OASIS
OBSERVATORIO DE ANÁLISIS DE LOS SISTEMAS INTERNACIONALES

Oasis
ISSN: 1657-7558
ISSN: 2346-2132
Universidad Externado de Colombia

Patiño Orozco, Germán Alejandro
Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos
Oasis, núm. 34, 2021, Julio-Diciembre, pp. 107-126
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/16577558.n34.07

Disponible en: https://www.redalyc.org/articulo.oa?id=53169476007

Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos

Germán Alejandro Patiño Orozco*

RESUMEN

Este artículo aporta algunas consideraciones sobre el debate acerca de la relevancia de la ciberseguridad como herramienta en la competencia internacional. El argumento central sostiene que las acciones en el campo de ciberseguridad representan una pieza clave en el marco de las relaciones competitivas de carácter gubernamental. A través del ejercicio de comparar el modelo de ciberseguridad chino y estadounidense se sostiene que este terreno se ha convertido en un imperativo de seguridad nacional para ambos países. Asimismo, propone la adopción de una forma comparativa integral para esquemas de ciberseguridad gubernamental. El artículo concluye con algunos tópicos para profundizar en el análisis de ciberseguridad bajo una perspectiva internacional.

Palabras clave: ciberseguridad, competencia internacional, ciberespacio, seguridad nacional, soberanía cibernética

CHINESE AND AMERICAN CYBER SECURITY MODELS: A COMPARATIVE

ABSTRACT

This article provides some insights into the debate about the relevance of cyber security as a tool for international competition. The central argument sustains that actions in the cyber security realm perform a key piece in competitive relations of governments. By making a comparison between Chinese and

* Doctor en estudios del desarrollo global por la Universidad Autónoma de Baja California. Profesor de cátedra en el Instituto Tecnológico y de Estudios Superiores de Monterrey (México) [german.patino@gmail.com]; [https://orcid.org/0000-0003-0275-0238].

Recibido: 26 de junio de 2020 / Modificado: 26 de agosto de 2020 / Aceptado: 10 de diciembre de 2020

Para citar este artículo:

Patiño Orozco, G. A. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. *OASIS*, 34, pp. 107-126

DOI: https://doi.org/10.18601/16577558.n34.07

American cyber security models the text upholds that this realm has become a national security imperative. Likewise, it proposes the adoption of a comprehensive comparative cyber security models of governments. The article concludes by offering some issues to analyze cyber security within an international perspective.

Key words: cyber security, international competition, cyberspace, national security, cyber-sovereignty

INTRODUCCIÓN

La ciberseguridad se ha convertido en una prioridad estatal a partir de la primera década del siglo xxi. La dependencia social en los sistemas digitales e informáticos se ha venido acentuando en las últimas décadas. Es por ello que esta misma situación de dependencia trae consigo vulnerabilidades inherentes a dichos sistemas. Así, la ciberseguridad se entiende como el intento para salvaguardar la integridad y continuidad de los sistemas digitales e informáticos a fin de garantizar los principios de confidencialidad de la información, la integridad en el intercambio seguro de datos, así como la operatividad y disponibilidad de la arquitectura técnica dentro de la infraestructura de las tecnologías de información y comunicación (Singer & Friedman, 2014).

En un mundo digital, la información es la esencia del valor, proteger esa información es, por lo tanto, primordial (Singer & Friedman, 2014, p. 35). Asimismo, la integridad significa que el sistema y los datos que contiene no han sido alterados o modificados indebidamente sin autorización. Además, la disponibilidad significa poder usar el sistema como está previsto (Singer & Friedman, 2014, p. 35). Por tanto, junto con estas propiedades, debe añadirse la resiliencia de los sistemas de información. Esta 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 ocurran de manera continua (Singer & Friedman, 2014, p. 36).

Con base en esto, grandes potencias han colocado la ciberseguridad como un asunto prioritario para garantizar su seguridad nacional. Este proceso se ha hecho evidente a través de dos mecanismos. Primero, 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 con propósitos maliciosos, de carácter gubernamental, 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 estos 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[1]. 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% eran 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% eran actividades relacionadas con espionaje, estas buscaban alterar el balance de información u obtener alguna información sensible para poseer recursos de negociación diplomática (148 incidentes). Por último, el 12.9% eran 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).

Esta situación ha traído consigo que las entidades gubernamentales busquen diferentes estrategias para corregir las vulnerabilidades y mitigar los riesgos. Esto se debe a que los Estados identifican que frente al espacio cibernético, por sus características estratégicas y su alcance, se deben tomar medidas para garantizar la integridad, confiabilidad y operatividad de la información. Por razón de lo anterior, se puede apreciar un cambio en los hábitos gubernamentales en la protección de la información. Este trabajo busca ilustrar el uso de medidas de protección de información, el despliegue de sistemas de control de acceso y la instauración de diferentes estándares que los gobiernos estadounidense y chino están desarrollando para gestionar la seguridad de la información.

Con base en esto, el texto busca realizar un tratamiento comparativo de los esquemas gubernamentales de ciberseguridad de la República Popular de China y de Estados Unidos de América, con el objeto de conocer qué efectos tiene la ciberseguridad sobre las políticas gubernamentales, al tratar de responder la interrogante, ¿con qué fin los Estados utilizan las actividades de ciberseguridad? En este texto, se entiende que 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.

Este trabajo se inserta en el supuesto que las actividades de ciberseguridad representan un pilar fundamental en el marco de una relación competitiva internacional, expresada en las interacciones sino-estadounidenses. Por ello, en primer lugar, se desmenuzan brevemente los proyectos de ciberseguridad

[1] Para fines de este trabajo, se entiende a la ciberseguridad como la acción de proteger la información, comunicaciones y tecnología causada por una operación intencional o accidental que ponga en riesgo la confidencialidad, integridad y disposición de datos.

chinos y estadounidenses como herramientas de posicionamiento internacional, lo que a la postre se traduce en un tipo particular de reglas, normas y principios que enarbola cada programa ciberespacial. En seguida, se presentan algunas delimitaciones conceptuales sobre la competencia internacional, basadas en la concepción de una disputa hegemónica dentro de un contexto transhistórico particular y, de otra parte, preguntarse qué función tiene la ciberseguridad en esta apuesta competitiva. Posteriormente, se describe la manera en la que se busca establecer y configurar la agenda internacional del fenómeno bajo ideas y estrategias específicas.

EL PAPEL DE LA CIBERSEGURIDAD EN LAS VISIONES SINO-ESTADOUNIDENSES

Junto con las visiones de ciberseguridad del gobierno de los Estados Unidos de América y la República Popular de China converge el debate sobre su rivalidad sistémica y el estudio de una posible transición hegemónica internacional. Por un lado, 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. 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, 2010; Christensen, 2015; Nathan, 2016).

Por otro lado, 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 (Krauthamer, 1995; Rachman, 1996; Layne, 2009; Jacques, 2009; Kirshner, 2010; Friedberg, 2011; Dobbins, 2012; Kupchan, 2012; Pillsbury, 2015). Con base en esto, sobresale el análisis de una 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 (Shambaugh, 2013). Siguiendo esta lógica, en este trabajo se asume que la ciberseguridad funge como una herramienta que, además de ser un soporte en la búsqueda de la seguridad para ambos, es una estrategia de competencia por la hegemonía en el ámbito internacional que se ve reflejada en las prácticas antitéticas sobre el orden global de seguridad. Por lo tanto, la seguridad del espacio cibernético se convierte tanto en un ámbito de cooperación como de conflicto para ambos Estados, propiciado por el desarrollo de las nuevas tecnologías de información y comunicación.

Si se puede establecer una principal diferencia entre los esquemas gubernamentales de la República Popular de China y los Estados Unidos de América, en relación con la ciberseguridad, es su apreciación del concepto. Para el gobierno chino, la ciberseguridad involucra aspectos que, además de la integridad, confidencialidad y disponibilidad de la información, considera que la información tiene un carácter sensible, por lo que el acceso a ese tipo de información se restringe a ciertas personas o grupos bajo un marco jurídico. Bajo esta perspectiva, el gobierno chino identifica que la confidencialidad de esta información estratégica fortalece su ejercicio gubernamental y, a su vez, permite el desarrollo y el bienestar general de la sociedad. Asimismo, pretende utilizar la ciberseguridad como herramienta para disminuir un alto porcentaje de puntos de riesgo que puedan vulnerar la legitimidad y el margen de acción política de su dirigencia. Es por ello que 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, el gobierno estadounidense también lo considera un dispositivo importante para 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 refleja una lógica estratégica en el dominio digital, que busca contar con los mecanismos para conseguir una posición de superioridad sobre otros competidores (Deibert & Rohozinsky, 2010). 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 antes enunciadas, ambos proyectos también tienen elementos que comparten. Por ejemplo, tanto el enfoque chino como el estadounidense de ciberseguridad tienen en común la premisa de que el mantenimiento de esta 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 (Valeriano, Jensen & Maness, 2019). Con base en esto, ambos gobiernos enarbolan sus estrategias de ciberseguridad 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, 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 como Alemania, Reino Unido y Rusia. En ambos casos (chino y estadounidense), distintos agentes gubernamentales y no gubernamentales ayudan a apuntalar esas visiones que buscan mantener o alcanzar una posición de privilegio

en el desarrollo tecnológico. Esto se puede apreciar de forma esquemática en la tabla 1.

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 (Ver Tabla 2).

En tercer lugar, 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, puesto que ambos gobiernos consideran que la información estratégica debe ser manejada cuidadosamente para el buen funcionamiento de la administración pública y la seguridad nacional.

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[2], en especial a lo que se refiere a los procedimientos y protocolos de seguridad de la información.

Tabla 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 Departamentos 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.

[2] Para este trabajo, se considera al ciberespacio como el sistema electrónico y electromagnético que sirve para almacenar, modificar, intercambiar y aprovechar información a través de redes e infraestructuras interconectadas por medio de tecnologías de la información y la comunicación. Además, incluye todos los dispositivos digitales que utilizan y se enlazan con el peldaño lógico-programático del espectro electrónico.

Tabla 2
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 Pinduoduo	Amazon eBay
Transferencias y pagos en línea	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).

Aunado a lo anterior, dichos 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 a las instituciones participantes, la compresión de áreas prioritarias y los mecanismos para gestionar los riesgos de ciberseguridad.

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.

Por otra parte, la República Popular de China apuesta por un proyecto de ciberseguridad basado en una mayor intervención estatal. Asimismo, 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 qué estándares y preceptos.

Con base en esto, la República Popular de China y los Estados Unidos de América 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 integridad, confidencialidad, disponibilidad de la información, así como también, sobre la gestión de los protocolos de seguridad que permitan el funcionamiento adecuado de la estructura digital, y que solventan la mayoría de interacciones de una sociedad que es cada vez más propensa y dependiente de las tecnologías de información y comunicación.

A su vez, esto refleja 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).

LA FUNCIÓN DE LA CIBERSEGURIDAD EN LA APUESTA COMPETITIVA INTERNACIONAL

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, p. 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, p. 258). Estas son fundamentales pues "no solo 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, p. 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, p. 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, p. 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, 2018). Esta fase se conoce como interregno hegemónico y se distingue por una intensa competencia interestatal, inter-empresarial, conflictos sociales y la reconfiguración de la estructura internacional (Morales, 2018, p. 482).

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 el presidente Xi Jinping, ha adoptado políticas y comportamientos exteriores más proactivos (Johnston, 2013). Por un lado, 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, pp. 315-320).

Por otro lado, considerando que las amenazas que atiende la ciberseguridad son aquellas relacionadas con el resguardo eficaz de la información, en particular la operatividad y disponibilidad de grandes flujos de datos, en consecuencia, las instituciones gubernamentales ponen un gran énfasis en la administración y protección de sus arquitecturas que actúan en la infraestructura de información y comunicación. Con base en esto, el empleo intensivo de sistemas informáticos de 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, se convierten en activos esenciales para tener en cuenta en el tema de ciberseguridad, además de que son pilares fundamentales para el gobierno chino en su búsqueda por tener un mayor impacto en la configuración del orden internacional (Berger, 2014)[3].

Al extender el ámbito del proyecto, la dirigencia china 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

[3] 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.

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, 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 que la posición china funja como el núcleo en el escenario mundial y desempeñar un papel significativo en su configuración. Para ello, los dirigentes chinos consideran que la protección y salvaguarda de 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 medidas de protección 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 también 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 dirigentes estadounidenses se apoyan no solo 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, 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 (Rovner & Moore, 2017)[4]. Además de lo anterior, el gobierno estadounidense ha buscado limitar la inversión extranjera en empresas tecnológicas y de telecomunicaciones, ha 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.

[4] Esta implicación de la ciberseguridad puede ser una oportunidad de colaboración bilateral entre Estados Unidos y China debido a la vulnerabilidad de los sistemas digitales. Es evidente que los ciberataques se han convertido en un medio de agresión más recurrente para las instituciones públicas y privadas, por lo cual, plantea un desafío de carácter sistémico que necesita medidas conjuntas para disminuir los riesgos de los sistemas entre dos economías sumamente interdependientes.

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, sobre todo 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[5].

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[6]. A partir de ese momento, se ha considerado que las acciones estadounidenses y chinas en el ciberespacio tienen un efecto contraproducente en la estabilidad y funcionalidad de la estructura digital global. Para Brandon Valeriano, Benjamin Jensen y Ryan C. Manes (2019, p. 171) estas acciones reflejan que las actividades en el ciberespacio son un "teatro para el espionaje, el sabotaje y el conflicto".

Es decir, a medida que los gobiernos desarrollan 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 (Deibert R., 2011). 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 (Klimburg, 2017).

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 nuevas formas de control y manipulación social de manera sofisticada, lo que limita derechos y libertadas en general (Kaplan, 2016; Zuboff, 2019).

---

[5] A su vez, se ha documentado que distintas organizaciones y agencias gubernamentales chinas han conducido actividades de ciberespionaje para beneficio industrial con base en el robo de información confidencial, sensible o estratégica (Deibert, 2013)

[6] En junio de 2013, los diarios *The Guardian* y *The Washington Post* publicaron los documentos que filtró el ex contratista de la Agencia de Seguridad Nacional de los Estados Unidos de América (NSA, por sus siglas en inglés) que mostraba el alcance de los programas de espionaje e inteligencia desplegados por las instituciones estadounidenses.

LA RELACIÓN SINO-ESTADOUNIDENSE Y EL ESTABLECIMIENTO DE LA AGENDA INTERNACIONAL EN MATERIA DE CIBERSEGURIDAD

La relación bilateral sino-estadounidense está entrelazada en diversos ámbitos: estratégica, diplomática, económica, social, cultural y políticamente. Además, opera en diversos niveles de acción: global, regional, nacional y localmente (Shambaugh, 2013). La ciberseguridad no es una dimensión separada de esta dinámica de interacciones, antes bien, está integrada en estos elementos de competencia y colaboración multifacética, multidimensional y multimodal. De esta manera, la importancia de sus interacciones radica en la dimensión y alcance de esta.

Por ejemplo, ambos cuentan con las dos economías más grandes del mundo, los presupuestos militares más altos, son los dos principales consumidores de 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. A su vez, son 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, incluido 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 (Lieberthal & Wang, 2012). 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 de hegemonía internacional (deLisle & Goldstein, 2017; Shambaugh, 2013; Helleiner & Kirshner, 2014).

Además, la divergencia de intereses, enfoques y políticas se hace cada vez más evidente en el entorno económico, ideológico, normativo, geopolítico y de seguridad contemporáneos (Goldstein, 2015). Por ejemplo, para David Shambaugh (2013, p. 75), los encuentros bilaterales y multilaterales, se han convertido más en foros para discutir y manejar los impulsos competitivos, que para forjar una cooperación real entre ambas naciones. Para Kenneth Lieberthal 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, 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 sus sistemas digitales, tanto gubernamentales como privados, ya que ninguno de los dos países desea ver la estabilidad del ciberespacio interrumpida por acciones terroristas, actividades criminales o que las nuevas tecnologías están fuera de su control, pues ninguno tolera algún tipo de comportamiento digital que interfiera con sus objetivos

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 (*wangluo zhuquan*网络主权), 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 en primer lugar a Estados Unidos (*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, 2016).

Por esta razón, han buscado implementar procesos de innovación tecnológica interna y han buscado un mayor protagonismo en la gobernabilidad de estándares globales para el funcionamiento del terreno ciberespacial (Gady, 2016). 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 la República Popular de China y los Estados Unidos de América (Lewis, 2018).

Justamente, en una estrategia 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 (Lu, 2017).

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 (*Internet Corporation for Assigned Names and Numbers*), IETF (*Internet Engineering Task Force*), World Wide Web Consortium y los equipos CERT sean los encargados de desarrollar los estándares de la arquitectura global del ciberespacio[7], deter-

[7] Los *computer emergency response teams* (Cert) son organismos público-privados que tienen como tarea coordinar respuestas a problemas e incidentes de seguridad informática. Además, funcionan como centros de enlace entre proveedores de productos o servicios digitales, en particular, a través de la identificación de vulnerabilidades y riesgos, así como emisión de soluciones técnicas. 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.

minen los sistemas de nombre de dominio y sean quienes den respuesta a los incidentes cibernéticos que se presenten.

En este tenor, ambos gobiernos pretenden dar respuesta a asuntos 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.

Ambos gobiernos han puesto a trabajar 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 que 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 la seguridad doméstica, 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 (Ver Tabla 1).

Junto con ello, el gobierno chino y el gobierno estadounidense han desarrollado una amplia cantidad de 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. De esta manera, se puede entender la fuerte competencia comercial y estatal en rubros como el desarrollo e imple-

mentación 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 3.

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 (Steinfeld, 2017). 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 la información (Steinfeld, 2017, pp. 112-113). Además, la estrategia basada en la competencia interestatal frena los impulsos sinérgicos necesarios para continuar apuntalando el desarrollo científico-tecnológico.

No obstante, han existido algunos mecanismos de diálogo cibernético entre los dos países desde 2013 para resolver sus diferendos (Lu, 2017). El primero fue el Grupo de Trabajo Cibernético Estados Unidos-China (*U.S.-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. En una segunda etapa, destaca el establecimiento del Diálogo Conjunto de Alto Nivel China-Estados Unidos sobre Crimen Cibernético y Asuntos Relacionados (*China-*

Tabla 3
Comparación de proyectos digitales gubernamentales

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).

US High-Level Joint Dialogue on Cybercrime and Related Issues).

Por último, en octubre de 2017 se presentó oficialmente el mecanismo de Diálogo Sino-Estadounidense de Ciberseguridad e Implementación de Normas (*China-US Law Enforcement and Cybersecurity Dialogue*), después de la Cumbre de Mar-a-Lago entre el presidente Donald J. Trump y el presidente Xi Jinping en abril de 2017. Sin embargo, a pesar de estos contactos entre el gobierno de China y el de los Estados Unidos por disipar visiones divergentes, 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 del Ejército Popular de Liberación de llevar a cabo actividades maliciosas en el ciberespacio (Gady, 2016)[8].

A pesar de estas proposiciones, las acciones gubernamentales sino-estadounidenses en materia de ciberseguridad parecen encaminarse en sentido competitivo. 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)[9]. 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 para prohibir a cualquier empresa adquirir servicios o productos con proveedores extranjeros (Guimón, 2019; Muñoz, 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)[10]. 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

[8] 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 Solar World y de la empresa proveedora de energía nuclear Westinghouse.

[9] Algunos países como Alemania, Australia, Canadá, Gran Bretaña, Japón y Nueva Zelandia han impuesto restricciones (o han considerado hacerlo) a los equipos y dispositivos tecnológicos provenientes de la República Popular de China.

[10] El temor expresado por las autoridades estadounidenses 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 con el gobierno de su país en el intercambio de información sensible y en tareas de espionaje.

generación de tecnología de la comunicación, así como también, en el impulso de la computación cuántica y la inteligencia artificial[11].

CONCLUSIONES

A lo largo de este artículo se puede observar las convergencias y divergencias entre dos enfoques gubernamentales en relación con el fenómeno de la ciberseguridad, acción que se ha hecho de forma escasa en la disciplina de relaciones internacionales, por lo cual se identifica como una fortaleza de esta propuesta. Con ello, salta a la vista la necesidad de seguir profundizando en este tipo de análisis. Bajo estas circunstancias, al contrastar las perspectivas sino-estadounidenses del fenómeno de ciberseguridad, se percibe que se ha desarrollado una estrategia integral para hacer frente a los riesgos y vulnerabilidades cibernéticos.

Asimismo, se aprecia una competencia por dirigir y encauzar el desarrollo técnico-científico, un punto que se ha vuelto neurálgico en la relación sino-estadounidense. Para conseguir, este objetivo, los gobiernos de ambos países han creado condiciones y estructuras institucionales necesarias para una implementación efectiva de sus estrategias. Para algunos analistas, los gobiernos de Estados Unidos y de la República Popular de China con este propósito generan una competencia creciente, tal vez al borde del conflicto, donde el punto focal no es la fuerza militar o la expansión territorial, sino que se observa a través "del control de las palancas modernas del poder: normas e instituciones globales, estándares relacionados con el comercio y tecnología" (Lewis, 2018).

Sin embargo, se mantiene incierto en qué medida las visiones sino-estadounidenses, en su afán competitivo, puedan ayudar a aminorar los riesgos y las vulnerabilidades de la seguridad de la información. Además, no está claro si estas perspectivas, en apariencia divergentes, producen un efecto estabilizador o colaboran para formar un esquema de ciberseguridad menos seguro y más incierto. Por último, no se puede anticipar si la discrepancia sino-estadounidense puede generar una espiral de fragmentación y escisión del ciberespacio en jurisdicciones nacionales que, por ende, transformen completamente la estructura digital tradicional.

Cabe resaltar que una limitante del enfoque Estado-céntrico, abrazado en gran medida por esta investigación en relación con el estudio de las actividades de ciberseguridad, es que deja fuera las percepciones y acciones de otros actores relevantes (privados), que comúnmente son quienes perfilan, en buena medida, la estructura del ciberespacio. No obstante, el

[11] La red 5G es un sistema que permitiría la interconexión de dispositivos, aparatos, equipos mobiliarios e inmobiliarios de manera simultánea, a una velocidad de ancho de banda de 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 2013. Además, desde el 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.

objetivo de este trabajo era analizar las medidas y visiones de la ciberseguridad de los agentes estatales, lo cual brinda una parte explicativa pertinente para un fenómeno multi-agencia.

Por tanto, para las autoridades de la República Popular de China y para el gobierno de los Estados Unidos de América, la ciberseguridad tiene un efecto directo en su comportamiento internacional, a través de una reestructuración de funciones gubernamentales, el desarrollo de legislaciones y normatividades específicas para el tratamiento del tema y un tratamiento integral del fenómeno. Por último, solo 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 que implica que otros Estados emulen las trayectorias sino-estadounidenses, una oportunidad que abre pautas para líneas de investigación futura.

BIBLIOGRAFÍA

Berger, S. (09/11/2014). *Xi Offers Vision of China-Driven 'Asia-Pacific' Dream.* From Jakarta Globe: http://jakartaglobe.id/international/xi-offers-vision-china-driven-asia-pacific-dream/

deLisle, J. & Goldstein, A. (2017). *China's Global Engagement: Cooperation, Competition and Influence in the 21st Century.* Washington: Brookings Institution Press.

Deibert, R. (2011). Tracking the Emerging Arms Race in Cyberspace. *Bulletin of Atomic Scientists.*

Deibert, R. J. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto: McClelland & Stewart.

Deibert, R. J. & Rohozinsky, R. (2010). Liberation vs Control in Cyberspace. *Journal of Democracy,* 21(4), 43-57.

Dobbins, J. (2012). War with China. *Survival,* 54(4), 7-24.

Escobar, A. (06/1994). Welcome to cyberia: notes on the anthology of cyberculture. *Current Anthropology,* 35(3), 211-231.

Friedberg, A. L. (2011). *A Contest for Supremacy: China, America and the Struggle for Mastery in Asia.* Nueva York: W.W. Norton.

Gady, F.-S. (28/01/2016). *What Does 2016 Hold for U.S.-China Relations in Cyberspace?* Retrieved noviembre 15, 2018 from China-US Focus: https://www.chinausfocus.com/peace-security/what-does-the-year-2016-hold-for-china-u-s-relations-in-cyberspace/

Goldstein, L. J. (2015). *Meeting China Halfway. How to Defuse the Emerging U.S.-China Rivalry.* Washington: Georgetown University Press.

Guimón, P. (15/05/2019). *Trump blinda las telecomunicaciones de EE. UU. contra Huawei en una nueva ofensiva contra China.* Retrieved mayo 16, 2019 from *El País*: https://elpais.com/internacional/2019/05/15/estados_unidos/1557957202_172429.html

Helleiner, E. & Kirshner, J. (2014). *The Great Wall of Money: Power and Politics in China's International Monetary Relations.* Ithaca: Cornell 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.

Johnston, A. I. (2013). How New and Assertive is China's New Assertiveness? *International Security,* 37(4), 7-48.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* New York: Penguin Press.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War.* Nueva York: Simon & Schuster.

Kirshner, J. (2010). The Tragedy of Offensive Realism: Classical Realism and the Rise of China. *European Journal of International Relations,* 18(1), 53-75.

Knight, W. (13/02/2019). *Claves para entender por qué EE.UU. teme que Huawei domine el 5G.* Retrieved mayo 21, 2019 from 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_pIlz09ivuyKqBWpBeIl8KsvvIkHZFvyIP51o-311fV8rd9vwe0Q

Kramer, F. D., Starr, S. H., Wentz, L. K. & (eds.). (2009). *Cyberpower and National Security.* Washington, DC: Potomac Books.

Krauthamer, C. (31/07/1995). Why We Must Contain China. *Time*.

Kupchan, C. (2012). *No One's World: the West, the Rising Rest, and the Coming Global Turn.* New York: Oxford University Press.

Layne, C. (2009). The Unipolar Illusion Revisited: The Coming End of the United States' Unipolar Moment. *International Security,* 34(1), 147-172.

Legro, J. W. (2000). Whence American Internationalism. *International Organization,* 54(2), 253-289.

Lewis, J. A. (30/11/2018). *Technologial Competition and China.* Retrieved enero 22, 2019 from Center for Strategic & International Studies: https://www.csis.org/analysis/technological-competition-and-china

Li, Z. (16/01/2016). *Different Values but Similar Visions for Cyberspace.* Retrieved enero 17, 2016 from China-US Focus: https://www.chinausfocus.com/peace-security/different-values-but-similar-visions-for-cyberspace

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.

Lu, C. (29/12/2017). *China-US Cyberspace Relations in the Trump Era.* Retrieved diciembre 29, 2018 from China-US Focus: https://www.chinausfocus.com/peace-security/china-us-cyberspace-relations-in-the-trump-era

Maness, R. C., Valeriano, B. & Jensen, B. (2017). *The Dyadic Cyber Incident and Dispute Dataset.* Retrieved julio 8, 2019 from http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf

Miller, T. (2017). *China's Asian Dream.* Londres: Zed Books.

Morales, D. (2018). Ciclos políticos hegemónicos: implicaciones para la gobernanza internacional. *Brazilian Journal of International Relations,* 7(3), 452-493.

Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace.* New York: McGraw Hill.

Muñoz, R. (20/05/2019). *Google rompe con Huawei, cuyos móviles se quedarían sin sus 'apps' y actualizaciones.* Retrieved mayo 20, 2019 from *El País*: https://elpais.com/economia/2019/05/19/actualidad/1558294622_546268.html

Pillsbury, M. (2015). *The Hundred Year Marathon: China's Secret Strategy to Replace America's as the Global Superpower.* Nueva York: Henry Holt.

Rachman, G. (1996). Containing China. *Washington Quarterly,* 19(1), 129-140.

Rovner, J. & Moore, T. (2017). Does the Internet Need a Hegemon? *Journal of Global Security Studies,* 2(3), 184-203.

Sanger, D. E., Barnes, J. E., Zhong, R. & Santora, M. (26/01/2019). *In 5G Race with China, U.S. Pushes Allies to Fight Huawei.* Retrieved enero 28, 2019 from The New York Times: https://www.

nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html

Segal, A. (2018). When China Rules the Web: Technology in the Service of the State. *Foreign Affairs,* 97(5), 10-18.

Shambaugh, D. (2013). *China Goes Global. The Partial Power.* Nueva York: Columbia University Press.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Nueva York: Oxford University Press.

South China Morning Post; Abacus; Edith Yeung. (2019). *China Internet Report 2019.* Hong Kong: *South China Morning Post*.

Steinfeld, E. S. (2017). Teams of Rivals: China, the United States, and the Race to Develop Technologies for a Sustainable Future. In J. deLisle, & A. Goldstein, *China's Global Engagement: Cooperation, Competition, and Influence in the 21st Century* (pp. 91-121). Washington: Brookings Institution Press.

Toca, G. (10/04/2019). *5G: la otra cara de la guerra digital.* Retrieved abril 11, 2019 from Esglobal: https://www.esglobal.org/5g-la-otra-cara-de-la-guerra-digital/?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork

U.S. Cyber Command. (04/2018). *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command.* Retrieved enero 23, 2019 from 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. (04/2018a). *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command.* Retrieved enero 23, 2019 from U.S. Cyber Command: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

U.S. Government White House. (09/2018). *National Cyber Strategy of the United States of America.* Retrieved enero 23, 2019 from U.S. Government White House: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Valeriano, B., Jensen, B. & Maness, R. C. (2019). *Cyber Strategy: The Evolving Character of Power and Coercion.* Nueva York: Oxford University Press.

Vida Liy, M. & Mars, A. (21/05/2019). *Donald Trum da una tregua de tres meses para imponer el veto a Huawei.* Retrieved mayo 21, 2019 from *El País*: https://elpais.com/economia/2019/05/21/actualidad/1558417928_415258.html

Xi, J. (2014). *The Governance of China.* Beijing: Foreign Languages Press.

Yuan, L. (03/10/2018). *Private Businesses Built Modern China. Now Gov't Is Pushing Back.* Retrieved mayo 21, 2019 from The New York Times: https://www.nytimes.com/2018/10/03/business/china-economy-private-enterprise.html

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future a the New Frontier Power.* New Yok: Public Affairs.