com.mx/gestion/Glosario-minimo-de-terminos-de-ciberseguridad-20180528-0073.html
Risse, T. (2000). Let's Argue! Communicative Action in World Politics. *International Organization, 16*(4), 523-544.
Risse-Kappen, T. (1995). *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures, and International Institutions.* Cambridge: Cambridge University Press.
Rocha, A., & Morales, D. (2018). El poder nacional-internacional de los Estados. Una propuesta trans-estructural. *Geopolítica, 9*(1), 137-169.

Roberts, M. E. (2018). *Censored. Distraction and Diversion Inside China's Great Firewall.* Princeton: Princeton University Press.
Rosecrance, R. (1999). *The Rise of the Virtual State: Wealth and Power on the Coming Century.* Nueva York: Basic Books.
Rosenau, J. N. (1990). *Turbulence in World Politics: A Theory of Change and Continuity.* Princeton, NJ: Princeton University Press.
Rosenau, J. N.; Singh, J. P. (2002). *Information Technology and Global Politics: The Changing Scope of Power and Governance.* Alabany: State University of New York Press.
Rosenau, James N.; Czempiel, Ernst. (1992). *Governance Without Government: Order and Change in World Politics.* Cambridge: Cambridge University Press.
Ross, R. (1997). Beijing as a Conservative Power. *Foreign Affairs, 76*(2), 33-44.
Rothkopf, D. J. (1998). Cyberpolitik: the Changing Nature of Power in Information Age. *Journal of International Affairs, 51*(2), 321-356.
Rothkopf, D. J. (1999). The Disinformation Age. *Foreign Policy*(114), 82-96.
Rothschild, E. (1995). What is Security? *Daedalus, 124*(3), 53-82.
Rovner, J., & Moore, T. (2017). Does the Internet Need a Hegemon? *Journal of Global Security Studies, 2*(3), 184-203.
Roy, D. (2013). *Return of the Dragon .* Nueva York : Columbia University Press.
Rozman, G. (2013). *China's Foreign Policy. Who Makes It and How Is It Made?* Londres: Palgrave MacMillan.
Ruggie, J. G. (1983). Continuity and Transformation in the World Polity: Toward a Neorealist Theory Synthesis. *World Politics, 35*(2), 261-285.
Ruggie, J. G. (1998). *Constructing the World Polity: Essays on International Institutionalism.* Londres: Routledge.
Russett, B., & Antholis, W. (1993). *Grasping the World Polity: Essays on International Institutionalism.* Londres: Routledge.
Ryan, C. (1991). *Prime Time Activism: Media Strategies for Grass Roots Organizing.* Boston: South End Press.
Schmidt, E., & Cohen, J. (2013). *The New Digital Age.* Nueva York: Knopf.
Schmidt, M. (13 de marzo de 2012). New interest in hacking as threat to security. *The New York Times*.
Schmitt, M. N. (2017). *Tallin Manual on the International Law Applicable to Cyber Warfare.* Nueva York: Cambridge University Press.
Schneier, B. (2012). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive.* Indianapolis: Wiley.
Schneier, B. (26 de noviembre de 2012). When It Comes to Security, We're Back to Feudalism. *Wired*.
Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Nueva York: W.W. Norton.
Schultze, C. (1973). The Economic Content of National Security Policy. *Foreign Affairs*(3), 523-540.
Schwartz, E. (1996). *NetActivism: How Citizens Use the Internet.* Sebastopol: Songline Studios.

Schweller, R., & Pu, X. (2011). After Unipolarity: China's Vision of International Order in an Era of U.S. Decline. *36*(1), 47-72.
Schweller, R., & Pu, X. (2011). After Unipolarity: China's Vision of International Order in an Era of U.S. Decline. *International Security, 36*(1), 47-72.
SAC. (15 de enero de 2016). *全国信息安全标准化技术委员会换届大会在京召开.*[The National Information Security Standardization Technical Committee Was Held in Beijing] Recuperado el 10 de noviembre de 2018, de [National Standardization Managament Commitee]国家标准化管理委员会: http://www.sac.gov.cn/xw/bzhxw/201601/t20160115_200544.htm
Sanger, D. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power.* Nueva York: Crown.
Sanger, D. E. (1 de junio de 2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*.
Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* Nueva York: Broadway Books.
Sanger, D. E., Barnes, J. E., Zhong, R., & Santora, M. (26 de enero de 2019). *In 5G Race with China, U.S. Pushes Allies to Fight Huawei.* Recuperado el 28 de enero de 2019, de The New York Times: https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html
Santa Cruz, A. (2000). *Un debate teórico empíricamente ilustrado: la construcción de la soberanía japonesa, 1853-1902.* Guadalajara: Universidad de Guadalajara.
Santa Cruz, A. (2012). *La política sin fronteras o la ubicuidad de lo distintivo: ensayos escogidos de Peter Katzenstein.* México: CIDE.
Santa Cruz, A. (2013). Constructivismo. En T. Legler, A. Santa Cruz, & L. Zamudio, *Introducción a las Relaciones Internacionales: América Latina y la política global* (págs. 36-50). México: Oxford University Press.
Sassen, S. (1998). On the Internet and Sovereignty. *Indiana Journal of Global Legal Studies, 5*(2), 545-559.
Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* Nueva York: Public Affairs.
Segal, A. (2018). When China Rules the Web: Technology in the Service of the State. *Foreign Affairs, 97*(5), 10-18.
Shcwartau, W. (1996). *Information Warfare.* Emeryville: Publisher Group West.
Shambaugh, D. (1996). Containment or Engagement of China: Calculating Beijing's Responses. *International Security, 21*(2), 180-209.
Shambaugh, D. (1996). Containment or Engagement of China: Calculating Beijing's Responses. *International Security, 21*(2), 180-209.
Shambaugh, D. (2012). *Tangled Titans: The United States and China.* Lanham: Rowman & Littlefield.
Shambaugh, D. (2013). *China Goes Global. The Partial Power.* Nueva York: Columbia University Press.
Shambaugh, D. (2013). *China Goes Global: the Partial Power.* Nueva York: Oxford University Press.
Shapiro, A. L. (1999a). *The Control Revolution.* Nueva York: Public Affairs.

Shapiro, I., & Wendt, A. (1992). The Difference that Realism Makes. *Politics & Society*(2).
Sheldon, R., & McReynolds, J. (2015). Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (págs. 188-222). New York: Oxford University Press.
Sheehan, M. (2005). *International Security: An Analytical Survey.* Boulder: Lynne Rienner.
Shenk, D. (1997). *Data Smog: Surviving the Information Glut.* Nueva York: Harper Edge.
Shih, G. (22 de abril de 2015). *Huawei CEO questions China's cybersecurity policies.* Recuperado el 16 de febrero de 2019, de Christin Science Monitor: https://www.csmonitor.com/Technology/2015/0422/Huawei-CEO-questions-China-s-cybersecurity-policies
Shirk, S. (2007). *China: Fragile Superpower.* Nueva York: Oxforrd University Press.
Shirk, S. (2010). *Changing Media, Changing China.* Nueva York: Oxford University Press.
Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs, 90*(1), 28-41.
Sierra Caballero, F. (2003). La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Pública*(3), 253-268.
Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media.* Boston, Nueva York: Houghton Mifflin Harcourt.
Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Nueva York: Oxford University Press.
Snyder, J. (1991). *Myths of Empire.* Ithaca, NY: Cornell University Press.
Sobers, R. (17 de abril de 2019). *60 Must-Know Cybersecurity Statistics for 2019*. Recuperado el 21 de junio de 2019, de Varonis Data Lab: https://www.varonis.com/blog/cybersecurity-statistics/
South China Morning Post; Abacus; Edith Yeung. (2019). *China Internet Report 2019.* Hong Kong: South China Morning Post.
Spade, J. M., & Caton, J. L. (2012). *Information as Power: China's Cyber Power and America's National Security.* Carlisle Barracks, PA: Army War College Information in Warfare Group.
Starr, S. H. (2009). Toward a Preliminary Theory of Power. En F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (págs. 43-88). Washington: Potomac Books.
Starrs, S. (2013). American Economic Power Hasn't Declined- It Globalized! Summoning the Data and Taking Globalization Seriously. *International Studies Quarterly, 57*(4), 817-830.
State Council. (26 de mayo de 2015). *Full text: China's Miltary Strategy*. Recuperado el 06 de noviembre de 2018, de China Daily: http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm
Steinfeld, E. S. (2010). *Playing our Game: Why China's Economic Rise Doesn't Threaten the West.* Oxford: Oxford University Press.
Steinfeld, E. S. (2017). Teams of Rivals: China, the United States, and the Race to Develop Technologies for a Sustainable Future. En J. deLisle, & A. Goldstein, *China's Global*

Engagement: Cooperation, Competition, and Influence in the 21st Century (págs. 91-121). Washington: Brookings Institution Press.

Stenslie, S., & Chen, G. (2016). Xi Jinping's Grand Strategy: From Vision to Implementation. En R. S. Ross, & J. I. Bekkevold, *China in the Era of Xi Jinping. Domestic and Foreign Policy Challenges* (págs. 117-136). Washington, DC: Georgetown University Press.

Stenslie, S., & Chen, G. (2016). Xi Jinping's Grand Strategy: From Vision to Implementation . En R. S. Ross, & J. I. Bekkevold, *China in the Era of Xi Jinping: Domestic and Foreign Policy Challenges* (págs. 117-136). Washington, DC: Georgetown University Press .

Sterling-Folker, J. (2013). *Making Sense of Internationl Relations Theory:.* Londres: Lyenne Rienner.

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy through the Maza of Computer Espionage.* Nueva York: Doubleday.

Stokes, M. A. (2015). The Chinese People´s Liberation Army Computer Network Operations Infrastructure. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Straetgy and Politics in the Digital Domain* (págs. 163-187). New York: Oxford University Press.

Stokes, M. A. (2015a). The Chinese People´s Liberation Army Computer Network Operations Infrastructure. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Straetgy and Politics in the Digital Domain* (págs. 163-187). New York: Oxford University Press.

Stone, J. (2012). Cyber War Will Take Place! *Journal of Strategic Studies, 36*(1), 101-108.

Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media.* Princeton: Princeton University Press.

Sutter, R. G. (2013). *Foreign Relations of the PRC.* Lanham, Maryland: Rowman & Littlefield.

Sutter, R. G. (2016). *Chinese Foreign Relations: Power and Policy since the Cold War.* Lanham, Maryland: Rowman & Littlefield.

Swaine, M. D. (1996). *The Role of the Military in National Security Policymaking.* Santa Monica: Rand.

Swaine, M., & Tellis, A. (2000). *Interpreting China's Grand Strategy. Past, Present, and the Future.* Santa Monica, California : RAND.

Symantec. (marzo de 2018). *Internet Security Threat Report (vo.23)*. Recuperado el 21 de junio de 2019, de Symantec: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Tammen, R. L., & (ed.). (2000). *Power Transitions Strategies for the 21st Century.* Nueva York: Chatham House.

Tammen, Ronald L. et al. (2000). *Power Transtitions: Strategies for the 21st Century.* Nueva York : Chatham House.

The Joint Chief of Staff. (8 de junio de 2018). *Joint Publication 3-12 Cyberspace Operations*. Recuperado el 14 de enero de 2019, de The Joint Chieff of Staff: https://fas.org/irp/doddir/dod/jp3_12.pdf

The Joint Chiefs of Staff. (2006). *Homeland Security Digital Library*. Recuperado el 14 de enero de 2019, de https://www.hsdl.org/?view&did=35693

Thomas, T. L. (2009). *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force.* Fort Leavenworth, KS: Foreign Military Studies Office.

Tickner, A. J. (1995). Re-visioning Security. En K. Booth, & S. Smith, *International Relations Theory Today* (págs. 175-197). Cambridge: Polity Press.

Toca, G. (10 de abril de 2019). *5G: la otra cara de la guerra digital.* Recuperado el 11 de abril de 2019, de Esglobal: https://www.esglobal.org/5g-la-otra-cara-de-la-guerra-digital/?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork

Toffler, A. (1980). *Third Wave.* Nueva York: Bantam Books.

Toffler, A., & Toffler, H. (1993). *War and Anti-War.* Nueva York: Warner Books.

Treviño, J. (2016). Organizaciones de la sociedad civil y la securitización de la migración internacional indocumentada en México. *Foro Internacional, 56*(2).

Tuchman, M. (1989). Redefining Security. *Foreign Affairs, 68*, 162-177.

Ullman, R. (1983). Redefining Security. *International Security, 8*(1), 129-153.

U.S. Chamber of Commerce. (2014). *2014 Cybersecurity Education & Framework Awareness Campaign. Improving Today, Protecting Tomorrow*. Recuperado el 14 de enero de 2019, de U.S. Chamber of Commerce: https://www.uschamber.com/cyber

U.S. Congressional Budget Office. (25 de junio de 2014). *S. 2519. National Cybersecurity and Communicatins Integration Centre Act of 2014*. Recuperado el 14 de enero de 2019, de U.S. Congresional Budget Office: https://www.cbo.gov/publication/45594

U.S. Cyber Command. (2018). *Cyber Command History.* Recuperado el 23 de enero de 2019, de U.S. Cyber Command: https://www.cybercom.mil/About/History/

U.S. Cyber Command. (junio de 2018). *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Recuperado el 14 de junio de 2019, de U.S. Cyber Command: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

U.S. Cyber Command. (abril de 2018a). *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command.* Recuperado el 23 de enero de 2019, de U.S. Cyber Command: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

U.S. Deparment of Defense. (30 de octubre de 2003). *Information Operation Roadmap.* Recuperado el 5 de octubre de 2018, de NSA Archive: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

U.S. Department of Defense . (abril de 2015). *The Department of Defense Cyber Strategy* . Recuperado el 14 de enero de 2019, de http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

U.S. Department of Defense. (2008). *National Defense Strategy of the United States.* Washington: U.S. Department of Defense.

U.S. Department of Defense. (2011). *National Military Strategy of the United States of America: Redefining America's Military Leadership*. Recuperado el 14 de enero de 2019, de https://www.hsdl.org/c/2011-national-military-strategy-redefining-americas-military-leadership/

U.S. Department of Defense. (3 de julio de 2011). *Strategy for Operating in Cyberspace.* Recuperado el 5 de diciembre de 2018, de U.S. Department of Defense: www .defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in _Cyberspace_July_2011.pdf.

U.S. Department of Defense. (2012). *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense* . Recuperado el 14 de enero de 2019, de http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf

U.S. Department of Defense. (2018). *Summary of 2018 National Defense Strategy of the United States of America.* Recuperado el 30 de mayo de 2019, de https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Department of Defense, Office of General Counsel. (2015). *Law of War Manual*. Recuperado el 14 de enero de 2019, de U.S. Department of Defense: http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf

U.S. Department of Homeland Security. (2003). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*. Recuperado el 14 de enero de 2019, de U.S. Department of Homeland Security: https://www.dhs.gov/homeland-security-presidential-directive-7

U.S. Department of Homeland Security. (2009). *National Infrastructure Protection Plan 2009*. Recuperado el 14 de enero de 2019, de U.S. Department of Homeland Security: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U.S. Department of Homeland Security. (2011). *Blueprint for a Secure Cyber Future. The Cybersecurity Strategy ofr the Homeland Security Enterprise*. Recuperado el 5 de enero de 2019, de U.S. Department of Homeland Security: http://www.dhs.gov/blueprint-secure-cyber-future

U.S. Department of Homeland Security. (marzo de 2013). *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity.* Recuperado el 28 de febrero de 2019, de Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf

U.S. Department of Homeland Security. (2014). *2014 Quadrennial Homeland Security Review*. Recuperado el 5 de enero de 2019, de U.S. Department of Homeland Security: http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf

U.S. Department of Homeland Security. (junio de 2014). *The 2014 Quadrennial Homelanda Security Review* . Recuperado el 14 de enero de 2019, de https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

U.S. Department of Homeland Security, Office of Inspector General. (14 de julio de 2014). *Implementation Status of the Enhanced Cybersecurity Services Program*. Recuperado el 14 de enero de 2019, de U.S. Department of Homeland Security: https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf

U.S. Department of Justice. (2 de julio de 2018). *Report of the Attorney General's Cyber Digital Task Force.* Recuperado el 23 de enero de 2019, de U.S. Department of Justice: https://www.justice.gov/ag/page/file/1076696/download

U.S. Department of Justice. (16 de octubre de 2018b). *Cybersecurity Unit*. Recuperado el 10 de noviembre de 2018, de U.S. Department of Justice: https://www.justice.gov/criminal-ccips/cybersecurity-unit

U.S. Government. (22 de mayo de 1998). *Critical Infrastructure Protection. Presidential Decision Directive 63.* Recuperado el 5 de diciembre de 2018, de Federation of American Scientists: www.fas.org/irp/offdocs/pdd/pdd-63.htm.

U.S. Government White House . (septiembre de 2018). *National Cyber Strategy of the United States of America.* Recuperado el 23 de enero de 2019, de U.S. Government White House: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

U.S. Government White House. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure*. Obtenido de U.S. Government White House: https://obamawhitehouse.archives.gov/cyberreview/documents/

U.S. Government White House. (2009). *The Comprehensive National Cybersecurity Initiative*. Recuperado el 14 de enero de 2019, de U.S. Government White House: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

U.S. Government White House. (2011). *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*. Recuperado el 10 de enero de 2019, de U.S. Government White House: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

U.S. Government White House. (2015). *National Security Stratey*. Recuperado el 7 de enero de 2019, de U.S. Government White House: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

U.S. House Committee on Homeland Security. (28 de junio de 2014). *National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCC Act). H.R. 3696*. Obtenido de U.S. House Committee on Homeland Security: https://www.congress.gov/bill/113th-congress/house-bill/3696

U.S. House of Representatives. (30 de noviembre de 2011). *Cyber Intelligence Sharing and Protection Act* . Recuperado el 31 de mayo de 2019, de U.S Government Information: https://www.govinfo.gov/content/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf

Väyrynen, R. (1995). Concepts of Security Revisited. *Mershon International Studies Review, 39*(2), 259-262.

Valeri, L. (2000). Securing Internet Society: Toward an International Regime for Information Assurance. *Studies in Conflict and Terrorism, 23*(2), 129-146.

Valeriano, B., & Jensen, B. (15 de enero de 2019). *The Myth of the Cyber Offense: the Case for Restraint.* Recuperado el 17 de enero de 2019, de CATO Institute:

https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint
Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: cyber conflict in the international system.* Nueva York: Oxford University Press.
Vaidhyanathan, S. (2011). *The Googlization of Everything.* Berkeley, Los Ángeles, California: University of California Press.
Vaidhyanathan, S. (2018). *Antisocial Media.* Nueva York: Oxford University Press.
Vaishnav, C., Choucri, N., & Clark, D. (2013). Cyber International Relations as an Integrated System. *Environment Systems and Decisions, 33*(4), 561-576.
Van Evera, S. (1997). *Guide to Methods for Students of Political Science.* Ithaca, Londres: Cornell University Press.
Varonis Data Lab. (2018). *Data Under Attack: 2018 Globa Data Risk Report from the Varonis Data Lab*. Recuperado el 21 de junio de 2019, de Varonis Data Lab: https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf
Velandia, K. (2 de marzo de 2017). *¿Cuáles son las armas con las que se combate en el ciberespacio, el nuevo frente de guerra del siglo XXI? (Y qué daño te pueden causar)*. Recuperado el 12 de marzo de 2018, de BBC: https://www.bbc.com/mundo/noticias-38926665
Ventre, D. (. (2014). *Chinese Cybersecurity and Defense.* Londres: Wiley.
Vida Liy, M., & Mars, A. (21 de mayo de 2019). *Donald Trum da una tregua de tres meses para imponer el veto a Huawei.* Recuperado el 21 de mayo de 2019, de El País: https://elpais.com/economia/2019/05/21/actualidad/1558417928_415258.html
Waldrop, M. (1998). Is there an information revolution? En C. R. Henry, & E. C. Peartree, *Information Revolution and International Security* (págs. 1-9). Washington: Center for Strategic and International Studies Press.
Walker, R. B. (1993). *Inside/Outside: International Relations ads Political Theory.* Cambridge: Cambridge University Press.
Walt, S. (1994). The Reinaissance of Security Studies. *International Studies Quarterly, 35*(2), 211-239.
Walt, S. M. (2010). *Is the Cyber Threat Overblown?* Recuperado el 2 de enero de 2018, de Foreign Policy: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown
Waltz, K. N. (1959). *Man, the State, and War.* Nueva York: Columbia University Press.
Waltz, K. N. (1979). *Theory of International Politics.* Readings: Addison Wesley.
Waever, O. (1995). Securitization and Desecuritization. En R. D. Lipschutz, *On Security* (págs. 46-86). New York: Columbia University Pres.
Wang, T. (14 de febrero de 2017). *全国已建成“网安警务室”家* [The nation has established Digital Security Policy Office]. Recuperado el 16 de febrero de 2019, de Guangming Ribao: http://epaper.gmw.cn/gmrb/html/2017-02/14/nw.D110000gmrb_20170214_2-04.htm
Weldes, J. (1996). Constructing National Interest. *European Journal of International Relations, 2*(3), 335-370.

Webster, F. (1997). What Information Society? En D. S. Papp, D. Alberts, & (eds.), *The Information Age: Anthology on Its Impact and Consequences.* Washington, DC: National Defense University Press.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism, 28*(2), 129-149.

Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges.* Washington: U.S. Institute of Peace Press.

Weiss, T. G., & Wilkilson, R. (2014). Global Governance to the Rescue: Saving International Relations. *Global Governance, 20*(1), 19-36.

Wendt, A. (1987). The Agent-Structure Problem in International Relation Theory. *International Organization, 46*(2), 391-425.

Wendt, A. (1992). Anarchy is What States Make of It: the Social Construction of Power Politics. *International Organization, 46*(2), 391-425.

Wendt, A. (1995). Constructing International Politics. *International Security, 20*(1), 71-78.

Wendt, A. (1999). *Social Theory of International Politics.* Cambridge: Cambridge University Press.

Westad, O. A. (2012). *Restless Empire: China and the World Since 1750.* Londres : Bodley Head.

White House. (2003). *The National Strategy to Secure Cyberspace.* Washington: The White House.

White House. (1 de octubre de 2009). *Press Release: National Cybersecurity Awareness Month.* Recuperado el 5 de diciembre de 2018, de White House. U.S. Government: www.whitehouse.gov/the_press_office/Presidential-Proclamation-National-Cybersecur ity-Awareness-Month/.

White House. (mayo de 2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Recuperado el octubre de 2018, de U.S. Government.

White House. (2018). *Information Technology. White House Fiscal Year 2018 Budget*. Recuperado el 13 de febrero de 2019, de White House: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf

White House. (28 de septiembre de 2018a). *Presidential Proclamation on National Cybersecurity Awareness.* Recuperado el 5 de diciembre de 2018, de White House, U.S. Government: https://www.whitehouse.gov/presidential-actions/presidential-proclamation-national-cybersecurity-awareness-month-2018/

White House. (2018b). *Information Technology, White House FY 2017 Budget.* Recuperado el 28 de febrero de 2019, de White House: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf

Williams, M. C. (1997). The Institutions of Security: Elements of a Theory of Securrity. *Cooperation and Conflict , 32*(3), 287-307.

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly, 47*(4), 511-529.

Williams, P. D. (2008). *Security Studies: An Introduction.* Abingdon: Routledge.

Wills, J. (2017). *Tug of War. Surveillance Capitalism, Military Contracting, and the Rise of the Security State.* Montreal, Kingston, Londres, Chicago: McGill-Queen's University Press.

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine.* París: Hermann.

Wines, D. (4 de mayo de 2011). *China Creates New Agency for Patrolling Internet.* Recuperado el 15 de julio de 2018, de New York Times: https://www.nytimes.com/2011/05/05/world/asia/05china.html

Wolfers, A. (1952). National Security as an Ambiguous Symbol. *Political Science Quarterly, 67*(4), 481-502.

Wu, I. S. (2008). *Information, identity and institutions.* Institute for the Study of Diplomacy. Washington, DC: Georgetown University.

Wu, T. (2011). *The Master Switch. The Rise and Fall of Information Empires.* Nueva York: Alfred A. Knopf.

Wu, X. (2004). Four Contradictions Constraining China's Foreign Policy Behavior . En S. Zhao, *Chinese Foreign Policy. Pragmatism and Strategic Behavior* (págs. 58-65). Nueva York, Londres: M. E. Sharpe.

Xi, J. (2014). *The Governance of China.* Beijing: Foreign Languages Press.

Xi, J. (27 de febrero de 2014a). *Xi Jinping leads internet security group*. Recuperado el 27 de octubre de 2018, de China Daily: http://www.chinadaily.com.cn/china/2014-02/27/content_17311358.htm

Xi, J. (25 de abril de 2016). *习近平在网信工作座谈会上的讲话全文发表*. Recuperado el 09 de febrero de 2019, de Xinhuanet: http://www.xinhuanet.com/politics/2016-04/25/c_1118731175.htm

Xinhua. (16 de diciembre de 2015). *China allows no compromise on cyberspace.* Recuperado el 16 de julio de 2018, de Xinhua Net: http://www.xinhuanet.com//english/2015-12/16/c_134924241.htm

Xinhua. (25 de marzo de 2016). *China's First National NPO in cybersecurity founded.* Recuperado el 16 de febrero de 2019, de Renmin Wang: http://en.people.cn/business/n3/2016/0325/c90778-9035817.html

Xinhua. (14 de enero de 2017c). *Procuratorates approve arrest of 19,000 telecom fraud suspects.* Recuperado el 28 de octubre de 2018, de Xinhua: http://news.xinhuanet.com/english/2017-01/14/c_135982423.htm

Xinhua. (1 de marzo de 2017). *Full Text: International Strategy of Cooperation on Cyberspace.* Recuperado el 28 de agosto de 2018, de Xinhua Net: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm

Xinhua. (24 de enero de 2017a). *Thousands of illegal apps taken offline in South China*. Recuperado el 31 de octubre de 2018, de Xinhuanet: http://www.xinhuanet.com//english/2017-01/23/c_136007345.htm

Xinhua. (25 de agosto de 2017b). *China to punish illegal publicity on internet forums.* Recuperado el 07 de enero de 2019, de Xinhuanet: http://www.xinhuanet.com//english/2017-08/25/c_136554917.htm

Yang, G. (2009). *The Power of the Internet in China. Citizen Activism Online.* Nueva York: Columbia University Press.

Ye, Z. (2015). From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. En J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (págs. 123-137). New York: Oxford University Press.

Yong, D. (1999). Conception of National Interests: Realpolitik, Liberal Dilemma, and the Possibility of Change. En D. Yong, & F.-l. Wang, *In the Eyes of the Dragon. China Views the World* (págs. 47-72). Nueva York: Rowman & Littlefield.

Yong, D.; Wang, F. L. (2005). *China Rising: Power and Motivation in Chinese Foreign Policy.* Lanham, Maryland: Rowman & Littlefield.

Young, D. (2012). *The Party Line. How Media Dictates Public Opinion in Modern China.* Singapur: Wiley.

Yuan, L. (03 de octubre de 2018). *Private Businesses Built Modern China. Now Gov't Is Pushing Back.* Recuperado el 21 de mayo de 2019, de The New York Times: https://www.nytimes.com/2018/10/03/business/china-economy-private-enterprise.html

Zetter, K. (11 de julio de 2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Nueva York: Crowm Publishing. Recuperado el 30 de mayo de 2019, de Wired.

Zetter, K. (25 de septiembre de 2015). *US and China Reach Historic Agreement on Economic Espionage*. Recuperado el 21 de junio de 2019, de Wired: https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/

Zhang, S. (28 de julio de 2016). *China sets goals of informatization*. Recuperado el 02 de noviembre de 2018, de CRI: http://english.cri.cn/12394/2016/07/28/3821s935816.htm

Zhao, Y. (2008). *Communication in China. Political Economy, Power, and Conflict.* Londres: Rowman & Littlefield.

Zheng, S. (23 de julio de 2017). *VPN crackdown an 'unthinkable' trial by firewall for China's research world.* Recuperado el 23 de febrero de 2019, de South China Morning Post: https://www.scmp.com/news/china/policies-politics/article/2103793/vpn-crackdown-unthinkable-trial-firewall-chinas

Zheng, W. (26 de marzo de 2019). *China's formet internet tsar Lu Wei jailed for 14 years for bribery.* Recuperado el 27 de marzo de 2019, de South China Morning Post: https://www.scmp.com/news/china/politics/article/3003357/chinas-former-internet-tsar-lu-wei-jailed-14-years-bribery

Zheng, Y., & Wen, C. (2016). The Development of China's Formal Political Structures. En R. S. Ross, & J. I. Bekkevold, *China in the Era of Xi Jinping: Domestic and Foreign Policy Challenges* (págs. 32-69). Washington, DC: Georgetown University Press.

Zhuge, J., Lion, G., Duan, H., & Roberts, T. (2015). Investigating the Chinese Online Underground Economy. En S. a. China and Cybersecurity: Espionage, *Lindsay, Jon R.; Cheung, Tai Ming; Reveron, Derek S.* (págs. 87-120). New York.

Zittrain, J. (2008). *The future of the internet and how to stop it.* New Haven: Yale University Press.

Zuo, M. (28 de julio de 2016). *China aims to become internet superpower by 2050*. Recuperado el 03 de noviembre de 2018, de South China Morning Post: https://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020