URVIO, Revista Latinoamericana de Estudios de Seguridad
ISSN: 1390-3691
ISSN: 1390-4299
revistaurvio@flacso.edu.ec
Facultad Latinoamericana de Ciencias Sociales
Ecuador

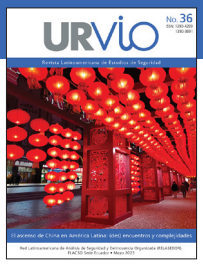
Aguilar-Antonio, Juan-Manuel
China y Estados Unidos: antagonismos y liderazgos en el ciberespacio frente a América Latina
URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 36, 2023, pp. 66-84
Facultad Latinoamericana de Ciencias Sociales
Quito, Ecuador

DOI: https://doi.org/doi.org/10.17141/urvio.36.2023.5845

Disponible en: https://www.redalyc.org/articulo.oa?id=552675983004

Los leones de Fu representan al Buda, son estatuas que custodian los ingresos de los edificios tradicionales chinos, en este caso la ciudad prohibida en Beijing (Pekin). Ambos felinos, macho y hembra, simbolizan el equilibrio, reflejando la filosofía del ying y del yang. El macho con una esfera en la pata representa el papel del hombre: proteger el mundo y la vida. Por su parte, la hembra con una cria cerca a su pata, representa el cuidando de la familia.

Tema Central



doi.org/10.17141/urvio.36.2023.5845

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 36, mayo-agosto 2023
pp.66-84 • RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

China y Estados Unidos: antagonismos y liderazgos en el ciberespacio frente a América Latina

China and the United States: antagonisms and leadership in cyberspace vis-à-vis Latin America

Juan-Manuel Aguilar-Antonio[1]

Recibido: 13 de enero de 2023
Aceptado: 10 de abril de 2023
Publicado: 31 de mayo de 2023

Resumen

Este trabajo tiene como objetivo mostrar al ciberespacio como el quinto dominio de la política internacional en el que la República Popular China y Estados Unidos construyen ciberpoder, con capacidad de influir en el desarrollo de las capacidades cibernéticas de América Latina. El texto se divide en siete secciones. En la primera se presenta la trascendencia del ciberespacio en la seguridad internacional. En la segunda, conceptos clave para el análisis del dominio desde las ciencias sociales. En la tercera se analizan las categorías de *hard power, soft power y smart power*. En la cuarta se describen índices internacionales para medir el ciberpoder y las capacidades cibernéticas. En la quinta, el método de análisis comparativo aplicado al estudio. En la sexta se compara el ciberpoder de China con el de Estados Unidos. En la séptima se analizan las asimetrías de América Latina y se identifican áreas de influencia y cooperación en la región. Se concluye que Estados Unidos es ejemplo de política nacional y estructura organizacional en ciberseguridad para América Latina, mientras que China es referente de recursos tecnológicos, con el potencial de penetrar en la estrategia económica de la región.

Palabras clave: seguridad cibernética, política internacional, China, Estados Unidos de América, América Latina

Abstract

This work aims to show cyberspace as the fifth domain of international politics, in which the People's Republic of China and the United States build cyber power, with the ability to influence the development of cybernetic capabilities in Latin America. The text is divided into seven sections. The first presents the importance of cyberspace in international security. The second presents key concepts for domain analysis from the Social Sciences. In the third section, the categories of hard power, soft power, and smart power are analyzed. The fourth section points out international indices to measure cyber power and cyber capabilities. The fifth describes the method of comparative analysis applied to the study. The sixth compares the cyber power of China and the United States. In the seventh, asymmetries and areas of influence and cooperation in Latin America are identified. It is concluded that the United States is an example of national policy and organizational structure in cybersecurity for Latin America, while China is a benchmark for technological resources, with the potential to penetrate the economic strategy of the region.

Keywords: cyber security, international politics, China, United States of America, Latin America

1 UNAM, Centro de Investigaciones sobre América del Norte (CISAN), alchemistffvii@hotmail.com, orcid.org/0000-0002-4686-685X

Introducción[2]

La ciberseguridad se ha transformado en un aspecto clave de la política internacional en el siglo XXI. La creciente dependencia del internet frente a un contexto adverso y cambiante de amenazas al Estado nación hacen clave el desarrollo de capacidades cibernéticas y ciberpoder. El vertiginoso avance de la tecnología profundiza la diferencia entre las naciones líderes en el desarrollo de una política nacional de ciberseguridad y las que aún la construyen. Cabe resaltar que el ciberespacio no está exento de una lucha de poder entre las naciones. Índices como el *National Cyber Power Index* (NCPI) y el *Cyber Capabilities And National Power* (CCNP) han delimitado quiénes son en la actualidad las potencias del dominio. Entre ellas se encuentran la República Popular de China y los Estados Unidos de América.

El ascenso del gigante asiático en el quinto dominio se empata con el surgimiento de tecnologías innovadoras como la inteligencia artificial, la computación cuántica, las redes 5g y el *big data*. Esa transformación cambiará la geopolítica internacional y la influencia de las potencias que las utilicen. En el caso de las Américas, la situación es compleja a razón de la divergencia notable de países como Estado Unidos, potencia de los ámbitos militar, político, económico y del ciberespacio respecto a América Latina, que enfrenta múltiples retos para su estabilidad interna y está en fases prematuras del desarrollo de capacidades cibernéticas y una política de ciberseguridad (Aguilar-Antonio 2020; 2021).

En la región no se han presentado casos de ataques a infraestructura crítica que vulneren la soberanía del Estado nación, como el caso *Stuxnet*, en Irán (2012). Tampoco casos de fuga de información reservada, capaz de dañar su política internacional, como el *Cablegate* de *Wikileaks* (2011), con la extracción de 200 000 cables diplomáticos del Departamento de Estado de Estados Unidos. No ha existido un incidente que combine el espionaje y la ciberexplotación de información de interés nacional por un actor extranjero, como fue el caso de *SolarWinds* (2020). Lo más cercano sería la extracción de información por parte del grupo hacktivista Guacamaya a las Fuerzas Armadas de Chile, Colombia, El Salvador, México y Perú, y su difusión en el portal Enlace Hacktivista en 2022. Esta tuvo un impacto moderado en la esfera política interna de cada país y devela cómo las naciones de América Latina no terminan de comprender la revolución internacional que se está gestando en el ciberespacio (Hurel 2022; Aguilar-Antonio 2021).

En adición, los efectos de la pandemia del virus SARS-CoV-2, durante los años 2020-2022, incrementaron exponencialmente el nivel de ciberamenazas globales. Por ejemplo, *Sonic Wall* (2021) indicó que durante el bienio 2019-2020 se dio el incremento más alto de ataques de *software* malicioso en el mundo, con una tasa de crecimiento del 57,6% al pasar de 9 900 000 000 a 15 600 000 000 en un año. Asimismo, *Mordor Intelligence* (2021) indica que entre 2015 y 2020 el mercado de la ciberseguridad se duplicó al pasar de los 13 730 000 000 a los 26 200 000 000 de dólares. En este contexto, Latinoamérica enfrenta un gran reto

2 Este artículo se realizó con apoyo del Programa de Becas Posdoctorales de la UNAM, el autor es becario del Centro de Investigaciones sobre América del Norte (CISAN), asesorado por el Dr. Leonardo Curzio Gutiérrez.

en el desarrollo de sus capacidades cibernéticas para contener las amenazas del ciberespacio y obtener beneficios de este nuevo dominio de la seguridad nacional. Este reto se dará de forma paralela a la consolidación del ciberpoder de potencias como Estados Unidos y la República Popular de China, naciones que tienen diferentes perspectivas de liderazgo en la comunidad internacional, que influenciarán el mundo en las próximas décadas (*Xuetong* 2019; *Nye* 2004).

Conceptos clave para entender al ciberespacio

Para abordar el ciberespacio como quinto dominio de la política internacional, es útil proporcionar un marco referencial de la perspectiva de los estudios de Ciencias Sociales. En este apartado introducimos varios conceptos definidos por *Kello* (2013) en su artículo *The Meaning of the Cyber Revolution*, el cual busca promover la difusión de los estudios de seguridad internacional del ciberespacio y presentar un marco conceptual para el análisis de disciplinas como la Ciencia Política y las Relaciones Internacionales, estos son:

a) Ciberseguridad*:* comprende las medidas de protección de un sistema computacional y la integridad de sus datos de una acción hostil. La ciberseguridad se concibe como un estado de integridad, que es determinado por la presencia o ausencia de la intrusión de un sistema informático y sus funciones, además de que será de vital importancia para la seguridad y sobrevivencia de la información de un Estado nación.
b) Malware: involucra el diseño de un programa malicioso para interferir con la funcionalidad o degradación de datos de un computador o red. Este incluye una amplia gama de códigos dañinos (virus, gusanos, troyanos, *spyware, adware, ransomware,* etc.). La finalidad del *malware* es crear una ruta de acceso a un sistema computacional adversario u objetivo, por lo que se considera un instrumento de hostilidad.
c) Cibercrimen: implica el uso del internet para un objetivo ilícito bajo la jurisdicción de una nación. Esto incluye fraudes bancarios, transmisión prohibida de datos, robo de propiedad intelectual y pornografía infantil. Dado que la ley doméstica no es aplicable en contra de otros Estados, el cibercrimen solo involucra actores privados enjuiciables por jurisdicciones nacionales.
d) Ciberataque: se refiere al uso de un *malware* para vulnerar un sistema informático por un objetivo político o económico que beneficie a un Estado nación. Se caracteriza por el deseo y la capacidad de los perpetradores de interrumpir operaciones informáticas o de destruir bienes físicos a través del internet. Puede tener efectos directos (en infraestructura física) e indirectos (negar acceso a sistemas, operaciones o funciones, así como destruir información).
e) Ciberexplotación: es la penetración en un sistema computacional adversario con la finalidad de extraer (pero no destruir) información. Es considerada una acción de inteligencia

> para obtener información de carácter secreto o negar el acceso a los usuarios legítimos. Esto puede ser denominado también como espionaje para adquirir conocimiento crucial de un oponente para planear futuros ataques u operaciones.

Entender el ciberespacio implica también diferenciar su parte física y virtual. En este sentido, se aclara que la parte física está ligada a recursos materiales o tangibles como la infraestructura de telecomunicaciones, que representa el medio físico por el cual se da la conectividad de internet y el tráfico de información (*Kittichaisaree* 2017). La infraestructura de telecomunicaciones está integrada por los sitios, satélites, cables de fibra óptica, redes telefónicas y Tecnologías de la Información y las Comunicaciones. El control, regulación, e incluso posesión de este tipo de tecnología es un factor vital para los Estados.

Por otro lado, la parte virtual del ciberespacio se relaciona al internet y representa la esfera inmaterial. Esto representa los *Internet Protocol* (protocolos IP) y los *Transmission Control Protocol* (ICT) que permiten la conexión y el tráfico de información por la red (*Kello* 2013). En los hechos, esto se refleja en sitios web, blogs, redes de conexión *wi-fi* o alámbricas, aplicaciones, servicios bancarios o gubernamentales, etc. Los protocolos de internet son diferentes del *software,* que representan los sistemas informáticos que crean los programas, sistemas operativos, lenguajes de programación, etc., para gestionar o compartir información.

Apuntes teóricos sobre *Hard Power* estadounidense vs. *Smart Power* chino

Para conceptualizar el ciberpoder es necesario retomar los preceptos del neorrealismo y los aportes *Joseph Nye Jr.* a las teorías de relaciones internacionales. Para Villamizar (2012) es clave la obra *Bound to lead: The changing nature of American power,* publicada en 1990, en la que *Nye Jr.* presenta el poder bajo dos diferentes ópticas. La primera, centrada en el poder duro o *Hard Power*, al que definió como un poder para coaccionar, el cual se materializa en la fuerza económica y militar. Y en segunda posición el poder blando o *Soft Power*, cuyo fin es generar la atracción a través de variables como la cultura, ciencia, turismo, comercio o cooperación internacional, en aras de lograr que otros deseen los beneficios que un país otorga. Lo cual, se transforma en un poder de influencia de una potencia internacional (*Nye Jr.* 1990; 2004).

La clasificación de *Soft Power* y *Hard Power* de *Nye Jr.* ha influenciado múltiples análisis en torno a la comprensión de la política exterior. Esto se refleja en el nivel de citas que alcanza la obra *Bound to lead: The changing nature of American power* que, en el índice de autor de *Nye Jr.*, en *Google Scholar*, alcanza una cifra de 6372 referencias. A pesar de esto, *Nye Jr*. (2011) dio una revisión a sus categorías en la obra *The future of power,* en la que añade un tercer concepto, definido como poder inteligente o *Smart Power.* A este último lo describe como una combinación del poder duro, de coerción, fuerza e imposición económica con el poder blando, de persuasión y atracción. De esta forma, el *Smart Power* es la habilidad de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

combinar poder duro y blando, mediante estrategias efectivas en contextos variables (Villamizar 2012).

En ese sentido, Rosas-González et al. (2023) indica que, en los inicios del siglo XXI, la noción de S*oft Power* de *Nye Jr.* contenía elementos que convergían con la noción de poder inmaterial, inserta en la doctrina de la diplomacia del panda de China, que se relaciona con la tradición milenaria de la nación asiática de explotar recursos culturales o ideológicos en aras de exaltar las emociones, ideas y percepciones en su política exterior. En los hechos, esto se materializó en 2007, cuando *Hu Jintao* utilizó la categoría al presentar el informe del XVII Congreso del Partido Comunista chino y la transformó en un concepto que se combinó con los preceptos de la cultura milenaria para alcanzar sus objetivos globales en el contexto del mundo multipolar, donde China es una potencia que ofrece alternativas a la visión unipolar del liderazgo de Estados Unidos (*Jintao* 2017).

Para *Chang-Liao* (2016) el peso e influencia de China se aceleró a partir del año 2008, en el que inició la segunda parte del mandato de *Hu Jintao*. Esto se dio por dos eventos que mostraron el auge de China como actor global: los Juegos Olímpicos y la crisis financiera global, en la cual se observó la fortaleza nacional de Beijing frente a otras potencias mundiales. También, el sustituir a Japón como la segunda economía del mundo, en 2010, marcó el punto de partida para que los líderes de Beijing hablaran del "sueño chino" y se perfilará una política exterior más activa, con énfasis en su defensa nacional, soberanía y la búsqueda de sus intereses de política exterior.

En este contexto, el ascenso de *Xi Jinping* como jefe de Estado estuvo marcado por una transición de la política exterior de China después de dos décadas, de pasar del mantra "ocultar las capacidades y esperar el momento oportuno," conocido como *Taoguang Yanghui* de *Deng Xiaoping*, a la visión "esforzarse por lograr metas" o *Fenfa Youwei*, presentada por *Jinping* en el primer foro de diplomacia periférica, organizado por su gobierno en octubre de 2013.

Desde sus inicios como mandatario, a Xi Jinping se le ha atribuido la aplicación de una serie de nuevas estrategias de política exterior. *Ferdinand* (2016) destaca tres: 1) el "nuevo tipo de relaciones de Gran Poder", que caracteriza las relaciones chino-estadounidenses desde que *Jinping* se reunió con Obama, en la Cumbre de Cooperación Económica Asia-Pacífico (APEC) de 2014, en Beijing (*Yinhong* 2015). 2) La "comunidad de destino común" o *Mingyun Gongtongti* que reinventó las relaciones de China con sus vecinos del sudeste asiático. Esta busca promover su influencia a la par de reforzar su soberanía marítima y refrendar sus posiciones de "una sola China" respecto a la cuestión de Taiwán. 3) La iniciativa "un cinturón, un camino" (conocida en inglés como *One Belt, One Road* OBOR) es un proyecto que busca crear un cinturón económico global que recree la ruta de la seda. Así, engloban a más de 60 países y 4 000 000 000 de personas, cuyas economías representan un tercio del PIB mundial.

Este viraje de la política exterior de China se empata con el arribo de *Donald Trump* a la presidencia de los Estados Unidos y la publicación de la Estrategia de Seguridad Nacional

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

de 2017, en la que su gobierno estableció que China debía ser considerada como un "poder revisionista", que desafiaba los intereses y valores de EE. UU (*White House* 2017). En este contexto emprendió tres acciones frente a la nueva diplomacia de *Xi Jinping*: 1) el inicio de la Guerra Comercial China-EE. UU., en marzo de 2018; 2) los intentos por evitar la alineación de países a China, principalmente en la región de las Américas, que estrecharan sus relaciones con el gigante asiático, en el ámbito político y comercial a través de mecanismos de coerción o actos de intimidación; 3) la promoción de una imagen negativa de la República Popular, en aras de conservar sus adeptos (Rosas -González et al. 2023).

Frente al incremento del nivel de antagonismo que ejercen los Estados Unidos en contra de China, *Zhang* y *Pu* (2019) indican que el *Soft Power* de la nación asiática evolucionó al *Smart Power*. Ya que, en el nuevo contexto internacional el *Soft Power* no era suficiente para contener los actos de intimidación de Washington DC. Con lo cual, Beijing empezó a combinar poder duro y blando, en aras de seguir con su estrategia de crecimiento comercial e influencia política a nivel global. En la faceta doctrinaria y teórica, el libro que representa esta evolución es *Leadership and the rise of great Powers* de *Yan Xuetong*, decano del Instituto de Relaciones Internacionales de la Universidad de *Tsinghua*, publicado en 2019. Allí, el autor hace una revisión de las teorías de relaciones internacionales, doctrinas morales y filosóficas chinas, para hacer una combinación de un paradigma moral-realista que sirve para entender los antagonismos entre los dos países (*Pu* 2019).

Xuetong (2019) centra el objetivo de la construcción de su teoría moral-realista para explicar el surgimiento de las grandes potencias en el siglo XXI. Para esto, aborda los conceptos de moralidad y liderazgo para enmarcarlos en el papel que ejercen los Estados nación y cómo este influye en cambios del sistema internacional. Este ejercicio, se da como preámbulo para explicar el liderazgo dual que está aconteciendo entre el ascenso de China como poder global y los intentos de Estados Unidos por mantener su hegemonía. En términos de política exterior, *Xuetong* (2019) clasifica el liderazgo de los Estados nación en cuatro tipos: inactivo, conservador, proactivo y agresivo. Sobre el primero indica que este define a países que prefieren no tomar ninguna acción para mantener el estatus internacional actual. Por su parte, el conservador, adopta un punto de vista económico determinista, que prioriza el poder económico. El liderazgo proactivo adopta una visión política determinista, haciendo hincapié en el papel crucial del talento de los líderes en la configuración de las reformas o acciones estratégicas que ayudan a la consolidación de una potencia global. El liderazgo agresivo adopta una visión social darwinista y prioriza los medios militares.

Después**,** *Xuetong* (2019) divide el liderazgo internacional en cuatro categorías: autoridad humana, hegemónico, anemocracia y tiranía, las cuales están basadas en la credibilidad estratégica del líder del sistema internacional y en si los demás países lo ven como una nación confiable o no. Esto se relaciona con sus acciones de política exterior, si son coherentes o no con sus actos y si estos son vistos como actos de doble moral. De esta forma, el liderazgo de autoridad humana implica que un país mantenga una alta credibilidad estratégica y lleve a cabo políticas con normas morales coherentes. El liderazgo hegemónico es confiable, pero

se aplica a discreción con base a los intereses que busca alcanzar la potencia global. En contraposición, el anemocrático no es confiable y se explica en la doble moral. Por último, el liderazgo tiránico es poco confiable, pero consistente a razón de que define a un país egoísta, que solo busca sus objetivos. En el marco del desarrollo de su paradigma teórico *Xuetong* (2019) no cae en el error o juicio de valor de definir a China o Estados Unidos de forma determinista en una de las categorías. Solo busca presentar una serie de conceptos que le permitan a los analistas de política internacional abordar las tensiones y rivalidades entre los dos países a través de nuevas ópticas.

Índices para comprender el ciberpoder y capacidades cibernéticas

En 2010, *Nye Jr.* publicó la obra *Cyber Power* con el fin de teorizar en torno al ciberespacio como nuevo dominio de la política internacional. En ella, el autor argumenta que este se ha transformado en el quinto dominio del poder de los Estados nación, cuyo uso supone la posibilidad de alcanzar objetivos o metas por parte de los países, actores privados, e incluso, individuos. De esta forma, *Nye Jr.* (2011, 3) define al ciberpoder como: "la habilidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en el ciber dominio".

La definición presenta al ciberespacio como un espacio de interacción, pero también de control y manipulación, en el que los actores de la política internacional utilizan el dominio para la búsqueda de sus intereses particulares. Con el paso del tiempo, más autores abordarían el concepto. Para *Sheldon* (2012) implica utilizar el ciberespacio en aspectos tácticos, técnicos y operacionales para que los Estados nación alcancen sus objetivos estratégicos en la política internacional. Por su parte, *Kuehl* (2009, 6) expresa que el concepto es: "[el] *centro de un conjunto nuevo de conceptos y doctrinas que son una palanca clave en el desarrollo y ejecución de política, ya sea contra el terrorismo, crecimiento económico o asuntos diplomáticos".*

Estas definiciones ayudaron a la construcción de múltiples índices que buscan medir el nivel de ciberpoder o el desarrollo de capacidades cibernéticas de los Estados nación. Entre estas se encuentran el *Global Cybersecurity Index* (GCI), el *National Cybersecurity Index* (NCSI), el *National Cyber Power Index* (NCPI), y el *Cyber Capabilities And National Power* (CCNP). Para los fines prácticos se indica que el NCPI y CCNP tienen como objetivo medir el ciberpoder de los Estados nación, e identifican a las potencias globales del ciberespacio. El GCI y el NCSI se centran en una visión cooperacionista y de gobernanza global. En ese sentido, se presenta una breve descripción de cada métrica:

- *Global Cybersecurity Index* (GCI): creado por la Unión Internacional de Telecomunicaciones (UIT), está vinculado a la Agenda Global de Ciberseguridad creada en 2004. El índice se divide en cinco pilares y 25 indicadores para analizar el compromiso de los Estados nación con el desarrollo de la ciberseguridad global. Es importante enmarcar

que el GCI está abocado a fomentar la cooperación internacional de las naciones, actores estatales y actores no estatales organizados, para garantizar la gobernanza y buena regulación del ciberespacio. Sus cinco pilares son: 1) marco legal, 2) medidas t*écnicas,* 3) estructura organizacional, 4) desarrollo de capacidades y 5) cooperación internacional. El GCI ha tenido un total de cuatro iteraciones, realizadas en 2014, 2017, 2018 y 2020. Y es la única métrica de ciberseguridad que presenta información sobre 193 países del mundo (GCI 2021).

- *National Cybersecurity Index* (NCSI): desarrollado por la *E-Governance Academy* del gobierno de Estonia, es un instrumento que mide las capacidades de resiliencia, y en forma discreta, de disuasión, de los Estados nación a través de un total de 12 indicadores. Estos son: 1. Política. 2. Delimitación de amenazas. 3. Desarrollo de educación. 4. Aportación global. 5. Nivel de desarrollo digital. 6. Protección de servicios esenciales. 7. Identificación electrónica y confidencialidad de servicios. 8. Protección de datos personales. 9. Respuesta a ciberincidentes (CIRC). 10. Administración de crisis cibernética. 11. Política de lucha contra el cibercrimen. 12. Operaciones militares. El NCSI inició sus primeros levantamientos en 2017 y proporciona información sobre 161 países.
- *National Cyber Power Index* (NCPI): medida creada por el *Belfer Center* de la *John F. Kennedy Goverment School* de la Universidad de Harvard, el cual se centra en presentar un análisis en torno al ciberpoder. Analiza un total de 30 países del mundo, con base a siete objetivos vinculados a la seguridad nacional y la política exterior: 1. Vigilancia y seguimiento de grupos domésticos. 2. Fortalecimiento y mejora de la ciberdefensa nacional. 3. Control y manipulación del entorno de información. 4. Recopilación de inteligencia en otros países para la seguridad nacional. 5. Creciente competencia cibernética y tecnológica nacional. 6. Destrucción o desactivación de la infraestructura y las capacidades de un adversario. 7. Definición de normas técnicas y normas cibernéticas internacionales. El NCPI resalta por encima del GCI y el NCSI, a razón de que profundiza en las capacidades de defensa y ofensa de los países, con el fin de ser una medida de ciberpoder y potencial comprobado de los Estados nación para atacar a otra nación o protegerse de una agresión de frente a un ciberataque. Es la medida que más se acerca a la visión neorrealista de *Nye Jr.* de ciberpoder. A la par expresa que considera como potencias del ciberespacio a un total de cinco países: Estados Unidos, China, Reino Unido, Rusia e Israel.
- *Cyber Capabilities And National Power* (CCNP): publicado por el International *Institute for Strategic Studies*, *think tank* del Reino Unido. La métrica se centra en evaluar el poder cibernético de 15 países a través de siete categorías, las cuales son: 1. Estrategia y doctrina. 2. Gobernanza, mando y control. 3. Capacidad básica de ciberinteligencia. 4. Ciberempoderamiento y dependencia. 5. Ciberseguridad y resiliencia. 6. Liderazgo mundial en asuntos del ciberespacio. 7. Capacidad cibernética ofensiva. Clasifica a cada país en tres diferentes niveles de ciberpoder, en los que el nivel 1 representa al más poderoso y el nivel 3 representa los de menos poder.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

Metodología de análisis comparativo de ciberpoder y capacidades cibernéticas

Presentada la disposición de múltiples métricas que permiten abordar el concepto de ciberpoder y el desarrollo de capacidades cibernéticas se decidió utilizar estas medidas para hacer un análisis comparativo. En este sentido, se optó por utilizar el método comparativo en ciencias sociales de corte cualitativo, por la disposición de la información para un análisis bibliográfico y documental de los índices.

Sobre el método comparativo, *Tonon* (2011) indica que es útil como estrategia de investigación, porque permite identificar y analizar similitudes y disimilitudes entre las unidades de estudio. Esta comparación se puede realizar a través del criterio de homogeneidad, aspecto clave que contemplan los índices del GCI, NCSI, NCPI y el CCNP. También, el análisis comparativo facilita analizar un número acotado de unidades de estudio, como pueden ser las ponderaciones de los países de forma ágil (Colino 2009).

De esta forma, se utilizarán estas métricas para hacer dos análisis, el primero corresponde a confrontar el nivel de ciberpoder entre Estados Unidos y China. Y el segundo a contrastar el nivel de desarrollo de capacidades cibernéticas de estas dos potencias con América Latina. Se indica que para realizar un análisis comparativo de ciberpoder entre Estados Unidos y China son de utilidad el NCPI y CCNP. Para analizar el nivel de asimetría de capacidades cibernéticas, entre estos actores y los países de América Latina, son útiles el GCI y el NCSI.

Comparativo del ciberpoder de Estados Unidos y China

En el primer análisis, centrado en el NCPI y relacionado al ciberpoder se encontró que ambos países están entre las cinco primeras posiciones en las siete variables de la medición. La métrica resalta cómo China ha invertido fuertemente en investigación y desarrollo de tecnologías, que permitan al país lograr múltiples objetivos en el ciberespacio en las últimas dos décadas (*Voo et al.* 2020). Estos resultados reflejan su posición cada vez más fuerte en el dominio. Al realizar el comparativo por cada una de las siete dimensiones se encontraron los siguientes hallazgos:

I. Vigilancia del Gobierno: China se encuentra en la posición número uno, mientras que Estados Unidos en la tres. Esto se debe a que el gigante asiático mantiene fuertes controles para contenido considerado ilegal por su gobierno, que no es de libre acceso para su población. También, es importante hacer notar que el país cuenta con cuerpos policiales y agencias de inteligencia con cibercapacidades para su regulación. Si bien, estas condiciones se asocian a que China es considerado un país autoritario, podemos citar que Estados Unidos tiene medidas similares a través de la Agencia de Seguridad Nacional.
II. Defensa Nacional: Estados Unidos se encuentra en la posición número cuatro y China en el número uno. El puntaje de esta dimensión se vincula a la capacidad de resiliencia cibernética y medidas activas de ciberdefensa. Con lo cual, China está más preparado que

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

los Estados Unidos para contener los efectos de un ciberataque, ya sea de un grupo *hacktivistas* o un Estado nación. Del mismo modo, episodios vinculados a grandes filtraciones como el *Cablegate* de *WikiLeak* (2011), el caso *Snowden* (2013) o más recientemente las filtraciones del Pentágono, denominado como *Pentagon Leaks* (2023), muestran una vulneración más sensible por parte de Estados Unidos.

III. Control de la información: Estados Unidos está en la posición número uno y China en tercer lugar. En este indicador se mide la capacidad del Estado para eliminar material extremista, refutar propaganda extranjera o contener el flujo de desinformación. Estados Unidos lidera a razón del papel de sus agencias militares y de inteligencia para contener a grupos extremistas o reclutar a nuevos adeptos entre la población civil. De forma sorprendente, aunque China mantiene una fuerte política de regulación de contenidos en internet, no lidera la dimensión.

IV. Capacidad ofensiva*:* Estados Unidos está en la primera posición y China en cuarto lugar. Esto implica que la potencia norteamericana tiene más capacidades para realizar una operación cibernética y militar capaz de alcanzar resultados efectivos, junto a países como Reino Unido, Israel y Rusia. La métrica indica que las operaciones ofensivas de Estado a Estado no son una acción que realice de forma constante, pero tiene el potencial de alcanzar sus objetivos. Asimismo, aclara que las operaciones cibernéticas de China se focalizan en actores privados, principalmente empresas, con el fin de obtener propiedad intelectual o beneficios económicos.

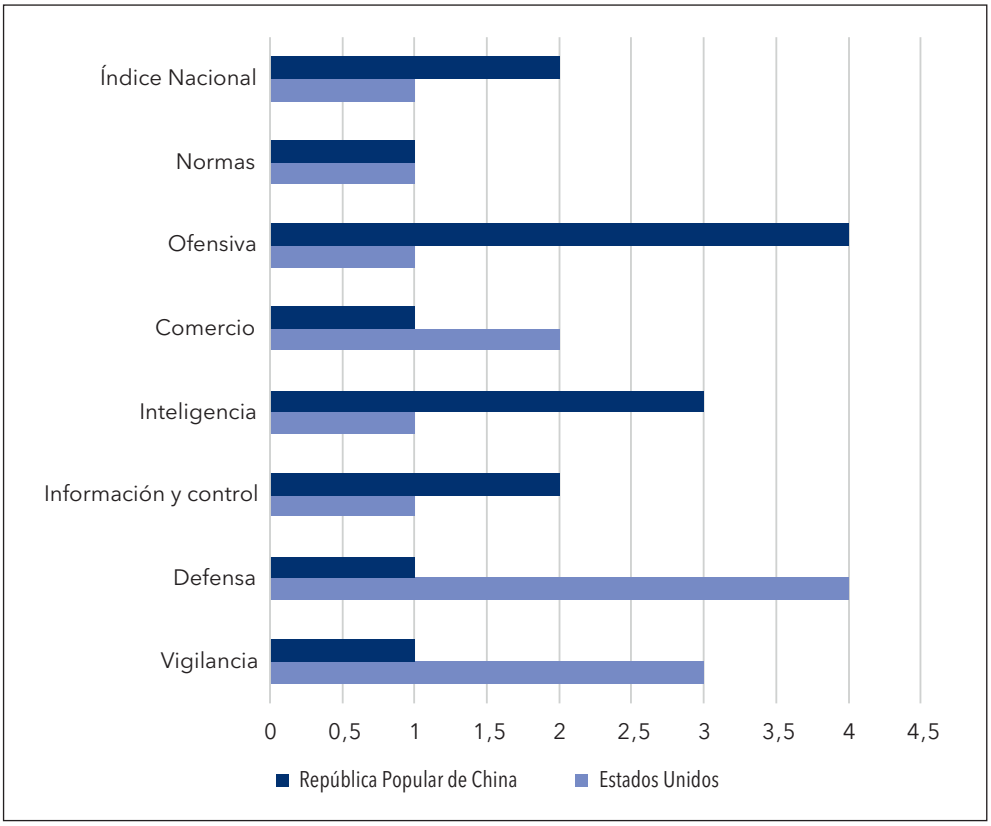
V. Uso del ciberespacio para inteligencia para la seguridad nacional: Estados Unidos está en la posición número uno y China en tercer lugar. En este indicador destaca la importancia de las filtraciones de *Edward Snowden*, de 2013 y 2015, que evidenciaron las altas capacidades de recolección de información de Estados Unidos, a pesar de las fuertes vulneraciones sufridas por estas filtraciones. No obstante, estos episodios ayudaron a reforzar sus medidas nacionales de ciberseguridad. Sobre el caso de China, no se han suscitado casos de vulneración, pero se asume que hace un buen uso de la inteligencia para la promoción de seguridad nacional, sobre todo con opositores políticos de escala nacional.

VI. Uso del ciberespacio para el desarrollo comercial: en esta dimensión destaca China por encabezar el liderazgo de la competencia comercial y tecnológica. Esto se relaciona con su capacidad de realizar operaciones cibernéticas en aras de ejecutar espionaje industrial o robo de propiedad intelectual, con el fin de incentivar y hacer crecer su industria y economía nacional a través de la explotación de información extraída que impacte en investigación, desarrollo de industrias nacionales y asociaciones público-privadas.

VII. Desarrollo de normas y marco legal de combate al cibercrimen: en este indicador, Estados Unidos se encontró en la primera posición, a razón de que en las últimas dos décadas creó un marco legal efectivo para la contención de ciberdelitos de carácter nacional e internacional. Por su parte, China está en quinta posición, a razón de tener mecanismos combate al cibercrimen, pero no enmarcados en códigos o leyes vinculados a referentes como el Convenio de Budapest u organismos internacionales.

El análisis anterior presenta que el ciberpoder entre los dos países no es asimétrico. Y su capacidad de vulnerarse desde el ciberespacio es altamente viable de cara a una confrontación en este nuevo dominio. Este comparativo puede verse en el gráfico 1.

Gráfico 1. Comparativo de ciberpoder, según las siete dimensiones del NCPI entre China y Estados Unidos[3]



Fuente: *Voo* et al. (2020).

Por otra parte, entre los hallazgos más trascendentales del CCNP (2021) se identificó que Estados Unidos es el único país en el nivel 1, reservado para Estados con fortalezas líderes en las siete categorías. Esto porque que percibe amenazas de Rusia y China y adoptó un enfoque sólido, para ampliar y fortalecer sus capacidades en contra de estos rivales. El índice resalta la orden ejecutiva firmada por el presidente *Joe Biden*, del 12 de mayo de 2021, tras el incidente de ciberseguridad contra *Colonial Pipeline*, un ataque a infraestructura nacional crítica que afectó al sistema de oleoductos de petróleo refinado más grande en los Estados Unidos.

3 En esta visualización es importante notar que entre más cerca esté del uno la barra indica que el país se encuentra en la posición más alta de los 30 países incluidos en el NCPI (2021).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

Por esto el CCNP (2021) indica que Estados Unidos goza de superioridad en términos de empoderamiento de la información y las comunicaciones, y cinco de los seis países que podrían considerarse sus pares son sus aliados o socios estratégicos. Por último, el estudio estima que, si bien Estados Unidos no es el principal país que realiza operaciones cibernéticas ofensivas en el mundo, es probable que sus capacidades cibernéticas sean las más efectivas y sofisticadas del mundo.

En el nivel 2 están los Estados que tienen fortalezas líderes en alguna categoría. Los Estados ubicados en ese nivel son: Australia, Canadá, China, Francia, Israel, Rusia y Reino Unido. Para determinar la clasificación relativa entre los Estados se debe analizar qué categorías son las más importantes. Por ejemplo, considerando la combinación de seguridad o inteligencia cibernéticas de clase mundial, capacidad cibernética ofensiva sofisticada y poderosas alianzas, Israel y el Reino Unido están en la parte superior del nivel. De forma alternativa, si los factores decisivos se evalúan como la cantidad de recursos (específicamente humanos

Gráfico 2. Niveles de poder, según el CCNP (2021)

Fuente: CCNP (2021).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

y financieros) dedicados a operaciones cibernéticas, la audacia operativa sin restricciones y la experiencia diaria, China y Rusia lideran el segundo lugar. Por último, si uno considera el potencial para pasar al primer nivel, China es el único país, debido a su gran y creciente capacidad industrial digital.

En el nivel 3 están los Estados que tienen fortalezas o fortalezas potenciales en alguna categoría, pero debilidades significativas en otras. El informe concluye que India, Indonesia, Irán, Japón, Malasia, Corea del Norte y Vietnam están en él. Al igual que con el segundo nivel, se debe determinar la categoría más importante para la clasificación de los Estados. Por ejemplo, Malasia está en la cima si la fortaleza central es seguridad cibernética. Si la audacia operativa y la experiencia en operaciones cibernéticas fueran clave, Irán lidera esta dimensión. Si uno cree que el potencial para subir de nivel es lo más importante, Japón es el único país considerado, debido a su industria de alta tecnología relacionada con el internet.

América Latina frente a China, Estados Unidos y las tecnologías del futuro

Una vez analizado el nivel de ciberpoder entre Estados Unidos y China, se procede a analizar el nivel de asimetría de capacidades cibernéticas, entre estos dos actores y los países de América Latina. Para este objetivo son útiles el GCI (2021) y el NCSI (2023). Para esto, es importante mencionar que en ambas mediciones se promediaron las calificaciones de los países de la región para analizarlos como conjunto.

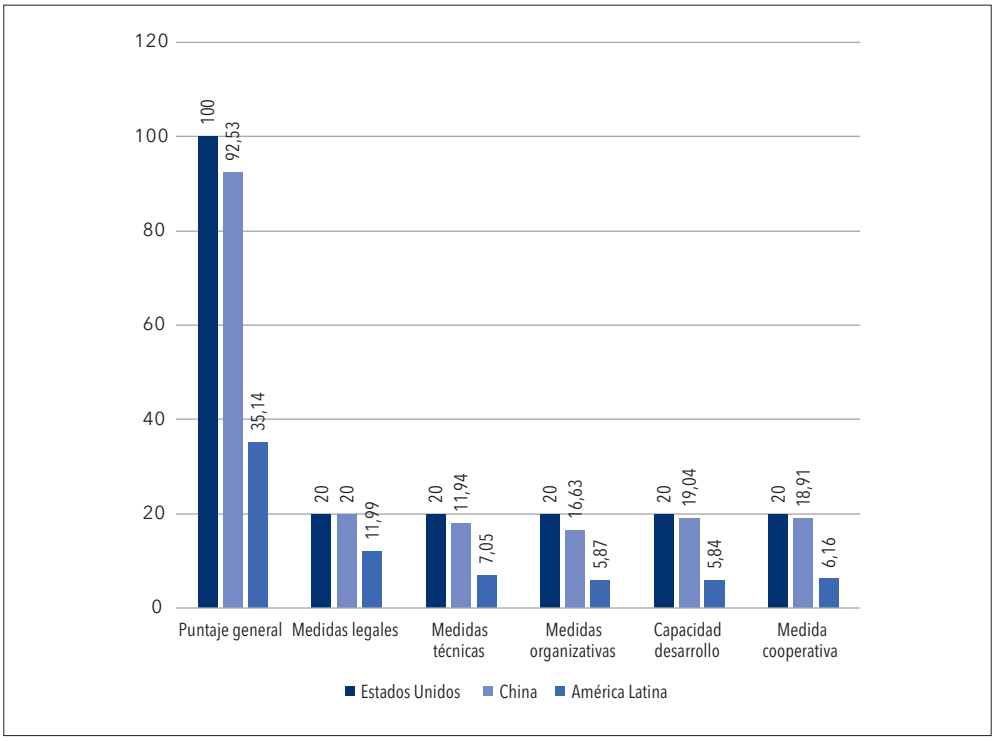
En el gráfico 3 se presenta la información de los tres actores. En él se observa que la métrica la lidera Estados Unidos con una calificación de 100 puntos, nota más alta del GCI (2021). Mientras que China alcanza una cifra de 92,53 puntos. Es importante aclarar que para alcanzar dicha cifra se suman las cinco dimensiones, en los que la nota más alta para cada una son 20 puntos. Estados Unidos alcanza esta cifra en todas, mientras que China solo lo hace en medidas legales. Las medidas en las que América Latina presenta fortalezas es en esta misma dimensión, con 11,99 puntos, lo que indica que los países han avanzado en leyes contra el cibercrimen y en la creación de estrategias nacionales de ciberseguridad. En contraposición, sus principales carencias están en medidas organizativas (5,87 puntos), las cuales implican la delimitación de responsabilidades y la estructura organizaciones para implementar una política nacional de ciberseguridad. Y la dimensión de capacidad de desarrollo (5,84), que implica la creación de una cultura de ciberseguridad en la población, el desarrollo de una industria nacional y expertos en la materia.

Con relación a los doce indicadores del NCSI[4] (2023), en el gráfico 4 se presenta el comparativo entre los tres actores. En él se destaca que las dimensiones entre las que mejor se

4 Los datos de Estados Unidos, China y América Latina se obtuvieron en la última actualización del NCSI con corte al 24 de abril de 2023.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

Gráfico 3. Comparativo GCI de Estados Unidos, China y América Latina



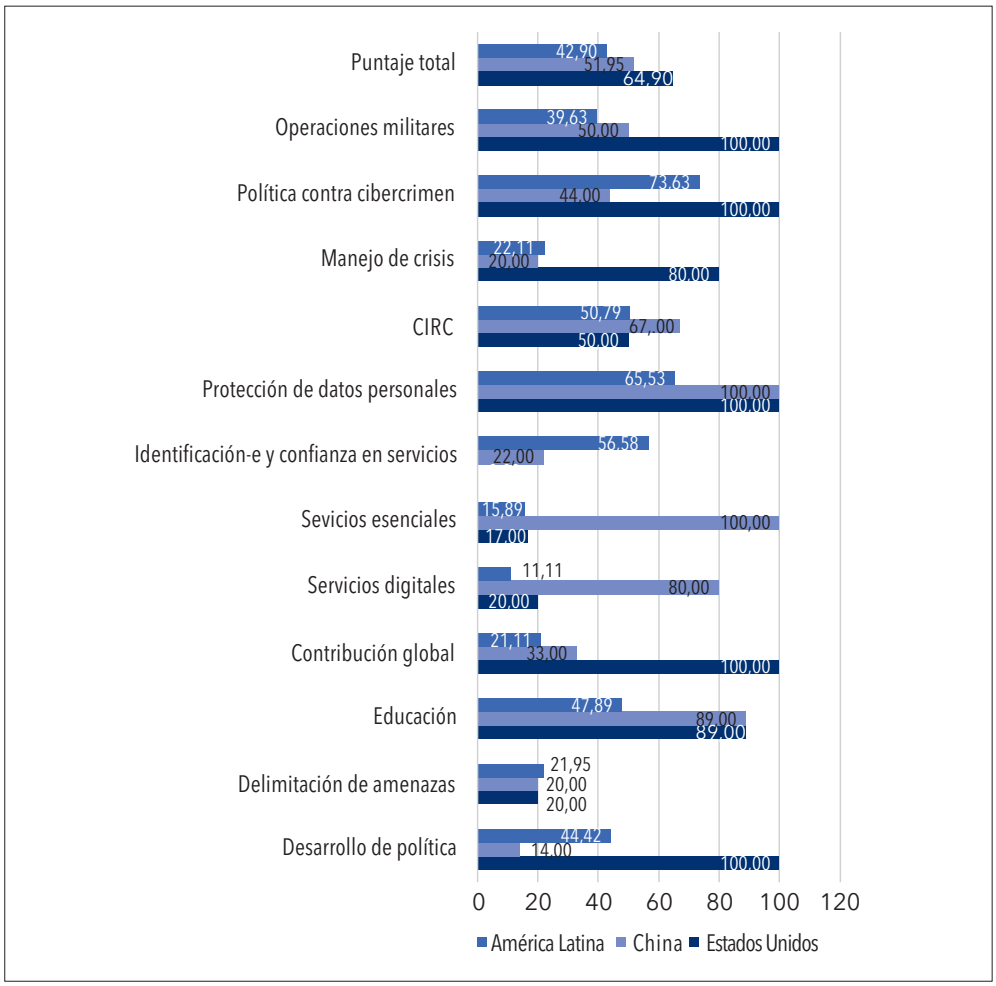
Fuente: GCI (2021).

encuentra posicionada la región son el desarrollo de política contra cibercrimen (73,63 puntos de un total de 100), protección de datos personales (65,53) e identificación electrónica y confianza de servicios (56,58). Sin embargo, la región detenta severas fallas en dimensiones como protección de servicios esenciales (15,89), protección de servicios digitales (11,11) Del mismo modo, destacan las bajas notas en contribución global (22.1), manejo de crisis cibernética (22,11) y operaciones militares (39.63).

La información de NCSI (2023) es relevante y da nuevas ópticas sobre las capacidades cibernéticas de Estados Unidos y China, desde un enfoque de la gobernanza global del ciberespacio. Por ejemplo, en el caso de la nación de Asia se le evalúa de forma severa en manejo de crisis (20,00), desarrollo de política (14,00), delimitación de amenazas (20,00) e identificación electrónica y confianza de servicios (22.00). Por su parte, Estados Unidos detenta notas bajas en delimitación de amenazas (20,00), protección de servicios esenciales (17,00), protección de servicios digitales (20,00). Incluso en la dimensión de identificación electrónica y confianza de servicios la medida da la nota de cero al país. Probablemente esto se deba a la gran cantidad brechas de información a empresas privadas y vulneraciones a agencias gubernamentales de Estados Unidos.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

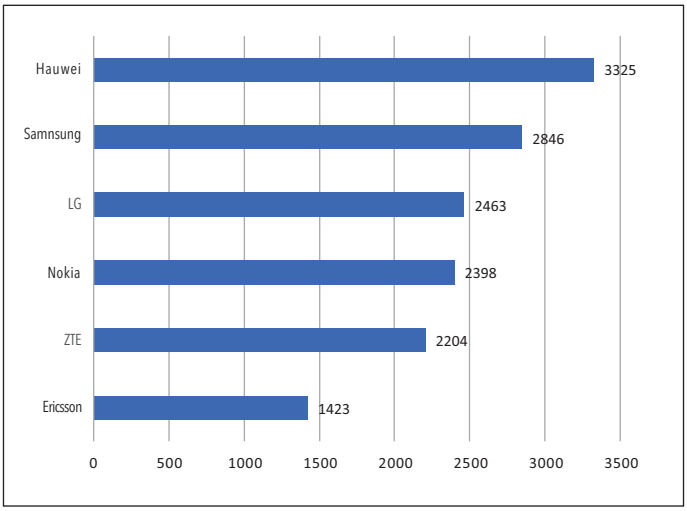
Gráfico 4. Comparativo NSCI de Estados Unidos, China y América Latina



Fuente: NCSI (2023).

En las fortalezas de China están protección de datos personales (100,00), protección de servicios esenciales (100,00) y desarrollo de programas de educación (89,00). Mientras que Estados Unidos destaca en desarrollo de política (100,00), contribución global (100,00), protección de datos personales (100,00), política contra cibercrimen (100.00) y operaciones militares contra el ciberespacio (100,00). El análisis de los instrumentos del GCI (2021) y el NCSI (2023) muestran que en el desarrollo de políticas nacionales, medidas legales, combate al cibercrimen y capacidad organizativa, Estados Unidos es un referente global y un ejemplo para la región latinoamericana. Se afirma esto porque dichos modelos de política se basan en referentes internacionales como la UIT y la ONU. A la par que, al ser un Estado democrático, la cercanía

Gráfico 5. Cinco empresas con más patentes concedidas en industria de redes 5G



Fuente: elaboración propia con base en IPlytics (2022).

con los gobiernos latinoamericanos se empata más en estas áreas. Por otra parte, China es una nación que presenta fuertes esferas de influencia en modelos de educación, y tiene potencial para ser proveedor clave en la protección de servicios esenciales y digitales para la región.

En el caso de China, destaca su liderazgo en el desarrollo de tecnologías innovadoras como la inteligencia artificial, la computación cuántica, las redes 5G, o el procesamiento de *big data*. En la actualidad, el país representa uno de los máximos referentes de desarrollo tecnológico y es considerada una potencia del ciberespacio en estas áreas. Esto se refleja en el peso cada vez mayor en el mundo de sus compañías tecnológicas como Huawei, Xiaomi, o las aplicaciones de redes sociales y sitios web de *e-commerce* como Ali Express o Tik Tok. En este sentido, es importante mencionar que con base al *World Intellectual Property Indicators 2022*, durante el periodo 2020-2021, China fue el país número uno que presentó solicitudes de patentes a nivel global, con una cifra de 1 585 663 casos, lo cual representó el 46,6% del total de solicitudes mundiales (WIPO 2022). En segunda posición se encontraron los Estados Unidos, muy por detrás, con 591 473 solicitudes, que representan solo el 17,4% global. Un ejemplo de desarrollo de China en esta área se observa en IPlytics, que documenta el número de patentes desarrolladas por compañías internacionales, en diferentes sectores. El cual indica que para el caso de las telecomunicaciones la empresa Hauwei lidera la lista de patentes a escala internacional con un total de 3 325.

También, en julio del 2021, la Universidad de Ciencia y Tecnología de China presentó el computador cuántico *Zuchongzhi*, que batió el récord establecido por Google en 2019 para la resolución de un problema de análisis de datos. Esto una muestra de la aceleración tecnológica de China para ser el líder en este sector y conseguir la supremacía en las distintas

áreas como computación cuántica e inteligencia artificial (*Zhang* et al. 2019). Otro aspecto trascendental de señalar es el desarrollo de "El Cerebro", un enorme sistema de vigilancia digital por parte del Estado, que recopila *big data* por medio de una compleja red de cámaras de videovigilancia, así como el procesamiento de información de su población a través de los dispositivos IoT. Dicho sistema permitió aplicar medidas coercitivas para el control de la población durante la pandemia de COVID-19 que ayudaron a superar más rápido la emergencia global de salud. Todas estas acciones se vinculan al hecho de que los líderes chinos han abrazado al desarrollo tecnológico y en materia de ciberseguridad como un aspecto clave en su posicionamiento global (Raud 2016).

Este poderío tecnológico puede materializarse en el futuro como componente de la estrategia política y económica de China en América Latina. Sobre esto *Farah* y *Babineau* (2019) indican que China ha invertido más de 250 000 000 000 de dólares en la región para incrementar su influencia. Esta estrategia económica se combina con acercamientos políticos a países con ideología de izquierda y antagónicos a Estados Unidos como Venezuela, Nicaragua y Cuba. Para *Ellis* (2022) esto refuerza los modelos políticos autoritarios de China en la región, a la par que garantiza el apoyo de las naciones latinoamericanas en iniciativas globales como la cuestión de Taiwán, así como la disponibilidad de recursos naturales y refuerza una dependencia económica que puede extender a áreas como la tecnología y la ciberseguridad.

Conclusiones

A lo largo de la presente investigación se identificó cómo el ciberespacio se ha vuelto una nueva esfera de influencia de los Estados nación y de la política internacional. También, los antagonismos de China y Estados Unidos, así como sus visiones en torno al desarrollo del poder por nociones como el *Hard Power* y el *Smart Power.* En el ámbito de la conceptualización del poder instrumentos como el NCPI y el CCNP muestran que la potencia asiática se encuentra cerca de superar o equipararse a los Estados Unidos. Por otra parte, los hallazgos de capacidades cibernéticas realizados entre el NSCI y el GCI indican que existe una asimetría en el desarrollo de América Latina, donde ambos actores puedes ser modelos para seguir o socios estratégicos.

En la construcción de una política de ciberseguridad, mecanismos contra el cibercrimen y creación de marco organizacional, Estados Unidos es un modelo para la región. Sin embargo, en el ámbito de la consolidación y creación de nuevas tecnologías como las redes 5G, la inteligencia artificial, y la computación cuántica, China es una nación líder. Por último, se debe decir que China cuenta con una estrategia de expansión de influencia en la región basada en el *Smart Power* y principalmente cimentada en la cooperación económica. No obstante, las condiciones de capacidades cibernéticas de América Latina hacen viable que esta pueda extenderse a la esfera de la tecnología y la ciberseguridad en el futuro. Aspecto que deberá vigilar Estados Unidos, en aras de no perder su liderazgo en la región y en el mundo.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 36 • mayo-agosto 2023 • pp.66-84
ISSN 1390-4299 (en línea) y 1390-3691

Bibliografía

Aguilar-Antonio, Juan. 2020. "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas". *Revista de Estudios en Seguridad Internacional* 6 (2): 17-43.

Aguilar-Antonio, Juan. 2021. "Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior". *Estudios Internacionales* 53 (198): 169-197.

CCNP (Cyber Capabilities and National Power). 2021. "National Power: A Net Assessment. International Institute for Strategic Studies". *The International Institute for Strategic Studies.* https://bit.ly/3AoKrcT

Chang-Liao, Nien-Chung. 2016. "China's new foreign policy under Xi Jinping". *Asian Security* 12(2): 82-91.

Colino, César. 2009. *Método comparativo. Diccionario Crítico de Ciencias Sociales. Terminología Científico-Social.* Madrid-México: Plaza y Valdés.

Ellis, Evan. 2022. "China's Role in Latin America and the Caribbean". *The Center for Strategic and International Studies*. https://bit.ly/3AlxTD9

Farah, Douglas y Babineau, Kathryn. 2016. "Extra-regional actors in Latin America". *Prism* 8(1): 96-113. https://bit.ly/2CtUAHQ

Ferdinand, Peter. 2016. "Westward ho—the China dream and "one belt, one road." Chinese foreign policy under Xi Jinping". *International Affairs* 92(4): 941-957.

GCI (Global Cybersecurity Index). 2021. "Global Cybersecurity Index. International Telecommunication Union", https://bit.ly/34rPZ4C

IPlytics. 2022. "Who is leading the 5G patent race?", https://bit.ly/3UWDp8D

Hurel, Louis-Marie. 2022. "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America". *Global Security Review* 2(7): 1-12.

Jintao, Hu. 2017. "Hold High the Great Banner of Socialism with Chinese Characteristics and Strive for New Victories in Building a Mo-derately Prosperous Society in all", https://on.china.cn/3MXWDJ4

Kello, Lucas. 2013. "The meaning of the cyber revolution: Perils to theory and statecraft". *International Security* 38(2): 7-40.

Kittichaisaree, Kriangsak. 2017. "Introduction: Perspectives of Various Stakeholders and Challenges for International Law". En *Public International Law of Cyberspace,* editado por Kriangsak Kriangsak. 1-22. Springer, Cham.

Kuehl, Daniel. 2009. "From cyberspace to cyberpower: Defining the problem. Cyberpower and national security". En *Cyber Power*, editado por Franklin D. Kramer, Stuart H. Starr y Larry Wentz, 24-43. Washington DC: National Defense University.

Mordor Intelligence. 2021. "Latin America Cybersecurity Market - Growth, Trends, Covid-19 Impact, And Forecasts (2022 - 2027)", https://bit.ly/3GWFCLI

NCSI (National Cyber Security Index). 2023. "National Cyber Security Index. E-Governance Academy", https://bit.ly/2XS1eAR

Nye Jr, Joseph. 1990. *Bound to lead: The changing nature of American power.* Basic books.
Nye Jr, Joseph. 2004. *Soft power: The means to success in world politics*. Public affairs.
Nye Jr., Joseph. 2010. *Cyber power.* Cambridge: Harvard University Press.
Nye Jr., Joseph. 2011. *The future of power.* Public Affairs.
Pu, Xiaoyu. 2019. "Leadership and the rise of great powers". *Cambridge Review of International Affairs*, DOI: 10.1080/09557571.2019.1676976
Raud, Mikk. 2016. "China and cyber: attitudes, strategies, organisation". The NATO Cooperative Cyber Defence Centre of Excellence.
Rosas-González, María, Priscila Magaña-Huerta y Rebeca Haro-Barón. 2023. "La ruta sanitaria de la seda y el poder suave de la República Popular China ante el SARS-CoV-2". *Foro Internacional* 63(1): 85-132.
Sheldon, John. 2012. "Deciphering Cyberpower: Strategic Purpose in Peace and War". *Strategic Studies Quarterly* 2 (5): 95–112.
Sonic Wall. 2021. "Threat Report 2021", https://bit.ly/3UQDzhD
Tonon, Graciela. 2011. "La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral". *Kairos: Revista de temas sociales* (27): 167-179.
Villamizar Lamus, Fernando. 2012. "Smart power y la política exterior de la República Popular de China hacia América Latina y el Caribe". *Revista Enfoques* 11(17): 33-51.
Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy y Anina Schwarzenbach. 2020. *National cyber power index 2020*. Belfer Center for Science and International Affairs/Harvard Kennedy School.
White House. 2017. "The national security strategy of the United States. Washington, DC: Executive Office of the President", https://bit.ly/3n1JGU8
WIPO. 2022. "World Intellectual Property Indicators 2022", https://bit.ly/3Lprtco
Xuetong, Yan. 2019. *Leadership and the rise of great powers*. Princeton University Press.
Zhang, Chunman, y Xiaoyu Pu. 2019. "Introduction: Can America and China escape the thucydides trap?". *Journal of Chinese Political Science* 24 (1): 1-9.
Zhang, Qiang, Feishu Xu, Li Li, Nai- Le Liu y Jian-Wei Pan. 2019. "Quantum information research in China". *Quantum Science and Technology* 4(4): 040503.