Escuela Superior de Guerra "General Rafael Reyes Prieto"

Estudios en
SEGURIDAD y DEFENSA

estud.segur.def. Bogotá, D. C., Colombia. V. 17 N.° 33 pp. 262. Enero - junio de 2022. ISSN 1900-8325 - eISSN 2744-8932

Revista científica *Estudios en Seguridad y Defensa*

Revista colombiana de seguridad y defensa
Bogotá, D.C., Colombia

ISSN: 1900-8325 - eISSN: 2744-8932
esdeguerevistacientifica.edu.co

La cibergeopolítica de China: un interés estratégico de Estado

Nixon Edier Vargas Chaparro
https://orcid.org/0000-0002-7381-035X
nixon.vargas@buzonejercito.mil.co

Cómo citar

Vargas Chaparro, N. E. (2022). La cibergeopolítica de China: un interés estratégico de Estado *Estudios en Seguridad y Defensa, 17*(33), 201-222.
https://doi.org/10.25062/1900-8325.328

Publicado en línea
Junio de 2022

Los contenidos publicados por la revista científica *Estudios en Seguridad y Defensa* son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.es

Para mayor información:
revistacientificaesd@esdegue.edu.co

Para enviar un artículo:

https://esdeguerevistacientifica.edu.co/index.php/estudios/login?source=%2Findex.php%2Festudios%2Fsubmission%2Fwizard

Cómo citar este artículo

Vargas Chaparro, N. E. (2022). La cibergeopolítica de China: un interés estratégico de Estado. *Estudios en Seguridad y Defensa, 17*(33), 201-222. https://doi.org/10.25062/1900-8325.328

La cibergeopolítica de China: un interés estratégico de Estado[1]

China's Cyber-Geopolitics: A Strategic State Interest

A cibergeopolítica da China: um interesse estratégico do Estado

NIXON EDIER VARGAS CHAPARRO[2]
Centro de Doctrina del Ejército Nacional de Colombia, Colombia

Resumen

El crecimiento exponencial de Beijing en el sistema económico está condicionando al escenario internacional de las próximas décadas; una situación en que las dinámicas del cambio climático y los avances en materia de tecnología definirán el contexto global del siglo XXI. Así las cosas, para Xi Jinping se vuelve un imperativo el desarrollo tecnológico; en especial, el dominio del ciberespacio. En términos generales, dentro su visión a largo plazo se encuentra ser la economía líder en el sistema internacional, definida por la política exterior del Partido Comunista Chino (PCCh).

Fecha de recepción

14 de enero de 2022

Fecha de aceptación

21 de abril de 2022

Palabras clave

China, ciber, estrategia, poder.

Keywords

China, cyber, strategy, power.

Palabras-chave

China, cibernético, estratégia, posso.

1. El artículo fue desarrollado en apoyo al grupo de investigación del Centro de Doctrina del Ejército Nacional, en el cual se desarrollan conceptos relacionado con los dominios de la guerra y sus teorías de poder.

2. Gerente en Seguridad y Análisis Sociopolítico. Estudiante de la Maestría en Estrategia y Geopolítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Analista del Centro Integrado de Información Militar Estratégica (CI3ME), del Ejército Nacional, e investigador del Centro de Doctrina del Ejército Nacional. Contacto: nixon.vargas@buzonejercito.mil.co

Dicho esto, se presenta la pregunta: *¿Cuál sería la estrategia de China en el ciberespacio, entendiendo que este es un factor determinante en el futuro del orden mundial?* Para buscar aproximarnos a la correspondiente respuesta, se desarrolló una investigación exploratoria con un enfoque cualitativo. De igual forma, se apeló a la *teoría del poder ciberespacial*, de Nye (2010), y a los componentes del ciberespacio (físico y virtual) planteados por Pătrașcu (2019), sumado ello a una revisión documental.

Se logró evidenciar que hay una serie de tareas que lleva a cabo el PCCh, en el marco de un probable plan estratégico, o una línea de acción, que busca desplazar a Estados Unidos de su liderazgo mundial económico y otros ámbitos, como el militar, el cultural, el ambiental, el espacial y, desde luego, el ciberespacial, donde tendrá una gran ventaja si materializa sus planes.

Abstract

Beijing's exponential growth in the economic system is conditioning the international scenario for the coming decades, a situation in which the dynamics of climate change and advances in technology will define the global context of the twenty-first century. Thus, for Xi Jinping, technological development becomes an imperative, especially in the domain of cyberspace. At a general level, his long-term vision includes being the leading economy in the international system, as defined by the foreign policy of the Chinese Communist Party (CCP).

Therefore, the question arises: What would China's strategy be in cyberspace, understanding that this is a determining factor in the future of the world order? An exploratory research study was developed with a qualitative approach to seek an answer, which employed the theory of cyberspace power proposed by Nye (2010) and the components of cyberspace (physical and virtual) raised by Pătrașcu (2019), in addition to a documentary review.

It was possible to show that there are a series of tasks carried out by the CCP within the framework of a probable strategic plan or a line of action that seeks to displace the United States from its economic world leadership and other domains, such as military, cultural, environmental, space, and, of course, cyberspace, where China will have a great advantage if it materializes its plans.

Resumo

O crescimento exponencial de Pequim no sistema econômico está condicionando o cenário internacional para as próximas décadas, situação em que a dinâmica das mudanças climáticas e os avanços tecnológicos definirão o contexto global do século XXI. Assim, para Xi Jinping, o desenvolvimento tecnológico torna-se imperativo, especialmente o domínio do ciberespaço em nível geral, dentro de sua visão de longo prazo de ser a economia líder no sistema internacional, definida pela política externa do Partido Comunista Chinês (PCC). Dito isso, surge a pergunta: qual seria a estratégia da China no ciberespaço, entendendo que esse é um fator determinante no futuro da ordem mundial? Para buscar aproximar-se dessa resposta, desenvolveu-se uma pesquisa exploratória com abordagem qualitativa. No entanto, recorrendo à teoria do poder do ciberespaço de Nye (2010), e aos componentes do ciberespaço (físico e virtual) propostos por Pătrașcu (2019), somados a uma revisão documental.

Foi possível mostrar que há uma série de tarefas que o PCCh realiza no âmbito de um provável plano estratégico ou linha de ação, que visa deslocar os Estados Unidos de sua liderança econômica mundial e outras esferas, como militar, cultural, ambiental, espacial e, claro, ciberespaço, no qual você terá uma grande vantagem se concretizar seus planos.

Introducción

Durante las últimas dos décadas se ha evidenciado cómo China ha incrementado a pasos agigantados su poder económico, lo cual le ha brindado las herramientas para incrementar su poder militar, diplomático, fiscal y del manejo de la información. Lo anterior, al punto de poner en duda el actual liderazgo hegemónico de Estados Unidos e iniciar una especie de guerra fría entre ambas potencias. Como lo plantea Kissinger (2014), los dirigentes chinos tienden a interpretar la mayoría de las acciones del gobierno de Estados Unidos como un intento de *frustrar el auge de China*. Así mismo, este exasesor gubernamental norteamericano afirma que en el lado estadounidense "el miedo es que una China en expansión socave de manera sistemática la preeminencia estadounidense" (p. 159). Entonces, lo que predijo Kissinger en 2014 fue plasmado por Barack Obama, Donald Trump y, ahora, Joe Biden, con sus políticas de aumentar las exportaciones, disminuir las importaciones estadounidenses e incrementar los aranceles para promover sus intereses y reducir la injerencia china en la economía local.

Sin embargo, esta contienda en el plano global también se debe al giro de la política exterior china, impulsado en los últimos años por Xi Jinping, y cuyo eje es el desarrollo del programa de inversiones llamado la *Nueva Ruta de la Seda*, cuyo propósito es aumentar la influencia de Beijing en el exterior y fortalecer sus recursos tecnológicos; esencialmente, el ciberespacio, en el cual hará énfasis este artículo, y de cómo, a través de este, buscaría incrementar su hegemonía en el ámbito global, además del aumento del control sobre la sociedad y la represión dentro de su país. En palabras de Wang Jisi, citado por González (2020), uno de los principales analistas chinos de política internacional "Las políticas estadounidenses han cambiado porque China ha cambiado" (párr. 3); también afirmó:

> Es posible que EE. UU. sea hoy una versión demediada de la sólida democracia que llegó a ser, pero China ha logrado combinar al mismo tiempo lo peor del nacionalismo, lo peor del capitalismo y lo peor del comunismo. Todo ello, con la última tecnología. (párr. 3)

Así las cosas, la pregunta que la presente investigación busca responder es: *¿Cuál es la estrategia de China en el ciberespacio, entendiendo que este es un factor determinante en el futuro orden mundial?* Por tanto, se apeló a una investigación de tipo exploratorio para determinar la estrategia de China en el ciberespacio para lograr la hegemonía mundial que tanto desea el gobierno chino. Para ello, se buscó establecer las teorías que abordan el poder en los dominios de la guerra, con mayor énfasis en el dominio ciberespacial. Adicionalmente, se discriminó qué tareas y misiones lleva a cabo China en relación con el dominio ciberespacial y, por

último, describir las implicaciones que tendrá China frente al dominio global y una importante influencia en el ciberespacio del mundo.

Ahora bien, la constante presencia de empresas tecnológicas chinas en el mundo y el desarrollo de infraestructura en esa misma escala obedece a una política exterior de China y a una estrategia frente a la disputa por la hegemonía tecnológica con Estados Unidos y la Unión Europea (UE).

Metodología

Durante la presente investigación se llevó a cabo un enfoque cualitativo en el proceso de recolección de datos, donde se abordó, por un lado, un nivel descriptivo, que buscó indagar sobre el marco conceptual de las teorías del poder en los dominios de la guerra planteados por las Fuerzas Militares (FF. MM.) de Colombia (2018). Adicionalmente a esto, en un nivel aplicativo, se buscó emplear la teoría del poder ciberespacial, de Nye (2010), al igual que los componentes del ciberespacio, de Pătrașcu (2019), a fin de identificar una posible estrategia por parte del gobierno chino de emplear el ciberespacio, y que lo lleve a ejercer una hegemonía global única en las próximas décadas.

Con base en la recolección de la información anterior, se hizo una revisión documental del nivel exploratorio, que condujo a determinar cuáles pueden ser las posibles tareas desarrolladas por China para dominar el ciberespacio en sus dimensiones física y virtual, dentro de una estrategia geopolítica. Una vez se recolectó la información, se compararon los resultados obtenidos entre: primero, la teoría del poder en el ciberespacio y sus componentes; y segundo, el desarrollo de las tareas llevadas a cabo por el PCCh en materia de ciberespacio y telecomunicaciones.

De esta manera, se generaron nuevos datos, que permiten caracterizar una estrategia china en las dimensiones del ciberespacio, en busca de tener control global de este o, por lo menos, tener una influencia importante en el ciberespacio. Al entender dicha estrategia, se buscaría innovar y cambiar el paradigma, además del enfoque con el que actualmente se observa al gigante asiático en el ciberespacio.

Marco referencial

Los dominios de la guerra y las teorías del poder aéreo, naval y terrestre

Este artículo pretende realizar una reflexión de cómo China, a través del ciberespacio —entendiendo que este es uno de los dominios de la guerra—, puede materializar sus objetivos y sus intereses en el sistema internacional. Para las FF. MM. de Colombia (2018), existen cinco dominios de la guerra. El primero es el *dominio terrestre*, definido como el área de la superficie de la *tierra* que termina en el nivel del mar y se superpone con el *dominio marítimo* en el segmento de los litorales. El segundo es el ya mencionado dominio marítimo, que son los océanos, los mares, las bahías, los estuarios, las islas, las zonas costeras y el espacio aéreo por encima de estos, incluidos sus litorales, y en el que China está muy interesado, ya que con el control de este dominio, a través de una flota naval militar, puede asegurar sus rutas comerciales en su proyecto de crear el Collar de Perlas[3].

El tercer dominio es el *dominio aéreo*, el cual comprende la atmósfera, que comienza en la superficie de la Tierra y se extiende hasta la altura donde sus efectos sobre las operaciones terrestres o navales se hacen insignificantes. El cuarto dominio es el *dominio espacial*, que es el ambiente donde la radiación electromagnética, las partículas cargadas y los campos eléctricos y magnéticos son las influencias físicas dominantes; abarca la ionósfera y la magnetósfera de la Tierra, el espacio interplanetario y la atmósfera solar. Y el último, y con base en el cual este artículo aborda las pretensiones de China, es el *dominio ciberespacial*, que es concebido como un dominio global dentro del *ambiente de la información*[4]; este último, consistente en redes interdependientes de infraestructura de tecnologías de la información y datos contenidos, que incluyen: internet, telecomunicaciones, redes, sistemas informáticos y procesadores y controladores integrados.

3 Teoría geopolítica sobre las posibles intenciones chinas en la región del océano Índico de instalar una red de bases militares y relaciones comerciales chinas a lo largo de sus líneas marítimas de comunicación, que se extienden desde la China continental hasta Port Sudan, en el Cuerno de África. Estas líneas marítimas atraviesan varios puntos importantes de congestión marítima, como el estrecho de Mandeb, el estrecho de Malaca, el estrecho de Ormuz y el estrecho de Lombok, así como otros centros estratégicos marítimos en Pakistán, Sri Lanka, Bangladés, Maldivas y Somalia.

4 Conjunto de individuos, organizaciones y sistemas que recolectan, procesan, difunden o actúan sobre la información. Manual Fundamental del Ejército MFE 3-0 Operaciones.

Figura 1. Dominios de la guerra

Fuente: Fuerzas Militares de Colombia (2018).

Pero para entender cómo cada uno de estos dominios puede materializar un instrumento de poder, se debe citar a los principales teóricos en relaciones internacionales de cada uno de estos. Primero, hablaremos del dominio terrestre, donde la teoría más conocida es la del *Heartland*, o del corazón continental (Mackinder, 2010), la cual, a su vez, afirma que quien controla la zona de Asia central-Rusia central-Siberia tiene las mejores probabilidades de controlar tanto el resto de Asia como el resto de Europa, y obtener así una posición privilegiada a escala mundial.

En la misma línea, Mahan (2013) determina que la cuestión de la extensión del poder continental para Estados Unidos pasa por el control de los océanos y los pasos internacionales marítimos, a partir de una poderosa flota militar y mercante. Así mismo, Douhet (1921) planteó la *teoría del poder aéreo*, la cual se basó en la aplicación de los principios de la aviación militar, cuyo objeto es dirigir su potencial destructor al corazón del adversario (ciudades, centros de producción y abastecimiento, etc.) para, de esa forma, quebrar su capacidad de lucha.

Teorías de poder en el ciberespacio

Ahora bien, centrados en el ciberespacio, en el cual se quiere hacer énfasis, tomaremos como referencia a Stevens y Betz (2011), quienes definen que, dentro del ciberespacio, los recursos estatales pueden usarse para *establecer normas y estándares* de una variedad de instituciones que impactan en el comportamiento de los usuarios; en otras palabras, el ciberespacio puede utilizarse para influir en las opiniones de audiencias extranjeras a través de organizaciones y medios.

De igual forma, Nye (2010) describe el *poder cibernético* como un régimen híbrido único, con propiedades físicas (infraestructuras, recursos, reglas de soberanía y jurisdicción) y propiedades virtuales, como se muestra en la tabla 1; estas últimas, con capacidad para dificultar el control gubernamental sobre las propiedades físicas. Bajo este concepto, pueden llevarse a cabo ataques de bajo costo desde el campo virtual o desde el ambiente de la información, y con ellos generar altos impactos y costos en el ambiente físico, debido a la estrecha relación entre los dos. Ahora bien, con el planteamiento de Nye (2010), lo opuesto también es cierto: el control sobre el ambiente físico puede tener efectos territoriales y extraterritoriales sobre el ambiente virtual.

Tabla 1. Objetivos del ciberpoder

	Dentro del ciberespacio	Fuera del ciberespacio
Instrumentos de información	• **Duro:** Ataques de denegación a servidores. • **Blando:** Establecer normas y estándares.	• **Duro:** Ataques a los sistemas de control de supervisión y adquisición de datos. • **Blando:** Campañas de diplomacia pública para influir en la opinión.
Instrumentos físicos	• **Duro:** Controles gubernamentales sobre empresas. • **Blando:** Infraestructura en apoyo a las actividades de derechos humanos.	• **Duro:** Bombardear enrutadores o cortar cables. • **Blando:** Protestas para nombrar o desprestigiar a proveedores cibernéticos.

Fuente: Nye (2010).

Por otro lado, el National Institute of Standards and Technology (2010) define el ciberespacio como "Un dominio global dentro del ambiente de la información que consiste en la red interdependiente de infraestructuras de sistemas de

información que incluyen Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados" (p. 2).

Kuehl (2012) define al *ciberpoder* como "La capacidad de utilizar el ciberespacio para crear ventajas e influir en eventos en todos los ambientes operacionales a través de los instrumentos de poder"[5] (p. 12). Según este autor, tal definición es más amplia que los enfoques de Mahan o Douhetian para el poder marítimo o aéreo, porque explícitamente hace referencia a otras formas de poder y está destinado a enfatizar el impacto sinérgico del poder cibernético y la integración de este con otras formas e instrumentos de poder.

Según Kuehl (2012), la tecnología es un factor obvio, porque la capacidad para *entrar* en el ciberespacio es lo que hace posible su uso. Esa tecnología cambia constantemente, y algunos usuarios países, sociedades, actores no estatales y similares pueden ser capaces de superar las viejas tecnologías para implementar y emplear unas nuevas, con una ventaja espectacular.

Entonces, como se puede apreciar, el elemento más vinculado al ciberpoder es la *información*. El poder en el ciberespacio es una dimensión del instrumento de la información, que para el caso del Ejército Nacional (EJC) se conoce como *comunicaciones estratégicas*. La información, bajo la sigla DIME (diplomacia, información, militar, económico), es uno de los varios enfoques actuales para instrumentos de poder, y podemos ver innumerables formas como el poder en el ciberespacio se vincula, apoya y habilita la creación y el ejercicio de las demás herramientas de poder.

Ahora bien, el poder en el ciberespacio juega un papel cada vez más vital en la fuerza económica. En el siglo XXI, la economía de un mundo globalizado e interconectado, el ciberespacio, es, quizás, el factor más importante que vincula a todos los actores locales, regionales y globales impulsando la productividad, abriendo nuevos mercados y permitiendo estructuras de gestión, que son, a la vez, más planas, pero con un alcance mucho más amplio.

Es que China es el país más dependiente de la economía digital y en ese campo el desarrollo es la perspectiva dominante, de ahí, la importancia del ciberespacio para el gigante asiático.

5 Los instrumentos de poder nacional se refieren a las herramientas que utiliza un país para influir en otros países u organizaciones internacionales, o incluso, en actores no estatales. Incluyen la diplomacia, la información, el poder militar y la economía (DIME). La Estrategia de Seguridad Nacional de Estados Unidos (en inglés, NSS, por las iniciales de National, Security Strategy) es un mandato del Congreso, y es el documento principal que establece cómo el presidente planea utilizar los instrumentos de poder para lograr los objetivos de seguridad nacional de Estados Unidos. https://www.thelightningpress.com/the-instruments-of-national-power/

Tal como lo argumenta Rosales (2020)

> […] las nuevas políticas impuestas por el gobierno de la república popular china es un llamado de Xi Jinping a convertir a China en una ciber-potencia, un desafío clave también para la transformación económica, pues el volumen de información que posee un país es el mejor indicador de su poder blando y su competitividad. En palabras del presidente chino citado por, tenemos que generalizar la infraestructura de internet, mejorar nuestra capacidad de innovación independiente, desarrollar la economía de la información y garantizar la seguridad informática. (pp. 246-247)

Desarrollo argumentativo

El plan de la cibergeopolítica de China para dominar el ciberespacio global

La teoría del poder del ciberespacio, planteada por Kuehl (2012), define al ciberpoder como "La capacidad de utilizar el ciberespacio para crear ventajas e influir en eventos en todos los ambientes operacionales a través de los instrumentos de poder" (p. 12). De igual forma, Nye (2010) afirma que el poder cibernético es un dominio con propiedades físicas (infraestructuras, recursos, reglas de soberanía y jurisdicción) y propiedades virtuales. Ahora, bien, ¿cómo China podría apelar a estas teorías para cumplir su sueño de ser la hegemonía global?

Según *The Epoch Times* (2021), una filtración de documentos del PCCh expuso el plan que tiene Beijing para controlar internet no solo en China, sino a escala global. Desde 2015, Xi Jinping, el líder chino, habría ordenado personalmente al régimen comunista del país que concentre sus esfuerzos en asegurar el control global de internet, como una de las líneas para desplazar el papel influyente de Estados Unidos en áreas clave como tecnología, inversiones y talento humano.

Para el mencionado diario, la visión de Beijing es usar la tecnología para gobernar internet. De esa forma, lograría controlar cada parte del ecosistema en línea, sobre las aplicaciones, el contenido, la calidad, el capital y la mano de obra. Esto iría de la mano del control y el manejo de la infraestructura, los protocolos y las políticas; es decir, China quiere expandirse en el dominio del ciberespacio, para que el PCCh controle todo el flujo digital del mundo. En caso de conseguirlo, podría someter al mundo a una censura global similar a la que existe en ese país.

Como lo explica Miliefsky (2021), lo primero que haría China en su estrategia por conquistar el ciberespacio sería *establecer las reglas* que gobiernan el sistema internacional del ciberespacio. En segundo lugar, instauraría agentes del PCCh

en puestos importantes en las organizaciones globales de internet. Por último, el régimen comunista aspiraría a controlar la infraestructura que subyace a internet, conocida como los *servidores raíz*. Estos servidores son instrumentos de *Big Data* que conectan a los usuarios con los sitios web que quieren visitar. Actualmente, como lo argumenta Miliefsky (2021), hay más de 1.300 servidores raíz en el mundo. De esos, apenas 20 están en China; Estados Unidos tiene aproximadamente diez veces más. Si el régimen chino ganara más control sobre servidores raíz, podría redirigir el tráfico a donde quisiera.

Es decir, si un usuario quisiera ir a un artículo de noticias sobre un tema que Beijing considera delicado, entonces el servidor DNS (por las iniciales en inglés de *Domain Name System*, o Sistema de Nombres de Dominio) del régimen podría dirigir al usuario a una página falsa que diga que el artículo ya no está en línea, o le brindaría información que no es relevante para el consultor. En palabras de Miliefsky (2021), "En el momento en que controlas la raíz, puedes falsificar o fingir cualquier cosa, puedes controlar lo que la gente ve y lo que la gente no ve" (p. 2).

¿Cómo China desarrollaría este plan bajo la teoría del poder del ciberespacio?

Como lo planteaba Nye (2010), el poder cibernético tiene unas dimensiones *físicas* (infraestructuras, recursos, reglas de soberanía y jurisdicción) y unas dimensiones *virtuales*. Bajo esa misma óptica, Pătrașcu (2019) apelando a los planteamientos de la Organización del Tratado del Atlántico Norte (OTAN), sostiene que el ciberespacio cuenta con tres niveles, descritos en la figura 2.

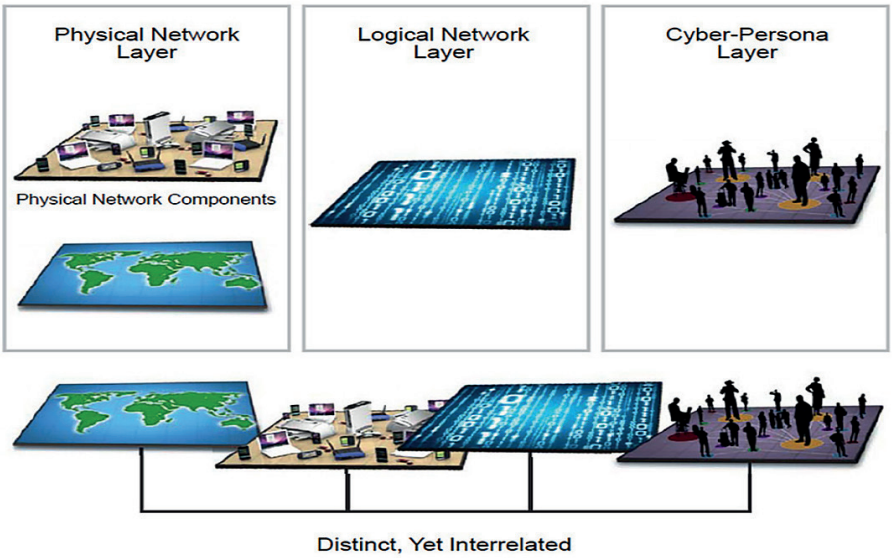
El primero de dichos niveles es el nivel *físico*, que proporciona la circulación de datos y consta de dos componentes: la *geografía* y la *red física*. La geografía la define como el espacio o el área física donde se alberga la infraestructura cibernética (suelo, agua, aire y espacio), mientras que la red física se compone de la *ciberinfraestructura*; es decir, elementos técnicos para la red física, que son una combinación de cableado, enlaces inalámbricos y satélites.

El segundo nivel es la *red*, o nivel *virtual*, en el que los dos componentes anteriores son vinculados de formas que extraen información y datos de la red física. Por ejemplo, el contenido de los sitios web alojados en servidores en múltiples áreas geográficas a las que se puede acceder con un solo localizador uniforme de recursos (en inglés, URL, por las iniciales de *Uniform Resource Locator*) o una sola dirección web.

El tercer nivel es conocido como interacción personal con la red, que representa un mayor nivel de abstracción de red y utiliza sus reglas para desarrollar una representación digital de la identidad de los individuos o las entidades en el ciberespacio. Este nivel consiste en la interacción de los usuarios de la red con una

o más identidades, y que puede ser visible y procesable. Estas identidades pueden incluir direcciones de correo electrónico, usuarios de redes sociales, protocolos de internet, números de teléfono móvil, contabilidad, etc.

Figura 2. Componentes del ciberespacio



Fuente: Pătrașcu (2019).

Bajo este planteamiento teórico, se procuró identificar la estrategia de China en cada una de esas dimensiones (física y virtual), con base en su política exterior. Esto buscará, a la luz de una estrategia geopolítica, interpretar cómo China pretende materializar sus intereses y su influencia a través del dominio ciberespacial, en su lucha por la hegemonía global contra Estados Unidos.

Estrategia en la dimensión virtual

En la dimensión virtual, el gobierno chino está llevando cabo varias tareas soportadas por su ya robusta economía, su diplomacia y su poderío tecnológico, donde se destaca que:

- El PCCh quiere rehacer una red muy similar a internet, a su propia imagen, semejanza y necesidades (Jennings, 2020), una red mundial unificada, donde los ciudadanos podrían verse obligados a conectarse a un mosaico de internet nacional regularizado por los estados; una idea conocida en China bajo el concepto de *soberanía cibernética*. Para esto, a través de sus empresas líderes en tecnología, como Huawei, China ha

planteado crear una red alternativa a internet, conocida como la New IP (por las iniciales de *Internet Protocol*, o protocolo de internet), la cual, según sus creadores, busca eliminar el internet tradicional, e incluir un modelo de gobernanza de *arriba hacia abajo*, en el cual los gobiernos tengan la capacidad para regular todo lo que circula en el ciberespacio. Para esto, cuenta ya con el apoyo de Rusia, Arabia Saudita e Irán. En palabras de Jennings (2020), "es la propuesta del sueño húmedo de un autoritario, que incluye la capacidad de censurar y autorizar conexiones de forma centralizada" (p. 1).

- Para la idea anterior, como lo explican Murgia y Gross (2020), China debe contar con el apoyo de la Unión Internacional de Telecomunicaciones (UIT), de la ONU, que establece estándares globales comunes para las tecnologías, y a la cual, el PCCh varias veces ha tratado de persuadir, con la idea de que el actual internet es una reliquia que ya llegó al límite de su destreza técnica. En sus inicios, la UIT supervisó las primeras redes telegráficas internacionales. Desde entonces, ha pasado de abarcar 40 naciones a 193, y se ha convertido en el organismo de normalización *de facto* para las redes de telecomunicaciones. Los estándares producidos allí legitiman las nuevas tecnologías y los nuevos sistemas a los ojos de ciertos gobiernos; particularmente, aquellos en el mundo en desarrollo que no participan en otros organismos de internet. Entendido esto, el PCCh ya le presentó a la UIT la New IP con la imagen de un mundo digital en 2030, donde la realidad virtual, los hologramas de tamaño natural, los carros autónomos y la cirugía remota son omnipresentes, y para lo que la red actual "no es apta". En esas reuniones, el gigante Huawei ha aseverado que es hora de una nueva red global con un diseño de arriba hacia abajo, donde los chinos deberían ser quienes la construyan.

- Otro elemento importante que viene desarrollando China en materia de la dimensión digital del ciberespacio, como lo plantea Griffiths (2015), es el *Gran Cortafuegos*, que Beijing comenzó a desarrollar desde 1990, para censurar el contenido de internet en el interior de la China continental. Este gran *Firewall* es la combinación de acciones legislativas y tecnologías aplicadas por el PCCh; su función es bloquear el acceso a sitios web extranjeros seleccionados y ralentizar el tráfico transfronterizo de internet. Ese efecto incluye limitar el acceso a fuentes de información extranjeras y bloquear herramientas de internet extranjeras. Palabras más palabras menos, China ya cuenta con dos décadas de experiencia para llevar a cabo actividades de censura en la China continental, lo que es una ventaja para llevarla a un plano mundial, o en su defecto, para patentar dichas prácticas en regímenes autoritarios.

Durante los últimos años, China ha realizado operaciones cibernéticas para obtener de manera ilegal datos, influir en los ciudadanos de países adversarios o sus aliados y afectar a las infraestructuras críticas. Para Lisa Institute (2019), China ha ido desarrollando una gran capacidad para configurar y modificar la información y los sistemas, y realizando ataques cibernéticos a Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda. Por otro lado, dichos ataques cibernéticos han sido empleados no solo para atacar infraestructura de adversarios chinos, sino también, como lo explica Andrade (2020), para el robo de propiedad intelectual sustituyendo la inversión en investigación y el desarrollo de las empresas respaldadas por Beijing, ataques de los cuales han sido objeto empresas estadounidenses como Apple y Tesla. Así mismo, la OTAN, la UE y la comunidad de inteligencia de Estados Unidos han señalado a China por sus constantes olas de ciberataques. En palabras de John Ratcliffe, director nacional de Inteligencia de Estados Unidos, citado por Earle (2020), "hubo interferencia extranjera en las elecciones presidenciales celebradas en noviembre de 2020" (p. 2), queriendo referirse al gigante asiático y sus capacidades en el ciberespacio.

- China entiende que el manejo del ciberespacio es sumamente complejo y, por ende, identifica riesgos en este, por lo cual restringió y penalizó las transferencias comerciales con criptomonedas, a fin de "limitar la fuga de capital, reducir la especulación financiera y evitar una volatilidad social" (Díez, 2021, p. 2).

Estrategia en la dimensión física

En la dimensión física, el gobierno chino está llevando a cabo varias tareas, entre las que se destacan:

- Por un lado, China busca tener el control de la infraestructura de internet, incluidos los servidores raíz (Thomas, 2021). Un servidor raíz es un servidor de nombres dentro de la zona raíz del DNS.

- Otro elemento dentro de la estrategia china en este ámbito, como se ha planteado en los últimos años (Triolo, 2020), es la *Ruta de la Seda Digital* (en inglés, DSR, por las iniciales de *Digital Silk Road*), introducida en 2015 por un libro blanco oficial del gobierno chino. Esta es un componente de la Iniciativa de la Franja y la Ruta de Beijing (en inglés, BRI, por las iniciales de Belt and Road Initiative). La DSR es concebida como una serie de proyectos o una marca de operaciones comerciales relacionadas con las telecomunicaciones, los datos o la venta de productos por parte de empresas de tecnología con sede en China, hacia África, Asia, Europa,

América Latina, el Caribe y el Reino Unido. Inicialmente se centró en inversiones en cables de fibra óptica y redes de telecomunicaciones.

- Con la DRS, una gran cantidad de actores tecnológicos chinos se expandieron en el ámbito mundial, con fines más económicos que geopolíticos, y que incluían: el comercio electrónico, los servicios en la nube y los gigantes de pagos Alibaba, Ant Financial, Tencent y JD.com, en el sudeste asiático y Europa. También participaban en redes sociales como Bytedance/Tiktok, en Asia y Estados Unidos; los desarrolladores de dispositivos inteligentes Transsion, Oppo, OnePlus y Xiaomi, en África y el sudeste asiático, y los fabricantes de drones DJI y XAG en los EE. UU., en Asia, el sudeste asiático y América Latina.

- Huawei tiene 91 contratos para proporcionar equipos de telecomunicaciones inalámbricas 5G en todo el mundo, incluidos 47 de Europa, a pesar de las advertencias de Estados Unidos de que la participación de Huawei equivalía a dar a los chinos acceso a secretos de seguridad nacional —una acusación rechazada por la compañía asiática—.

- Por otro lado, el informe de 2021 sobre Inversión Extranjera Directa (IED) en América Latina y el Caribe, de la Comisión Económica para América Latina y el Caribe (CEPAL) (Zaiat, 2021), da cuenta de que los proyectos realizados desde 2013 en todo el mundo en el marco de la DSR han representado más de 17.000 millones de dólares, con más de 10.000 millones de dólares invertidos en comercio electrónico y pagos digitales, y más de 7.000 millones de dólares destinados a préstamos e IED en infraestructura de redes de telecomunicaciones y cables de fibra óptica.

- Actualmente, China está desarrollando la tecnología 5G, una red de ancho de banda mucho mayor en comparación con las 4G, que servirá como la columna vertebral digital para un mundo más automatizado. En torno a esta tecnología, actualmente se lleva a cabo una disputa entre cuatro empresas que dominan el mercado de las tecnologías de redes básicas necesarias para las redes 5G (González, 2019); dos de ellas son europeas/occidentales (Ericsson y Nokia), y dos, chinas (Huawei y Hisilicon). Lo que es claro es que las 5G constituirá una base tecnológica capaz de realizar una rápida innovación en la constitución de la cadena de suministros, y segura tanto para el espionaje como para el boicot de infraestructuras críticas. A su vez, el liderazgo 5G proporcionará una base de innovaciones tecnológicas que impulsarán la capacidad militar y el crecimiento económico.

- No pueden dejarse de lado todos los proyectos de infraestructura que lleva a cabo China en todo el mundo; sobre todo, en Latinoamérica (BBC, 2019). Ejemplo de ello son Panamá, Ecuador, Venezuela, Chile, Uruguay, Bolivia, Costa Rica, Cuba y Perú; todos estos, acompañados por componentes tecnológicos chinos como cámaras de seguridad, escáneres de aeropuertos como HikVision y NucTech, redes inalámbricas, fibra óptica, cables submarinos, etc.

Análisis del geociberpoder de China

Tomando como base la teoría del poder cibernético de Nye (2010), a continuación, en la tabla 2 se explican las dimensiones físicas y virtuales, resaltando el poder de las tareas desarrolladas por China camino a su hegemonía global. Se aplica la teoría de Nye para hacer una aproximación a la estrategia geopolítica de China.

Tabla 2. Objetivos del ciberpoder de China

	Dentro del ciberespacio	Fuera del ciberespacio
Instrumentos de información	• **Duro:** Realiza ataques de denegación a servidores de Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda. • **Blando:** Busca establecer normas y estándares en la UIT, para implementar la New IP y reemplazar la actual red.	• **Duro:** Recopila información de la infraestructura crítica más sensible a escala mundial, para mantenerla en el objetivo de ataques físicos. • **Blando:** Vende la tecnología 5G como la mejor opción para el futuro en temas como IOT, *Machine Learning* y *Big Data*, provistas por China.
Instrumentos físicos	• **Duro:** Realiza controles gubernamentales llevados a cabo a escala local en China. • **Blando:** Proporcionó tecnología a varios países para apoyarlos durante la crisis de la pandemia por el SARS-CoV-2.	• **Blando:** » Busca desprestigiar la clásica red de internet. » Construye infraestructura a nivel global tanto de vía de comunicaciones como de telecomunicaciones, con la cual desarrolla su geociberpolítica. » Implementa la DRS a través de empresas de tecnología a escala global, como Huawei y ZTE, que tienen inundado el mercado global con dispositivos celulares.

Fuente: elaboración propia.

Se puede observar que las actividades desarrolladas por China en el ciberespacio durante la última década develan, a la luz de la teoría del poder planteado por Kuehl (2012), "La capacidad de utilizar el ciberespacio para crear ventajas e influir en eventos en todos los ambientes operacionales a través de los instrumentos de poder" (p. 12). Una estrategia o una línea de acción con la que, sin duda, como ya mencionamos, busca desplazar a Estados Unidos de ese liderazgo mundial económico, al igual que de ámbitos, como el militar, el cultural, el ambiental, el espacial y, desde luego, el ciberespacial, donde tendrá una gran ventaja si materializa sus planes.

Consideraciones e implicaciones en la escena mundial

Gobiernos como los de Rusia, Irán y Arabia Saudita están de acuerdo, respecto a la idea de China de crear una nueva internet que apalanque su poder en el ciberespacio y cambie el modelo actual de gobernanza de internet; esencialmente, la autorregulación sin ley por parte de empresas privadas, en su mayoría estadounidenses. Ello, a causa de que existen gobiernos, ya sean democráticos o autoritarios, que, cansados de ser excluidos de la influencia en el ciberespacio, están haciendo campaña para obtener más influencia en la web.

> En este mismo sentido, el líder del equipo de investigación de Huawei, Sheng Jiang, argumentó a la UIT en una reunión llevada a cabo el pasado mes de septiembre de 2021 donde asistieron representantes gubernamentales del Reino Unido, Estados Unidos, Países Bajos, Rusia, Irán, Arabia Saudita y China, que "el sistema (la IP) ya está siendo construido por ingenieros de la industria tecnológica y la academia en varios países. (*Financial Times*, 2020, p. 3)

En este orden de ideas, si la nueva IP fuera legitimada por la UIT, los operadores estatales podrían optar por implementar un internet occidental o uno chino. Así las cosas, se contaría con dos versiones de internet: una versión capitalista, dirigida por el mercado y basada en la vigilancia, que es explotadora; y una versión autoritaria, también basada en la vigilancia, según Zuboff (2019). Ahora habría que esperar si Europa y América del Norte se unirán a fin de construir los marcos legales y tecnológicos para una alternativa democrática.

Si fuese el caso adquirir la nueva red china por parte de diferentes Estados, necesitarían permiso de su proveedor de internet para hacer cualquier cosa a través de internet. Dichos permisos irían desde descargar una aplicación hasta acceder a un sitio, y los administradores podrían tener el poder para denegar el acceso.

Hechos ocurridos en China en el último año, así como en Irán y Arabia Saudita, dan pistas de cómo se vería esta idea al implementar esta nueva red en otros países. Los gobiernos en mención bloquearon la conectividad global a internet durante períodos prolongados, en el marco de disturbios civiles, y permitiendo solo el acceso restringido a servicios esenciales como la banca o la atención

médica. Otro ejemplo es Rusia, que implementó una nueva ley de *internet soberano*, aprobada en noviembre pasado, y consagra el derecho del gobierno a monitorear de cerca el tráfico web; además, mostró la capacidad del país para separarse de la web global; una capacidad que las empresas chinas, incluida Huawei, ayudaron a construir a los rusos.

En contraposición, Fältström, citado por Murgia y Gross (2020), afirmó que la belleza de internet es su naturaleza *sin permiso*, demostrada durante la Primavera Árabe. Para este ingeniero, quien es conocido como uno de los padres de internet en Suecia, debe existir un equilibrio entre poder comunicarse y controlar, donde las personas que tienen voz son siempre más importantes.

No obstante lo anterior, como afirma Fältström, el internet de hoy no tiene un regulador, y su poder está, en gran parte, en manos de un puñado de corporaciones estadounidenses, como Apple, Google, Amazon y Facebook. Ahora bien, Estados Unidos, Reino Unido y Europa se han interesado en adaptar el sistema actual para introducir más poder regulatorio y dar a las agencias de inteligencia mayor acceso a los datos personales de los usuarios.

Ante esto, muchos expertos temen que con la Nueva IP, los proveedores de servicios de internet —generalmente, de propiedad estatal— tengan el control y la supervisión de todos los dispositivos conectados a la red y puedan monitorear y bloquear el acceso individual, con el modelo que plantea China.

Lo cierto es que, según dice Niels ten Oever, un exdelegado holandés en la UIT,

> […] la internet era concebida como una infraestructura neutral, pero se ha convertido en un brazo de control politizado. Cada vez más, la Internet se utiliza para objetivos políticos, para reprimir a las personas económica y físicamente, se observó en Cachemira, Myanmar y en las revelaciones de Snowden. (*Financial Times*, 2020, p. 3)

Conclusiones

Como se pudo observar, el poder cibernético es un dominio con propiedades físicas (infraestructuras, recursos, reglas de soberanía y jurisdicción) y propiedades virtuales; en este se evidencia una serie de actividades por parte del PCCh para influir en el ciberespacio tanto en la dimensión física como en la virtual. Así las cosas, el gobierno de Beijing comprende que puede y debe aprovechar sus propias capacidades en el ciberespacio para crear ventajas e influir en eventos en todos los ambientes operacionales a través de este, como instrumento de poder.

Ahora bien, lo que podemos observar es que, de una u otra forma, China tiene claro cómo emplear el ciberespacio para sus intereses como nación, y con base en eso, desarrolla una estrategia en dicho ámbito, la cual le generará la superioridad necesaria en su camino al sueño chino de ser el líder económico en el siglo XXI. Así las cosas, la administración de Xi Jinping ha visto en el diseño de la infraestructura y los estándares de internet mundial un elemento central de su política exterior digital, con el propósito de ejercer una hegemonía global mediante el ciberespacio.

Dentro de la estrategia de China en la dimensión virtual se puede destacar que la New IP (propuesta que no se trata de una necesidad real de nueva tecnología, sino de intentar alterar la estructura de gobierno de internet) es un esfuerzo del gigante asiático y su conglomerado de empresas para cambiar la forma como se utiliza la internet, apoyados por gobiernos que quedaron en gran parte excluidos cuando esta se fundó, en la segunda mitad del siglo XX. Entonces, los conflictos que se desarrollen para controlar el ciberespacio —y en especial, internet— podrán ser los nuevos espacios donde el poder político y el económico se desplieguen durante el siglo XXI. En consideración a ello, Beijing está buscado tener influencia en muchas organizaciones que regulan y estandarizan el área de la tecnología en el mundo entero, como es el caso de la UIT en los últimos dos o tres años, a fin de lograr incorporar esta red alterna a internet.

En esos términos, si bien dicho proyecto posibilitaría generar una red global mejorada, el precio podría ser la libertad. Lo anterior, considerando que el régimen chino ha demostrado que puede controlar y vigilar intensamente su internet nacional para evitar que se lo use como una herramienta para cohesionar la población y movilizarla en contra del gobierno; es decir, combinado con el éxito económico de sus empresas, China ha hecho que esta visión sea increíblemente atractiva para los regímenes autocráticos en el mundo.

Ahora bien, desde la perspectiva de la dimensión física, Estados Unidos y otras naciones han cometido un error estratégico al no visualizar el valor de la infraestructura como un activo en el crecimiento y el desarrollo de mercados, conforme lo ha hecho Beijing. En tal sentido, dentro de la estrategia de China en la dimensión física se puede afirmar que el PCCh viene desarrollando una gran cantidad de proyectos de infraestructura en varios países del mundo, con los que el gobierno de Xi Jinping tiene una serie de acuerdos y entendimientos. Es decir, China sabe que se debe construir mucha infraestructura para la materialización de la *Nueva Ruta de la Seda*, que la apalancará como hegemonía económica mundial; y por eso, en los últimos diez años han sido sus empresas las que han proporcionado infraestructura en temas de vías y telecomunicaciones; particularmente, en África y, en cierta medida, América Latina.

Dicho de otra manera, China quiere una infraestructura tecnológica que le dé el control absoluto que ha logrado políticamente, y un diseño que coincida con su impulso totalitario, que no solo la lleve a ejercer la hegemonía mundial, sino que, además, ayude a facilitar el dominio de la población en general, elemento que debe preocupar a analistas internacionales en los nuevos escenarios geoestratégicos.

Para finalizar, se logra inferir cómo China desarrolla una estrategia para controlar el ciberespacio no solo desde la dimensión virtual, sino a partir de la dimensión física, a través del desarrollo de infraestructura a escala mundial, en el marco de la iniciativa de la BRI, o *Nueva Ruta de la Seda*. Esto refuerza la intensión de Beijing de dominar el ciberespacio y la tecnología dentro de una de las líneas de acción de esta nación, con el objeto de restarle protagonismo a Estados Unidos en el sistema internacional y cambiar el *statu quo* donde el gigante asiático tendrá un rol más influyente.

Referencias

Andrade, H. (2020, 25 de noviembre). Así fue cómo China robó inventos a Apple y a Tesla. *Primer Informe*. https://primerinforme.com/actualidad/asi-fue-como-china-robo-inventos-a-apple-y-a-tesla/

BBC. (2019, 26 de abril). Los países de América Latina que forman parte de la Nueva Ruta de la Seda de China. https://www.bbc.com/mundo/noticias-america-latina-48071584

Díez, P. M. (2021, 24 de septiembre). Banco de China prohíbe las criptomonedas. *ABC Economía*. https://www.abc.es/economia/abci-china-prohibe-criptomonedas-para-evitar-volatilidad-y-fugas-capital-202109241756_noticia.html

Douhet, G. (1987). *El dominio del aire*. Instituto de Historia y Cultura Aeronáutica. (Obra original publicada en 1921)

Earle, G. (2020, 17 de diciembre). *Trump's director of national intelligence John Ratcliffe DELAYS report on foreign interference in election and 'battles analysts to beef up its criticism of China*'. https://www.dailymail.co.uk/news/article-9061707/Trump-loyalist-intel-director-John-Ratcliffe-holding-report-election-interference.html

Financial Times. (2020, 30 de marzo). Financial Times: Dentro de la controvertida misión de China para reinventar internet. https://infotalqual.net/financial-times-dentro-de-la-controvertida-mision-de-china-para-reinventar-internet

Fuerzas Militares de Colombia. (2018). *Manual Fundamental Conjunto MFC 1.0 Doctrina Conjunta*. Escuela Superior de Guerra.

González., A. (2019, 13 de agosto). *Análisis de la guerra del 5G: EEUU vs China*. Lisa Institute. https://www.lisainstitute.com/blogs/blog/guerra-5g-eeuu-china

González,R.(2020).Chinatieneunplanparahacerseconlahegemoníaglobal.*ElConfidencial*. https://blogs.elconfidencial.com/mundo/tribuna-internacional/2020-05-08/china-plan-hacerse-hegemonia-global-coronavirus_2583087/

Griffiths, J. (2015, 26 de octubre). La expansión del Gran Cortafuegos: así es como China libra su guerra en Internet. *CNN en Español*. https://cnnespanol.cnn.com/2015/10/26/la-expansion-del-gran-cortafuegos-asi-es-como-china-libra-su-guerra-en-internet/

Jennings, R. (2020, 24 de abril). China wants to control all the internet with 'New IP' plan. *Security Boulevard*. https://securityboulevard.com/2020/04/china-wants-to-control-all-the-internet-with-new-ip-plan/

Kissinger, H. (2014). *World order*. The Penguin Press.

Kuehl, D. T. (2012). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security.* http://connections-qj.org/article/cyberspace-cyberpower-defining-problem

Lisa Institute. (2019). *Análisis internacional de Amenazas desde la perspectiva de EE. UU. 2019-2020*. LISA Institute.

Mackinder, H. J. (2010). El pivote geográfico de la historia. Geopolítica(s). *Revista de Estudios sobre Espacio y Poder, 1*(2), 301-319. https://revistas.ucm.es/index.php/GEOP/article/view/36331

Mahan, A. T. (2013). Análisis de los elementos del poder naval. Geopolítica(s). *Revista de Estudios sobre Espacio y Poder, 4*(2), 305-334.

Miliefsky, G. (2021, 2 de mayo). *Gary Miliefsky*. https://primerinforme.com/reportaje/china-tiene-un-plan-para-controlar-internet-en-el-mundo-y-lo-esta-aplicando/

Murgia, M., & Gross, A. (2020, 27 de marzo). *Inside China's controversial mission to reinvent the internet*. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

National Institute of Standards and Technology. (2010, 24 de june). *Cyberspace*. https://acqnotes.com/acqnote/careerfields/cyberspace

Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Pătrașcu, P. (2019). Missions and actions specific to cyberspace operations. *International Conference Knowledge-Based Organization, 25*(3), 51-56. doi:10.2478/kbo-2019-0117

Rosales, O. (2020). *El sueño chino Cómo se ve China a sí misma y cómo nos equivocamos los occidentales al interpretarla*. Grupo Editorial Siglo XXI.

Stevens, T., & Betz, D. (2011). Chapter One: Power and cyberspace. *Adelphi Series, 51*(424), 35-54, doi: 10.1080/19445571.2011.636954.

The Epoch Times. (2021, 6 de mayo). Chinese Leader Xi Jinping lays out plan to control global internet: Leaked documents. https://www.theepochtimes.com/mkt_app/chinese-leader-xi-jinping-lays-out-plan-to-control-the-global-internet-leaked-documents_3791944.html

Thomas, G. (2021, 3 de mayo). *Leaked documents reveal Xi Jinping's Communist Chinese plan to control the internet's root*. https://circleid.com/posts/20210503-leaked-documents-reveal-chinas-plan-to-control-internet-root/

Triolo, R. G. (2020, 8 de mayo). Will China control the global internet via its digital silk road? https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Zaiat, A. (2021, 31 de agosto). *China extiende la Ruta de la Seda Digital a América Latina en las narices de EEUU*. https://mundo.sputniknews.com/20210831/china-extiende-la-ruta-de-la-seda-digital-a-america-latina-en-las-narices-de-eeuu-1115623685.html

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.