ROI | 2025 Núm. 1 e54

El ciberespacio desde la perspectiva china: análisis estratégico y operacional

Cyberspace from a Chinese perspective: strategic and operational analysis

Francisco Javier Montilla Aguilera
Universidad de Granada, Andalucía, España

Recibido: 02/08/2024 · Aceptado: 13/12/2024

Resumen
En este artículo realizamos un análisis sobre la estrategia general de China en el ciberespacio en el siglo XXI, y a través de sus principales actividades operativas para alcanzar sus objetivos en este aspecto. Nuestro principal objetivo es definir las líneas maestras de la ciberestrategia china en el ámbito de la seguridad internacional. Irá acompañado de otros objetivos específicos que son identificar los pilares teóricos de la ciberestrategia china, identificar las principales acciones cibernéticas de China en la última década, y reflejar los puntos de conexión entre la ciberestrategia china y su política exterior. El método que utilizamos es básicamente una revisión especializada de la literatura y la prensa. Al final concluimos que la concepción china del ciberespacio difiere radicalmente de la perspectiva occidental basada en valores, y que intentan controlar la red creando su propio sistema, al tiempo que tratan de utilizar el ciberespacio para perjudicar a sus enemigos mediante operaciones en la zona gris del conflicto. De este modo pueden atraer a otros países que están en contra del sistema dominado por Estados Unidos, una línea seguida en casi todas las actuaciones de política exterior que llevan a cabo.

Palabras clave
China, ciberespacio, ciberestrategia, zona gris.

Abstract
In this article we conduct an analysis on China's overall strategy in cyberspace in the 21st century, and through its main operational activities to achieve its objectives in this regard. Our main objective is to define the outlines of China's cyber strategy in the field of international security. It will be accompanied by other specific objectives which are to identify the theoretical pillars of Chinese cyber strategy, to identify China's main cyber actions in the last decade, and to reflect the points of connection between Chinese cyber strategy and its foreign policy. The method we used is basically a specialized literature and press review. In the end we conclude that the Chinese conception of cyberspace differs radically from the Western value-based perspective, and that they try to control the network by creating their own system, while trying to use cyberspace to harm their enemies through operations in the gray zone of conflict. In this way they can attract other countries that are against the U.S.-dominated system, a line followed in almost every foreign policy action they take.

Keywords
China, cyberspace, cyberstrategy, grey zone.

Cómo citar: Montilla Aguilera, F. J. (2025). El ciberespacio desde la perspectiva china: análisis estratégico y operacional. *Orden Internacional, Revista de Estudios Internacionales, 1*, e54. https://doi.org/10.33732/roi.54

Introducción

La etapa final del siglo XX y los comienzos del siglo XXI se han constituido como el escenario de la revolución tecnológica, la cual reviste una importancia tal que determinados autores sitúan a la era de la información al nivel de la revolución industrial o la agrícola. Los avances tecnológicos han cambiado nuestra forma de relacionarnos entre nosotros y con el propio mundo. El espacio cibernético se ha convertido en un lugar más donde desarrollar nuestras actividades cotidianas, lo cual no ha pasado desapercibido para los Estados y los actores internacionales. Desde un punto de vista militar, el espacio cibernético es un nuevo dominio de la guerra que ofrece multitud de posibilidades para conseguir o favorecer determinados intereses estratégicos.

Los desarrollos tecnológicos más importantes tradicionalmente han tenido su origen en EEUU, potencia hegemónica a nivel global durante tantos años, y la potencia que más ha cultivado la aplicación del uso militar del ciberespacio. Sin embargo, en el dominio cibernético el resto de potencias que hoy son rivales de los estadounidenses se han puesto al día y ya países como China o Rusia han adquirido conciencia de su importancia y lo usan a su favor. Nuestro objeto de análisis va a ser el caso chino, quienes perciben en el ciberespacio una forma tanto de protección como ataque a potenciales rivales. Para ello el gigante asiático se ha dotado de una estrategia peculiar en el dominio cibernético, muy distinta a la del resto de sus grandes competidores.

La pregunta de investigación sobre la que va a girar este artículo es fundamentalmente cómo China ha usado el ciberespacio de cara a favorecer la consecución de sus principales intereses estratégicos, y para ello el objetivo principal va a ser definir las principales líneas de la ciberestrategia de China en el ámbito de la seguridad internacional. Para esclarecer este objetivo nos planteamos a su vez los siguientes objetivos específicos:

- Identificar los pilares teóricos de la estrategia cibernética china.
- Señalar cuáles han sido las principales acciones cibernéticas de China en la última década.
- Reflejar los puntos de conexión entre la estrategia ciber de China con su política exterior.

Desde el punto de vista metodológico nuestra investigación va a consistir en una revisión de la literatura académica y especializada, así como también nos serviremos de la prensa y noticias recientes, al tratarse de una cuestión de completa actualidad. Trataremos de seguir un enfoque en el que principalmente vamos a identificar las principales líneas de acción de China en el ciberespacio a nivel interno y externo, así como las repercusiones que puede tener de cara a la seguridad internacional y al

equilibrio de poder del sistema durante las décadas venideras. Nuestra investigación va a seguir un esquema inductivo, ya que vamos a partir de conceptos generales para posteriormente analizar aquellos aspectos concretos de la actividad ciberespacial china. Para ello en primer lugar es importante disponer de una noción general del concepto de zona gris, ya que es el poso teórico fundamental para entender la importancia de las operaciones cibernéticas hostiles, así como la concepción que China tiene del ciberespacio, la cual difiere de la concepción occidental. También trataremos las líneas generales de la política exterior del país especialmente desde la llegada al poder de Xi Jinping, actual líder chino. Tras ello pasaremos al análisis de la cuestión para dar respuesta a la pregunta con la que iniciamos el artículo, y para ello vamos a realizar un análisis general de la estrategia cibernética china, así como el análisis de determinadas actuaciones tras las que se encuentra el gigante asiático, generalmente no de forma pública.

Aproximación teórica a la actuación china en el ciberespacio

Operaciones en la zona gris y guerra irrestricta

La naturaleza de los conflictos y de las relaciones entre Estados ha cambiado de forma notable desde el final de la Guerra Fría, aunque ya desde la segunda mitad del siglo XX. Rara vez encontramos conflictos convencionales a día de hoy (aunque los sigue habiendo, como el caso de la guerra ruso-ucraniana), haciendo un uso de la fuerza militar de forma directa. En cambio, en los últimos años la literatura especializada en conflictos y seguridad ha venido usando el concepto de "guerra híbrida" para referirse a aquellas acciones que realiza un Estado integrando los medios convencionales y otros medios no convencionales para explotar las debilidades de las fuerzas enemigas.

Este concepto cuenta con otros antecedentes, como guerra asimétrica, guerra compuesta o guerra complejo-irregular, que vienen a expresar una idea similar, pero los cuales fueron desechados por la academia fruto de la complejidad y heterogeneidad de los mismos (Colom, 2012). Tras ello, será Hoffmann quien, tras la Guerra de Verano de 2006 entre Israel y Hezbollah cuando el concepto de guerra híbrida se populariza, gracias al análisis de Hoffmann de multitud de experiencias históricas. De esta forma, el concepto de guerra híbrida "se caracteriza por la plena integración en tiempo y espacio de procedimientos típicamente convencionales con tácticas propias de la guerra irregular" (en Colom, 2012).

Como ocurre con la gran parte de conceptos o términos que adquieren gran popularidad y se ponen de moda, se corre el riesgo de que acabe convirtiéndose en una *buzzword* y que se acabe utilizando para designar cualquier fenómeno, haciendo que pierda su esencia inicial. Para evitar esto, en los últimos años se ha venido desarrollando el concepto de "conflicto en la zona gris". Para conceptualizar este concepto nos serviremos del artículo de Jordán (2018) *"El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo"*.

Para entender el concepto de zona gris en las relaciones entre dos Estados es importante tener en cuenta que la zona negra sería el conflicto convencional (guerra abierta) y la zona blanca sería la ausencia de conflicto (paz). Sabiendo esto, la zona

gris se configura como ese espacio en la relación entre dos actores en la cual no hay conflicto abierto, pero la relación tampoco es pacífica al completo. Siguiendo a Jordán, los conflictos en la zona gris incluyen varios elementos definitorios que los caracterizan, como son la **ambigüedad** (ya que no existe ni conflicto abierto ni tampoco paz, por lo que el criterio para diferenciar las acciones de unas propias de la guerra de otras propias de la política con buena fe va a ser complejo y sometido a criterio subjetivo), **las estrategias multidimensionales** (lo cual nos recuera a la guerra híbrida, ya que la zona gris es el espacio en el que esta se desarrolla por excelencia, y hace referencia al uso de medios muy diversos y distintos a los convencionales con intención coercitiva), la existencia de **intereses sustanciales en juego** (la zona gris entrará en juego cuando los beneficios esperados de abandonar la vía diplomática tradicional, y especialmente para aquellos Estados con menor poder relativo que en un conflicto convencional verían reducidas sus posibilidades de triunfar) y el **gradualismo** (las acciones se van desarrollando de forma paulatina que permite una adaptación táctica para evitar la respuesta del rival).

Es importante diferenciar y dejar claro que la zona gris se trata de un tipo de conflicto, siempre por debajo del umbral de la guerra y marcado por la ausencia de paz entre dos Estados. En ese conflicto se pueden usar estrategias híbridas, las cuales también se pueden usar en un conflicto que sea una guerra abierta. Por ello decimos que las estrategias pueden ser híbridas o convencionales, mientras que la zona gris es el tipo de conflicto.

Para analizar el nivel estratégico y operacional de la acción cibernética china es importante conocer los fundamentos teóricos básicos del conflicto en la zona gris, en el sentido de que las acciones que China realiza en ese ámbito, fundamentalmente aquellas que revisten un carácter ofensivo contra rivales, son realizadas en el ámbito de la zona gris. Resulta importante señalar también que la realización de estas acciones que se encuadran en la zona gris de los conflictos se ven favorecidas por el hecho de que China sea un estado iliberal en el que la rendición de cuentas y el proceso de toma de decisión no es tan riguroso ni está sometido a unas reglas tan rígidas como en las democracias liberales tradicionales.

Debemos tener en cuenta que la conceptualización del conflicto en la zona gris tiene su origen en la academia Occidental, lo cual no ha pasado desapercibido para los intelectuales chinos. Los teóricos del país proponen su propio concepto para explicar este fenómeno, y la acción de China tanto en el ciberespacio como a nivel internacional: la guerra irrestricta (UW). Es uno de los conceptos popularizados en las últimas décadas para hacer alusión a los diferentes tipos de estrategias que se pueden utilizar en un conflicto. Se entiende como una "guerra combinada que trasciende las principales áreas y métodos de los asuntos militares y no militares, donde se deben incluir todas las dimensiones que ejercen influencia sobre la seguridad nacional y donde se persigue un objetivo político por medio del ejercicio de la violencia en un sentido amplio" (de Pablo López, 2015). En suma, se trata de un concepto muy similar al de guerra híbrida, ya que apenas la única diferencia entre ambas que se plantea es el factor temporal, ya que se argumenta que la guerra irrestricta tiene una consideración secuencial (todas las acciones multidimensionales se realizan de forma ordenada de

forma que se obtenga el resultado esperado), mientras que las acciones híbridas se pueden realizar de forma simultánea.

La principal crítica a este concepto radica en su ambigüedad, así como se critica al concepto de guerra híbrida por el mismo motivo, ya que no especifica si las acciones que engloba se diferencian entre un conflicto en el espacio de guerra o en el espacio de zona gris. El principal punto de interés del concepto es que nos ofrece una visión propia de la academia china para entender la forma de proceder del Estado a nivel internacional, ya que el concepto fue inicialmente propuesto por los coroneles del ELP, Qiao Liang y Wang Xiangsui, en su obra *"Unrestricted Warfare – Thoughts on War and Strategy in a Global Era"* (1999), donde establecen la idea de la desaparición de los límites del campo de batalla, pudiendo serlo espacios naturales, pero además la política, el militar, lo económico, la cultural y la psique. Señalan además que el espacio tecnológico que une a los dos ámbitos es cada vez más importante, y el valor de perseguir objetivos reales de manera secuencial. A pesar de ello, numerosos autores han encuadrado las acciones chinas en el ciberespacio como una parte de la guerra irrestricta que el país lleva a cabo contra sus potenciales enemigos en el camino por la hegemonía mundial, y han analizado dichas acciones desde ese prisma. En esta investigación haremos alusión a dichas acciones como de guerra irrestricta, pero siempre teniendo en cuenta que se trata de estrategias que se llevan a cabo en una relación entre dos estados que se rigen por el conflicto en la zona gris, un término mucho más preciso y más aceptado por la academia en general.

El ciberespacio para China

Una vez que hemos encuadrado las acciones ciberespaciales de China en el espacio de la zona gris de los conflictos, resulta necesario a su vez entender la concepción que se tiene del ciberespacio en el gigante asiático, ya que difiere en gran parte de la propia de los Estados occidentales.

La cultura de una comunidad impregna la forma de entender y de concebir el mundo y los elementos que lo integran (Yaqing, 2012). Las condiciones culturales, históricas y económicas tienen un gran impacto a nivel de la doctrina militar de cada ejército, la cual afecta en gran medida a la concepción del ciberespacio. En este sentido, la cultura en general y la doctrina militar en específico de China se ven marcadas por el llamado siglo de humillación, cuando se vio sometida al dominio colonial de potencias como Japón o Rusia, entre otras. Este momento realmente es un punto de inflexión para lo que posteriormente se ha convertido China, ya que el giro en política exterior que ha promovido Xi Jinping desde su llegada al poder se ha visto motivada por los fantasmas de ese pasado colonial, así como por reclamar el lugar como potencia mundial que consideran que les corresponde por su potencia económica (Sierra y Marrades, 2022).

Uno de los elementos que China consideró hace dos décadas que iban a servir para promover ese impulso de su posición mundial serían los avances tecnológicos. Bajo la dirección de Jiang Zemin, en el Décimo Plan Quinquenal (2001-2005) en el que se establece "como prioridad nacional la promoción del sector tecnológico de la información, el aumento de la accesibilidad a la red y la promoción del uso de las tecnologías digitales" (Austin, en Expósito, 2024a). El principal interés de

China en potenciar su producción y capacidad tecnológica radicaba en el potencial desestabilizador de las nuevas tecnologías, así como en el hecho de la dependencia tecnológica de EEUU en ese momento. En este sentido se constituye en una especie de protección y de emancipación al mismo tiempo.

A lo largo de este artículo hemos estado hablando de ciberespacio continuamente, ya que desde la perspectiva Occidental este se constituye como el quinto dominio de la guerra (tierra, aire, mar, espacio y ciberespacio), siendo concebido por autores como Kuehl (en Recalde, 2016) como "un ámbito operativo cuyo carácter distintivo es el uso de la electrónica y espectro electromagnético para almacenar información a través de las TIC y basados en sistemas de infraestructuras conectadas", o Rattray como un espacio artificial para la gestión de la información constituido por una serie de infraestructuras variadas.

Pero desde la concepción china esta interpretación difiere. Como señala Expósito (2024b), la doctrina china entiende el ciberespacio como una interacción del discurso doctrinal chino de dos ámbitos distintos, como son el espacio electromagnético y el ámbito de la informatización (*xinxihua*). El primero de ellos se entiende vinculado con el hardware en sí mismo considerado y con los sistemas que tienen aplicación en la guerra electrónica y la explotación del espacio electromagnético, mientras que la informatización se constituye como un sistema integral de sistemas, y la utilización de la tecnología de la información desde un punto de vista amplio. Así, la concepción china entiende por dominio de la información el dominio del espectro electromagnético (la red de computadoras) y al dominio de la informatización (Cheng, en Expósito, 2024b).

Colom (2020) nos señala un enfoque similar. Para la perspectiva china la información se constituye como un elemento clave tanto para la protección del espacio nacional como para la proyección exterior del poder, donde las estrategias informativas multidimensionales, que analizaremos posteriormente de forma detenida. Esto se debe fundamentalmente a que, en la era de la información, los líderes chinos conciben que el auge y caída de las potencias está fundamentalmente determinado por su capacidad para generar y manejar la información.

Teniendo esto en mente, a continuación, vamos a analizar cómo se configura la acción china en el especio ciber, tanto a nivel estratégico general como a nivel de operaciones, y trataremos de ponerlo en conexión con su estrategia de política exterior general. Nos basaremos fundamentalmente en una revisión de la literatura especializada y de la prensa de cara a poder interpretar y dar un sentido de conjunto a la acción del gigante asiático en este aspecto, que se configura como uno de los pilares de su ascenso a nivel político.

China en el ciberespacio: análisis estratégico y operacional

Análisis estratégico

La concepción desde el polo chino de la tecnología como factor clave en el auge del país ha venido prácticamente de la mano con el giro asertivo en su política exterior. Esto es importante ya que el desarrollo tecnológico del país ha sido una pieza central

en sus operaciones de política exterior, de defensa y de legitimación exterior, así como también en su desarrollo económico.

El desarrollo tecnológico del país y su giro en clave exterior encuentran su base en la misma motivación: la necesidad de salir de la irrelevancia internacional y dejar atrás los fantasmas del siglo de la humillación (Rodríguez, 2016). Las élites chinas tienen en mente que el estado natural del país se encuentra en el centro del sistema *Tianxia* (todo bajo el cielo), conceptualizado por Zhao Tingyang (2021), que ofrece refleja una organización internacional en el que China se constituye como el imperio del centro a través de una relación similar a la del vasallaje con el resto de estados satélites. Desde la llegada de Xi Jinping al poder en 2012, el uso de expresiones como "ciber-superpotencia", "hacer de China una potencia nacional en el ciberespacio" y los conceptos estratégicos asociados a ellas han sido bastante recurrentes en discursos importantes e iniciativas del Gobierno chino (Kania et al, 2017).

Con este objetivo en mente, el gigante asiático adquiere conciencia del potencial disruptivo que puede tener el desarrollo tecnológico dentro de su sistema, y de las posibilidades que ofrece a nivel exterior.

Internet llegó a China en el año 1994, siendo incorporado bajo la categoría de telecomunicaciones, pero a raíz de su rápido desarrollo y expansión de su dominio como lugar de creación de redes transnacionales y de disensión fue rápidamente incorporado a la propaganda a mediados de la década. Esto llevó a la prohibición por parte del gobierno de determinados sitios web y el bloqueo del acceso a redes externas que suministraban contenido como noticias o pornografía, generando un recelo que ha permanecido en China desde el comienzo de la expansión de internet global, lo que hizo que se construyeran muy pocos puntos de entrada y de salida de la red del país, generando una situación más propicia para controlar la red (Adee, 2019). Con el objetivo de comenzar a monitorear el acceso a internet desde China se comenzó a trabajar en un cuerpo de instituciones y leyes regulatorias del mismo conocido como el Gran Cortafuegos (Chan, 2018).

Ya en el año 2015 el Ministerio de Defensa de China publicó un *paper* articulando la estrategia militar del país, y en él se instaba al ELP a abandonar su "mentalidad tradicional" centrado en la guerra terrestre, y poniendo en el centro los principios del Sueño Chino como objetivos a conseguir a través de dicha estrategia. Estos principios se pueden entender a su vez en otros tres subprincipios, como son la soberanía, la modernidad y la estabilidad. Una de las aristas de la soberanía es precisamente la soberanía en el ciberespacio, por lo que se convierte en un pilar central para conseguir esos objetivos y asegurar la estabilidad interna (Kolton, 2018).

Por un lado, a nivel interno la línea general de China es crear un ecosistema cibernético propio, sin posibilidad de injerencia externa, posibilitado por el conocido Gran Cortafuegos (proyecto Escudo Dorado). Se trata de una serie de medidas legislativas y tecnológicas para impedir el uso común de internet en su territorio, impidiendo así la conexión exterior, y evitando el flujo de pensamiento y comunicaciones que a la larga podrían ser causa de contestación social al gobierno de Pekín. Se implantó en el año 1998, pero es desde el año 2008 que lleva a pleno rendimiento (Novared, 2022).

El sistema funciona de manera tal que, si un usuario quisiera acceder a una página o noticia que el sistema considera perjudicial para sus intereses, el servidor DNS (*Domain Name System*) podría dirigirlo a una página falsa o a otra con información que no sea relevante para él (Vargas Chaparro, 2022).

Por otro lado, a nivel exterior la actuación cibernética china se encauza por otros medios. Las ciber-operaciones (que China define como "guerra en redes") van encaminadas hacia las operaciones psicológicas o de denegación y engaño. Además, también se han llevado a cabo campañas de ciberataques y robos de información a ciudadanos y empresas de países rivales (entre ellos Apple o Tesla) con el objetivo de usarla a su favor, aunque siempre negando la autoría.

Hay un tipo de operaciones que se realizan tanto en el plano interno como externo a la vez, y que responden a la misma finalidad. Estas operaciones tienen un carácter asimétrico y permiten evitar el conflicto cuerpo a cuerpo, adquiriendo un carácter de lo más variado, por lo que se conocen como operaciones multidimensionales. Una de las premisas de la doctrina china con respecto a las operaciones psicológicas, de propaganda política, guerra legal o penetración en las redes adversarias es que deben llevarse a cabo tanto en tiempos de paz como de guerra. Esto implica que la frontera entre ambas se difumine, y "sea legítimo emplear múltiples actividades psicológicas, propagandísticas, electrónicas o cibernéticas que no solo apoyen la consecución de la ventaja informativa en caso de crisis sino también apoyar el desarrollo nacional de todas sus dimensiones" (Colom, 2020).

Por otro lado, Vargas-Chaparro (2022) propone un análisis de la estrategia cibernética de China con base en el planteamiento de Patrascu (2019) sobre los tres niveles del ciberespacio. Para este autor, el ciberespacio se compone de tres niveles, como son el nivel físico (compuesto por la geografía y la red física), el nivel virtual (la red) y la interacción de las personas con la red. Dado el nivel de abstracción y de complejidad de este último, el autor analiza la acción china en los dos primeros niveles.

En el nivel virtual China pretende crear una red alternativa a Internet gracias a empresas como Huawei, conocida como New IP (*Internet Protocol*), que busca sustituir a la red tradicional y fomentar un modelo en el que los gobiernos puedan controlar todo lo que circula en la red, configurándose como un modelo en el que la disensión y la crítica podrían ser fácilmente controlados y eliminados. Para ello debe contar con el apoyo de la Unión Internacional de Telecomunicaciones que depende de ONU, que se encarga de verificar y legitimar las nuevas tecnologías y sistemas a ojos de determinados gobiernos. Además, en este nivel el autor integra también el Gran Cortafuegos, con una misión no sólo de protección interna del sistema, sino como telón de fondo del ataque cibernético a países rivales no sólo hacia infraestructuras críticas, sino también para el robo de propiedad intelectual a determinadas empresas, como hemos apuntado con anterioridad.

En el nivel físico China se centra en el control de la infraestructura tecnológica, y en esa empresa tiene un lugar central la Ruta de la Seda Digital, que se concibe como esa parte de la Ruta de la Seda o BRI constituida por empresas de telecomunicaciones, proyectos tecnológicos, inversiones en fibra óptica, redes de telecomunicaciones, así como todo tipo de elementos de carácter tecnológico. El aspecto tecnológico ha

sido uno de los principales en los que China ha asentado su estrategia de crecimiento más allá de sus fronteras, posibilitada por la potencia de sus empresas tecnológicas, como en el ámbito del comercio electrónico, los servicios en la nube, y los gigantes de pagos *AliBaba, Ant Financial, Tencent y* JD.com, redes sociales *TikTok*, desarrolladores de dispositivos inteligentes y fabricantes de drones. Además, la inversión en infraestructuras tecnológicas y de red más allá de sus fronteras permite a China ampliar su modelo de gobernanza de internet a países que consideran atractivo el modelo de gobernanza que propone el país, con un mayor control de los gobiernos sobre los contenidos y funcionamiento del mismo, especialmente tentador para aquellos países de corte más autoritario.

El autor sostiene que de acuerdo con la teoría del poder de Kuehl (2012), la acción china va dirigida a conseguir "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", y que pretende usarla como forma de desplazar a EEUU de su posición de liderazgo mundial.

A la vista de lo expuesto podría parecer que la expansión tecnológica de China es soportada por las empresas del país en solitario, pero el Gobierno de Pekín juega un rol bastante importante en la misma. De esta forma hay autores que califican la estrategia china como tecnonacionalismo (Cuenca y Vázquez, 2021). Este proceder consiste en una fuerte inversión pública en las empresas tecnológicas punteras y en la implementación de medidas proteccionistas que las favorezcan. No se trata de una práctica que lleve a cabo China en exclusiva, sino que la mayoría de países que hoy están a la cabeza del sector tecnológico han implementado una forma de actuar que sigue esta lógica, como Japón, Corea del Sur, o Taiwán. Para entender el motivo que existe detrás de esta actuación debemos retrotraernos al afán de soberanía y de recuperar el lugar que antaño tuvo el país, con la concepción *Tianxia* en el centro, algo que está en el núcleo de la política exterior china durante la última década.

Esta concepción se ve bien reflejada en las intervenciones públicas del gobierno chino sobre ciberseguridad. En diciembre de 2015 Xi Jinping inauguró la Conferencia Mundial de Internet (WIC), un evento organizado por la Administración del Ciberespacio de China, y en cuyo discurso señaló la necesidad de apostar por un ciberespacio regulado y de evitar su militarización. Además, subrayó que la ciber-soberanía debe ser unas de las premisas que rijan en la sociedad internacional actual (Real Instituto Elcano, 2016). A este respecto es importante tener en cuenta las contradicciones que subyacen a este discurso, ya que los ciberataques por parte de grupos relacionados con el gobierno chino vienen siendo frecuentes desde hace décadas. Esta línea argumental se entiende desde la visión china de pretender desmarcarse del orden establecido y proporcionar un nuevo marco en el que se rijan las relaciones interestatales acorde con los principios y valores que Pekín defiende, y que cada vez más países del mundo compran.

Desde Pekín también se plantea la importancia de la cooperación internacional en el ámbito ciberespacial como componente esencial de la soberanía en la red, lo cual hizo que en el año 2017 publicaran el documento sobre Estrategia de Cooperación Internacional en el Ciberespacio (publicada en línea por Xinhua News). Esta se divide en

seis bloques, como son la soberanía y la seguridad en internet; desarrollar un sistema de reglas internacionales; promover una gobernanza justa de internet; proteger los derechos e intereses legítimos de los ciudadanos; promover la cooperación en economía digital; y construir una plataforma para el intercambio de ciber-cultura (Xinhua, 2017). En el documento observamos cómo la posición de China respecto a la gobernanza de internet y su regulación es similar a la que mantiene en otros ámbitos de la sociedad internacional a través de jugar el rol de abanderado de los países de la periferia del sistema que reclaman más peso en la toma de decisiones, como por ejemplo al reclamar un sistema de gobernanza justa y transparente, dando preeminencia a la soberanía y apostando por un acceso libre a internet mientras se aseguren los intereses públicos y nacionales. Por otro lado, se señala que el papel de salvaguardar la soberanía china en la red corresponde al ejército chino (ELP), por lo que este se centrará en desarrollar sus capacidades tecnológicas para poder asegurar el fin de la no injerencia supranacional (Schreiber, 2018).

En lo relativo a la incorporación tecnológica en el ámbito de las Fuerzas Armadas es importante resaltar que ha sido un proceso que en primera instancia se caracterizó por la emulación, concretamente a EEUU, ya que en el ámbito militar fueron pioneros en introducir innovaciones tecnológicas desarrolladas a finales del siglo pasado. En China se consideró que la innovación tecnológica podía ser el pilar de la RMA del Ejército de Liberación Popular en el nuevo siglo (Colom, 2020). Así se configura la guerra informativa china, en cuyo desarrollo ha tenido gran incidencia las lecciones aprendidas de la Guerra del Golfo y la Operación Tormenta del Desierto, poniendo en el centro el concepto de guerra informativa (IW).

La guerra informativa se define como aquellas operaciones de información que se realizan tanto en tiempos de paz como de guerra para conseguir o promover determinados objetivos específicos sobre un adversario específico (Mulvenon, 1999). Para los teóricos chinos, la IW tuvo un papel clave en la Operación Tormenta del Desierto en el reconocimiento de lugares estratégicos y posiciones iraquíes, destruyendo de forma rápida el equipamiento enemigo (de origen iraquí, soviético y chino). Mulvenon recoge varias definiciones sobre la IW de teóricos chinos, pero todas comparten un núcleo común, como es la informatización -*wangluohua*- del campo de batalla. El objetivo último de la IW es el dominio de la información definido como la habilidad para defender la propia información mientras se explota y se asalta la estructura informativa del oponente. A continuación, trataremos el tema de la IW con más profundidad en el aspecto operacional, pero es importante saber que, a raíz de la Guerra del Golfo, el ELP ha puesto en el centro de su acción la necesidad de tomar ventaja en ese ámbito, desarrollando numerosos centros de excelencia, revistas, libros y producción científica de todo tipo referidas al mismo.

Además, retomando los principios generales de la estrategia de cooperación internacional de China en el ciberespacio, el principal aliado del país en esta materia ha sido Rusia, coincidiendo que ambos comparten intereses y valores similares en el dominio de la red. Esta cooperación se ha dado especialmente en el marco de la Organización de Cooperación de Shanghái, habiendo firmado acuerdos de cooperación en la materia. Hay autores como Margolin (2016) que señalan que más que cooperación

de lo que se trata es de un "matrimonio de conveniencia" al tener como objetivo común la estabilidad del régimen, así como una pretensión de mayor protagonismo internacional.

Para tener una idea general, el comandante Kolton (2018) explicita de forma gráfica la composición de la ciber-estrategia de China no solo desde el punto de vista militar, la cual por definición se compone de medios, modos y fines. Comenzando por el final, y recogiendo la idea de lo que venimos comentando a lo largo de este apartado, el fin último de la misma se compone de la ciber-soberanía, con el Partido Comunista Chino reteniendo la autoridad en el ciberespacio y salvaguardando el Sueño Chino en todos los dominios, otorgando la posibilidad de ejercer la soberanía plena en todos ellos. Por otro lado, los medios en la estrategia se configuran como aquellos elementos a utilizar para conseguir los fines, y en el caso de la ciber-estrategia china es una nueva ciber-fuerza conjunta con ciber-capacidades avanzadas tales como entendimiento ciber-situacional, ciberdefensa y *targeting* preciso. Finalmente, en lo relativo a los modos que se constituyen como las formas de articular los medios para conseguir los fines, el comandante los recoge en los siguientes: parar y controlar ciber-crisis mayores; proteger la red nacional e información de seguridad; salvaguardar la seguridad nacional y estabilidad social; apoyar los esfuerzos del país en el ciberespacio; y participar en la ciber-cooperación a nivel internacional.

Análisis operacional

Los ataques en el ciberespacio se configuran como un recurso a la orden del día en los tiempos que corren desde el punto de vista de que permiten obtener información muy valiosa (la mayoría de comunicaciones, información o sistemas del mundo funcionan vía informática) a la vez que resulta sencillo denegar la autoría de los mismos. Estas operaciones se encuadran en los conflictos en zona gris, especialmente los relativos al robo de datos, información sensible o ataques a infraestructuras críticas. Resulta importante afirmar que utilice China en exclusiva, sino que en mayor o menor medida prácticamente todas las potencias tecnológicas del mundo llevan a cabo ataques en la red a día de hoy.

En lo que se refiere a la autoría, al ser difícil de probar, hay que atender a criterios técnicos para poder juzgar al respecto, ya que cuando se producen ataques dirigidos al robo de información o ataques a infraestructuras de determinados países no suele ser habitual que el país agresor reconozca la autoría. Vamos a proceder a realizar un análisis de los ciberataques más conocidos de la última década sobre los que se ha responsabilizado a China, sin entrar a juzgar la cuestión de la autoría.

En la Tabla 1 recopilamos algunos ejemplos de ciber-acciones ofensivas cuya responsabilidad se ha adjudicado al Gobierno chino, aunque como señalamos su vinculación no está clara. Aunque bien es cierto que los ataques de este estilo siguen una tendencia al alza en la última década, lo cual no deja de ser llamativo, y deja entrever que posiblemente sí que haya un nexo con Pekín. Hemos tratado de incluir ciberataques con objetivos variados, ya que abarcan desde ataques a organismos públicos o empresas hasta infraestructuras críticas. Por otro lado, también se han denunciado diversos ataques a diputados y políticos occidentales (EEUU y Reino Unido) con el

objetivo de conseguir información privada[1]. Además, vemos reflejadas en ellos algunas de las cuestiones que hemos comentado anteriormente, como el robo de datos y de propiedad intelectual a determinadas empresas de defensa estadounidenses, con el objetivo de usarla en favor propio. Un ejemplo claro de esta actuación es que el caza J-35 chino tiene un diseño prácticamente idéntico al del caza F-35 estadounidense, hasta tal punto que muchos oficiales norteamericanos piensan que se ha basado en diseños robados a su ejército durante alguno de estos ciberataques[2].

Tabla 1. *Recopilación de operaciones de ciberataques vinculados a China en la última década*

FECHA	OPERACIÓN	EN QUÉ CONSISTE	OBJETIVO	MEDIO
2009-2010	Aurora	Ataque masivo contra más de 30 grandes empresas como Google, Adobe o Juniper.	Robar datos sensibles a estas empresas	Grupos de hackers APT1 (posible vinculación al ELP).
2014-2015	Sin nombre oficial	Ataque a la Oficina de Administración de Personal.	Dejar al descubierto información sensible de 21'5 millones de personas y contratistas	Grupos de hackers supuestamente vinculados al Gobierno
2012-2015	Sin nombre oficial	Ciberespionaje a empresas de defensa de EEUU.	Robar información clasificada y tecnología militar.	Actores chinos presuntamente.
2017	Sin nombre oficial	Intento de infección agencias gubernamentales y empresas privadas.	Tratar de influir en el funcionamiento de las mismas usando una puerta trasera en el software SolarWinds Orion	Grupo SolarWinds. Supuesta relación con el gobierno de Pekín.
2023	Sin nombre oficial	Ataque a infraestructuras de comunicaciones críticas de EEUU en Guam.	Atacar el funcionamiento de las mismas, dado que es una base de apoyo a Taiwan.	Grupo de hackers Volt Typhoon.

Fuente: elaboración propia.

[1] Reino Unido acusa a china de "maliciosos" ataques cibernéticos contra sus diputados. El Mundo, 25 de marzo de 2024. https://www.elmundo.es/internacional/2024/03/25/6601a6ade85ece0e248b458a.html

[2] China ya tiene un nuevo "caza invisible" para su nuevo portaviones. El Confidencial, 27 de julio de 2022. https://www.elconfidencial.com/tecnologia/novaceno/2022-07-27/china-copia-f35-eeuu-nuevo-portaaviones_3466826/

En otro apartado, la presencia china en redes sociales y en el ámbito global también es creciente desde el punto de vista de la realización de operaciones de propaganda, psicológicas y de engaño de cara al resto del mundo. Esta empresa se ha expandido especialmente desde el año 2009, y en ella han jugado un papel fundamental las agencias estatales de noticias como *Xinhua* (primero en inglés y progresivamente ha ido creciendo hasta existir en varios idiomas como español, alemán o italiano) y *China Daily*. Estos medios cuentan con página web accesible desde el resto del mundo, así como con cuentas en redes sociales como *X* o *Facebook*. Las operaciones de desinformación y propaganda a través de estos medios consisten en la publicación de noticias sobre China con un contenido similar a las publicadas por los medios occidentales, pero con una visión mucho más positiva de las mismas y sirviendo de altavoz para el blanqueamiento del régimen de Pekín. Entre ellas se pueden encontrar supuestas alabanzas de diplomáticos extranjeros al régimen o a las políticas del país, o por ejemplo presentar las protestas de Hong-Kong de 2019, que eran contra el Gobierno, como a favor del Gobierno[3], o incluso para deshumanizar a los protestantes. Además, en las redes sociales occidentales, estos medios han tratado de usar la opción de promocionar su contenido, ante lo cual dichas plataformas se han tratado de proteger advirtiendo a sus usuarios sobre la problemática de la publicidad engañosa. El objetivo de China con estas acciones es generar una opinión positiva en una parte significativa de las sociedades objetivo, entre las cuales figuran los países del Sur Global como uno de sus principales objetivos (Ohlberg, 2019). Además también se ha constatado la existencia de una especie de "policía de internet" compuesta por dos millones de usuarios que se encargan de la vigilancia de la red empleando *software* de minado de datos para rastrear palabras clave en la red y en motores de búsqueda como Baidu, filtrando las URLs para no dar lugar a palabras consideradas como "dañinas o antisociales" para el régimen, además de contar con una suerte de ejército en la red que contribuyen a generar comentarios positivos y censurar los negativos sobre el país en redes sociales (Chan, 2018).

A nivel interno las operaciones en la red cuentan con el Gran Cortafuegos como soporte. La ciberseguridad interna china se basa en la Ley de Ciberseguridad implementada en el año 2017, en la cual todo queda bajo el control del Partido. Esta Ley establece que el Ministerio de Seguridad Pública puede tener acceso a todos los datos brutos de los ciudadanos chinos en internet, que debe procesar. No existirá ningún dato con carácter confidencial, ya que toda comunicación podrá ser conocida por el Estado, una condición a la que también están sometidas las empresas extranjeras operando en el país. Antes de esta Ley las empresas extranjeras podían evitar estos controles usando sistemas VPN, pero estos han quedado radicalmente prohibidos. Esto hace que no existan secretos comerciales ocultos para el Gobierno, que tiene acceso a canales de comunicación como WeChat.

---

[3] Chinese State Media And Others Are Spreading False Information About The Protests In Hong Kong, 15th June 2019.
https://www.buzzfeednews.com/article/lmashkoor/hoaxes-hong-kong

Este sistema de protección integral se conoce oficialmente con el nombre de Esquema de Protección Multinivel de Ciberseguridad ("MLPS 2.0"), con un sistema enormemente complejo (Harris Sliwoski, 2020). Este sistema permite que, al tener controlados los datos de las empresas extranjeras que operan en China, todos ellos quedan expuestos al Gobierno, que al tener a su vez participación en la mayoría de empresas punteras en el sector tecnológico, pueden usar los datos de dichas empresas foráneas. Finalmente, esta intervención permite ejecutar operaciones de propaganda y desinformación a nivel interno mucho más agresivas que las que realiza fuera de sus fronteras, y evitar que la información de fuera entre en el país y pueda desestabilizar al régimen.

En suma, nos encontramos con un sistema que a nivel operacional es bastante poco sofisticado, que prioriza el control del Partido de la información y que se favorece de la flexibilidad y ventajas que otorgan la existencia de un sistema iliberal en el que la rendición de cuentas y la legalidad brillan por su ausencia. Estas operaciones que hemos analizado encajan bien en la conceptualización que hemos hecho anteriormente de las operaciones en la zona gris, ya que suelen ir dirigidas a desestabilizar y a contribuir a conseguir objetivos en un escenario que no es de guerra, pero tampoco es competición pacífica.

Conclusiones

Como hemos observado a lo largo de nuestra investigación, la red tiene una importancia central para China en el marco de su consolidación como superpotencia mundial y a la hora de disputar la hegemonía mundial a EEUU. Respecto a la pregunta que vertebra este trabajo, que gira alrededor de cómo China ha usado el ciberespacio de cara a favorecer la consecución de sus principales intereses estratégicos, podemos concluir con varios puntos.

China concibe la red como un espacio con un enorme potencial disruptivo de su sistema político, así como uno que ofrece grandes posibilidades de cara al crecimiento económico, militar y político del país. Dada la importancia de este espacio y las posibilidades que ofrece Pekín pretende controlar todos los aspectos relacionados con su regulación y funcionamiento, con el fin último de asegurar su soberanía en la red para llegar a conseguir materializar los principios preconizados en el Sueño Chino. Este control se puede llevar a cabo por todo el sistema legislativo y normativo que el país ha venido implementado desde hace décadas, así como por las ventajas físicas derivadas de la escasa inclusión del país en el sistema de red global. En última instancia se trata de maximizar capacidades y aprovechar oportunidades para utilizarlo como instrumento de poder.

A nivel interno la prioridad es mantener todo el ciberespacio y, en consecuencia, todos los datos e información que circulan por ella, bajo el control del Partido y del Estado. A nivel externo las operaciones en la red que China lleva a cabo revisten un carácter variado. Se pueden enmarcar como acciones híbridas o de guerra irrestricta en un escenario de conflicto en la zona gris con sus tradicionales enemigos (especialmente EEUU, países de la UE y contra Taiwán). En ellas incluimos operaciones de influencia en la opinión pública y por otro lado las operaciones de ataques informáticos a través

de grupos de hackers vinculados al gobierno de Pekín. Las operaciones en la red le permiten a China mantener la estabilidad del régimen y a la vez ir consiguiendo objetivos estratégicos fuera de sus fronteras, así como obtención de inteligencia e información, permitiéndoles negar la autoría de las mismas de forma más fácil, por lo que hemos trabajar sobre indicios cuando analizamos las actividades de este tipo.

Esta línea estratégica de la actuación china en el plano cibernético va muy en consonancia con la política exterior que viene desplegando en el siglo XXI y, especialmente, desde la llegada de Xi Jinping a la dirección del país. Partimos desde el punto de vista de que las acciones en la red son una parte fundamental de su acción exterior, y por ello comparten una serie de objetivos. La actividad china es sigilosa y en ningún momento pretende ser disruptiva ni entrar en conflictos directos. En lugar de la fuerza o de la coerción directa, China prefiere hacer uso de la influencia y de la dependencia que el resto del mundo puede tener del gigante asiático. En esa línea va la intención de crear un ciberespacio propio y diferente de la tradicional red de Internet, en el cual los Gobiernos tengan mucha más capacidad de decisión que en el actual. Esta pretensión es común a la de muchos otros gobiernos del mundo, especialmente aquellos de corte autoritario e iliberal, que ven en los valores y en la concepción china una propuesta mucho más atractiva desde su óptica que la tradicional propuesta Occidental. En la línea de esta pretensión se enmarca la cooperación con países aliados como Rusia de cara a reclamar una nueva regulación de la red que permita a los gobiernos controlar los contenidos que circulan por ella con el objetivo de asegurar los intereses nacionales, lo cual tratándose de gobiernos de corte autoritario es un argumento que puede servir para enmascarar el control de la disensión que pretenden llevar a cabo.

Esta ambición de China no se da únicamente en el espacio cibernético, sino que la vemos en otros muchos aspectos de su acción exterior, como en la creación del Banco Asiático para la Inversión en Infraestructuras, o en la reclamación de un papel mucho más activo de los BRICS en la seguridad internacional. Las iniciativas de Pekín que pretenden aumentar la presencia de empresas propias invirtiendo en infraestructuras tecnológicas a nivel mundial también son parte de la estrategia cibernética china, ya que posibilitan ampliar la red física con la que el país pueda expandir su modelo de internet a nivel global.

Desde el punto de vista de la concepción china del sistema internacional esto puede explicarse desde la concepción *Tianxia*, en la que China se constituye como el centro del sistema que a su vez cuenta con estados vasallos por la vía de la cooperación y el beneficio mutuo. Es un debate por resolver si la acción exterior china se guía más por los principios de esta doctrina o por los principios de la lógica realista tradicionalmente imperante en las relaciones interestatales.

Antes de finalizar es útil resaltar que a la hora de realizar esta investigación hemos encontrado varias limitaciones que nos han lastrado, como por ejemplo la falta de información fiable sobre la doctrina china en el ciberespacio (que tiene carácter secreto), o la no existencia de una lista concreta de acciones ofensivas potencialmente realizadas por agentes conectados con Pekín en el ciberespacio, así como por supuesto la dificultad de confirmar que el gobierno chino esté detrás, por lo que nos basamos en meras suposiciones e intuiciones.

Así, podemos determinar que el ciberespacio (a pesar de que desde la perspectiva china no existe tal cosa) ha adquirido en apenas veinte años la condición de espacio de confrontación por la hegemonía mundial, a la vez que se constituye como un medio para conseguirla, siendo compuesto por una doble vertiente que hace de él uno de los aspectos más interesantes a seguir en la pugna entre potencias globales. China sabe que las nuevas guerras se libran en la red, y tiene una estrategia sólida para ganarlas.

Referencias

Adee, S., Por qué los esfuerzos de Rusia y China para poner fronteras a internet suponen el fin de la red tal y como la conocemos. BBC News. (2019). Obtenido en https://www.bbc.com/mundo/vert-fut-48618084

Chan, S., Cybersecurity under Xi-Jinping. Por *Digital Center*, (2018). Obtenido en https://www.digitalcenter.org/wp-content/uploads/2018/01/Cybersecurity-under-Xi-Jinping-analysis.pdf.

Colom, G., "Vigencia y limitaciones de la guerra híbrida", *Revista Científica General José María Córdova*, n. 10, 2012.

Colom, G., La guerra informativa china en la zona gris. *Upo*. (2020). Obtenido en https://www.academia.edu/42116810/La_guerra_informativa_china_en_la_zona_gris

Cuenca, A., Vázquez, J., *Tecnonacionalismo: la estrategia de China para convertirse en una superpotencia*. Observatorio de Política China [OPCh]. (2021). Obtenido en https://politica-china.org/areas/sistema-politico/tecnonacionalismo-la-estrategia-de-china-para-convertirse-en-una-superpotencia

Expósito, J., "China en el ciberespacio", *Revista Ejércitos*, 2024a.

Expósito, J., "El dominio de la información: el ciberespacio visto desde China", *Revista Ejércitos*, 2024b.

Harris S., Ciberseguridad en China: No hay lugar donde esconderse. (2020). Obtenido en https://harris-sliwoski.com/es/chinalawblog/china-cybersecurity-no-place-to-hide/#II_Chinas_Comprehensive_Network_Security_Program

Jordán, J., "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", *Revista Española de Ciencia Política*, n. 48, 2018, 129-151.

Kania, E., *et al.*, China's Strategic Thinking on Building Power in Cyberspace. *New America*. (2017). Obtenido en https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

Kolton, M., "Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence", *The Cyber Defense Review*, 2018.

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

Liang, Q., Xiangsui, W., *Unrestricted Warfare*. PLA Literature and Arts Publishing House. Beijing. (1999). Obtenido en https://www.c4i.org/unrestricted.pdf

Margolin, J., Russia, China, and the Push for "Digital Sovereignty". *Digital Society.* (2016). Obtenido en https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

Mulvenon, J., The PLA and Information Warfare. (1999), en J. Mulvenon y R.Yang, *The People's Liberation Army in the Information Age*. RAND Corporation.

Novared, *¿Qué es el Gran Cortafuegos de China, sistema que censura Facebook y Google?*. (2022). Obtenido en https://www.novared.net/que-es-el-gran-cortafuegos-de-china-sistema-que-censura-facebook-y-google/

Ohlberg, M., Propaganda beyond the Great Firewall. Chinese party-state media on Facebook, Twitter and YouTube. *Mercator Institute for China Studies.* (2019). Obtenido en https://merics.org/en/comment/propaganda-beyond-great-firewall

Pablo López, M., La guerra irrestricta ¿un nuevo modo de hacer la guerra? *Estudios CEEAG*, nº 11. (2015). Recuperado de https://www.academia.edu/19706360/Guerra_Irrestricta_un_nuevo_modo_de_hacer_la_guerra

Pătrașcu, P., "Missions and actions specific to cyberspace operations. *International Conference Knowledge-Based Organization*", Vol. 25, n. 3, 2019, 51-56.

Real Instituto Elcano, La ciber-soberanía china. Comentario 20 de enero de 2016. (2016). Obtenido en https://www.realinstitutoelcano.org/comentarios/la-ciber-soberania-china/

Recalde, L., "El ciberespacio: el nuevo teatro de guerra global", *Revista de Ciencias de Seguridad y Defensa,* Vol. 1, n. 2, 2016. Obtenido en https://journal.espe.edu.ec/ojs/index.php/revista-seguridad-defensa/article/view/RCSDV1N2ART6

Rodríguez, M. E., "La evolución de la política exterior china/ The Evolution of China´s Foreign Policy", *Araucaria*, Vol. 18, n. 35, 2016.

Schreiber, C., El futuro de China y Rusia como aliados en el ciberespacio. Análisis GESI, 2/2019. (2019). Obtenido en https://www.seguridadinternacional.es/?q=es/content/el-futuro-de-china-y-rusia-como-aliados-en-el-ciberespacio

Sierra, A., Marrades, A., La nueva era de China. La gran estrategia para el sueño de Xi Jinping, *Fuera de Ruta*, 2022.

Tingyang, Z., *Tianxia: una filosofía para la gobernanza global,* Herder, 2021.

Vargas-Chaparro, N. E., "La cibergeopolítica de China: un interés estratégico de Estado", *Estudios En Seguridad y Defensa*, Vol. 17, n. 33, 2022, 201-222.

Xinhua News, China presenta primera estrategia sobre cooperación en el ciberespacio. (2017). Recuperado de https://spanish.xinhuanet.com/2017-03/02/c_136094904.html

Yaqing, Q., "Cultura y pensamiento global: una teoría china de las relaciones internacionales", *Revista CIDOB d'Afers Internacionals*, 2012, 67-90.