ARTÍCULOS

Cuadernos de Nuestra América/Nueva Época/No. 014 / enero-marzo, 2025/
RNPS: 2529 /ISSN: 2959-9849/ 269 pp.

La Triple dimensión del ciberespacio chino: defensa, ciencia y tecnología

The triple dimension of Chinese cyberspace: defense, science and technology

M. Sc. Elio Perera Pena

Licenciado en Periodismo. Máster en Historia Contemporánea y Relaciones Internacionales. Investigador Auxiliar del Centro de Investigaciones de Política Internacional (CIPI). Profesor Auxiliar del Instituto Superior de Relaciones Internacionales (ISRI) Raúl Roa García. Diplomado en Estudios sobre los Estados Unidos y en Relaciones Cuba-Estados Unidos.

ORCID: 0000-0003-1086-2854

e-mail: eliopererapena@gmail.com

Fecha de recepción: febrero de 2025.
Fecha de publicación: abril de 2025.

Resumen

El ciberespacio se ha convertido en un ámbito crucial para la gobernanza y la soberanía de los Estados, especialmente en el caso de China que ha desarrollado una estrategia integral de gobernanza digital. El Gobierno chino priorizó la construcción de una infraestructura tecnológica, incluyendo Inteligencia Artificial (IA) y computación en la nube, para fortalecer su control sobre el ciberespacio y garantizar la seguridad nacional.

Palabras claves: *ciberespacio, gobernanza digital, tecnologías, China, Estados Unidos.*

Abstract

Cyberspace has become a crucial area for the governance and sovereignty of states, especially in the case of China which has developed a comprehensive digital governance strategy. The Chinese government prioritized the construction of a technological infrastructure including Artificial Intelligence and Cloud Computing to strengthen its control over Cyberspace and ensure National Security.

Keywords: *Cyberspace, Digital Governance, Technologies, China, USA.*

Introducción

El término ciberespacio fue acuñado por el escritor William Gibson en su novela de ciencia ficción *Neuromante* (1984), en la que lo describió como una realidad virtual consensuada. Desde entonces el concepto ha trascendido la ficción para convertirse en un escenario tangible.

El ciberespacio se puede definir como un entorno digital creado por la interconexión global de sistemas informáticos, redes y dispositivos, en el que la información fluye y las interacciones humanas se llevan a cabo de manera virtual.

Ha experimentado una evolución significativa desde sus inicios. En las décadas de los ochenta y noventa se limitaba principalmente a redes académicas y militares estadounidenses como ARPANET. Con la llegada de Internet el ciberespacio se expandió rápidamente incorporando a millones de usuarios y dando lugar a nuevas formas de comunicación como el correo electrónico y los foros en línea. La proliferación paulatina de dispositivos móviles y de las redes sociales han transformado al ciberespacio en un ente omnipresente e integral en la vida cotidiana.

En cuanto a comunicación y conectividad, revolucionó la forma en que las personas se comunican eliminando barreras geográficas y temporales. Las criptomonedas y las Fintech[1] son ejemplos de cómo el ciberespacio ha transformado la economía creando nuevas oportunidades.

Sobre su intervinculación con la cultura y el entretenimiento, la digitalización de la cultura ha dado lugar a modos de creación y consumo como el *streaming* de música y video, videojuegos en línea y el arte digital.

El ciberespacio: un dominio estratégico

El ciberespacio se ha convertido en un campo de batalla estratégico para el hemisferio. En China el ciberespacio es visto como un componente esencial de la seguridad nacional y el desarrollo económico. El Gobierno chino ha implementado políticas estrictas para regular el ciberespacio, incluyendo el gran cortafuegos (Firewall) de China, que controla el flujo de la información y protege la infraestructura digital.

En el X Plan Quinquenal (2001-2005) se estableció 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. En el Congreso del Partido Comunista chino, celebrado en 2002, la información fue reconocida como esencial para el crecimiento del poder nacional integral; y en consecuencia en 2005 se publica la Estrategia Nacional 2006-2020 para el Desarrollo de la Información.

En cuanto al tratamiento, estudio y control del ciberespacio el Ejército Popular de Liberación siempre le otorgó a la Información y su infraestructura técnica de recopilación, resguardo y distribución una importancia crucial por cuanto está en el deber de ejercer la protección de sus intereses nacionales.

Así lo demuestra un artículo escrito, por el entonces coronel, Wang Baocun en el *Pla Daily* de abril de 1998:

> La oportunidad creada por la nueva Revolución militar es única en la vida. Nuestro ejército disfruta de muchas condiciones favorables para la informatización. Nuestro país ha logrado un rápido proceso en informatización y tiene la energía potencial para extender este trabajo a los militares. Una característica importante de la actual Revolución Militar es que la informatización local comienza antes y se desarrolla más rápido que en las fuerzas armadas y es tecnológicamente más avanzada. Después de generar suficiente energía potencial el trabajo se extenderá a los militares y desencadenará una enorme transformación militar (Expósito, 2022).

Mientras que para la mayoría del denominado Occidente y por ende también para los Estados Unidos, existen cinco dominios, tierra, mar, aire, espacio y ciberespacio, para los especialistas chinos el ciberespacio se concibe como la interacción de dos ámbitos distintos, el espectro electromagnético y la Informatización.

En las últimas décadas, China ha emergido como una potencia global en el ámbito científico y tecnológico, consolidando su posición por medio de una estrategia integral que vincula el desarrollo de las ciencias con la expansión del ciberespacio.

Desde la implementación del Plan "Made in China 2025" el gobierno ha priorizado la innovación tecnológica como motor del desarrollo, enfocándose en áreas como la IA, el *big data* y la ciberseguridad, lo que permite posicionar a China como líder en la cuarta revolución industrial.

Presentada en el año 2015, es una estrategia industrial que busca transformar a China en una potencia manufacturera de alta tecnología. El objetivo es reducir la dependencia de tecnologías extranjeras y promover la innovación local en sectores clave como la robótica, la IA, los vehículos eléctricos y la biotecnología. La Internet de las cosas es un componente esencial que la complementa, ya que permite la creación de fábricas inteligentes y cadenas de suministro más eficientes.

Internet plus, presentada también en 2015, fomenta la integración de Internet con sectores tradicionales como la agricultura, la logística y los servicios financieros. Busca impulsar la digitalización de la economía y promover el uso de tecnologías emergentes como la Internet de las cosas, la *big data* y la computación en la nube.

---

1 Empresa que utiliza tecnología para ofrecer servicios financieros de manera innovadora, eficiente y accesible. El término proviene de la combinación de las palabras "finanzas" y "tecnología".

La Internet de las cosas es fundamental para Internet plus, ya que facilita la conectividad entre dispositivos y sistemas permitiendo la creación de ecosistemas digitales interconectados.

La proliferación de dispositivos conectados permite que la Internet de las cosas facilite el desarrollo de plataformas de comunicación avanzadas como *Wechat* y *Alipay*, que integran múltiples servicios en una sola aplicación.

La relación entre las citadas iniciativas es que, la Internet de las cosas actúa como un puente entre Made in China 2025 y la Internet plus, ya que posibilita la convergencia de la manufactura avanzada y la digitalización de la economía.

Por un lado, Made in China 2025, utiliza la Internet de las cosas para modernizar la industria y mejorar la productividad. Por el otro, Internet plus aprovecha la Internet de las cosas para crear nuevos servicios y modelos de negocios basados en datos. Esa sinergia ha permitido a China posicionarse como líder global en innovación tecnológica.

La relación entre las ciencias y el ciberespacio se ha fortalecido, gracias a una inversión masiva en investigación y desarrollo (I+D). El país ha destinado recursos significativos a la formación de talentos en disciplinas STEM (ciencia, tecnología, ingeniería y matemáticas) y ha establecido centros de excelencia en innovación tecnológica, lo que ha permitido el desarrollo de algoritmos de IA, que se aplican en sectores como, la medicina, la logística y la defensa.

En el ámbito internacional, la República Popular China ha adoptado un enfoque de cooperación, mientras participa activamente en organismos internacionales de ciberseguridad, y promueve iniciativas como la nueva ruta de la seda digital, que busca promover el desarrollo tecnológico en otras naciones.

El futuro de la relación entre las ciencias y el ciberespacio chino, está marcado por tendencias emergentes, que prometen transformar aún más la sociedad. La adopción de tecnologías como el 5G y la Blockchain,[2] están redefiniendo la forma en que las personas interactúan con el mundo digital.

Al mismo tiempo que la nación asiática enfrenta el reto de equilibrar el crecimiento tecnológico con la sostenibilidad y la equidad social, desarrolla como uno de los pilares fundamentales de su política gubernamental, la estrategia de ciberpotencia, entendida como la necesidad de desarrollar una estructura digital robusta, que desarrolle la tecnología cuántica, la IA y sus derivaciones, hacia el mayor desarrollo posible de todas las áreas implicadas en la defensa del ciberespacio.

En IA se ha posicionado como líder global, con empresas como Baidu, Alibaba y Tencent a la vanguardia de la investigación. En el ámbito de la big data, ha aprovechado su vasta población y la proliferación de dispositivos conectados, para recopilar y analizar cantidades masivas de información, lo que ha mejorado la eficiencia en sectores como el transporte y la planificación urbana.

El ciberespacio es vulnerable ante amenazas como ciberataques, espionaje digital y guerra cibernética. Ante esas posibilidades, la computación cuántica ofrece herramientas para fortalecer la seguridad cibernética.

En la era digital actual, la computación cuántica y el ciberespacio se han convertido en dos de los cimientos fundamentales para el desarrollo tecnológico y la seguridad nacional. China, como una de las potencias globales en innovación tecnológica, ha invertido significativamente en ambas áreas, reconociendo su potencial para transformar la economía, la defensa y la sociedad.

La computación cuántica: un nuevo paradigma tecnológico

La computación cuántica representa un salto revolucionario en la capacidad de procesamiento de información. A diferencia de las computadoras clásicas, que utilizan *bits* para representar datos como 0 o 1, las computadoras

2 Blockchain es una tecnología de registro distribuido que permite almacenar información de manera segura, transparente y descentralizada. Consiste en una cadena de bloques enlazados entre sí, donde cada bloque contiene un conjunto de transacciones o datos verificados. Esos bloques están conectados mediante técnicas criptográficas.

cuánticas emplean qubits, que pueden existir en múltiples estados simultáneamente, gracias al fenómeno de superposición cuántica. Eso permite resolver problemas complejos en un espacio de tiempo muy veloz, a diferencia de las computadoras tradicionales, que demorarían períodos prolongados.

China incrementa su rol de líder global en la investigación y desarrollo de la computación cuántica. En 2020, el país logró un hito histórico, al demostrar la supremacía cuántica con su computadora Jiuzhang, capaz de realizar, en minutos, cálculos que tomarían miles de años a las supercomputadoras más avanzadas. No solo se posiciona China así en la vanguardia de la tecnología cuántica, sino que representa también implicaciones profundas para el ciberespacio.

En cuanto a sus avances en esa área, ha logrado hitos significativos, como el desarrollo de redes de comunicación a larga distancia; ejemplo de lo cual es la red troncal Beijing-Shanghai.[3]

La vinculación entre esos elementos se manifiesta en varias áreas clave:

1. *Criptografía cuántica y seguridad cibernética.*

Uno de los impactos más significativos de la computación cuántica en el ciberespacio, es su capacidad para revolucionar la criptografía. Los algoritmos cuánticos tienen el potencial de romper los sistemas de encriptación actuales, que son la base de la seguridad en línea, lo que representa una amenaza para la infraestructura crítica, las transacciones financieras, y las comunicaciones seguras.

Ante ese desafío, China ha invertido en el desarrollo de la criptografía cuántica, particularmente en la Distribución de Claves Cuánticas (QKD, por sus siglas en inglés). En 2016, China lanzó el primer satélite cuántico del mundo, Micius, que demostró la viabilidad de la comunicación cuántica segura a largas distancias. Ese avance sienta las bases para una red de comunicación global invulnerable a los ataques cibernéticos tradicionales.

2. *Inteligencia Artificial y análisis de datos.*

La computación cuántica tiene el potencial de acelerar el desarrollo de la IA, y el análisis de grandes volúmenes de datos. En el ciberespacio, eso se traduce en una mayor capacidad para detectar patrones, predecir amenazas y optimizar redes.

La República Popular China, que ya es un líder en IA, cuenta con la posibilidad de utilizar la computación cuántica para fortalecer su dominio en el ciberespacio, tanto a nivel nacional como internacional.

Las redes cuánticas permiten la transmisión de información con un nivel de seguridad sin precedentes, lo que refuerza el liderazgo chino, al fortalecer su posición en el ciberespacio y promover sus estándares tecnológicos a nivel internacional

La computación cuántica ofrece ventajas estratégicas. Podría ser utilizada para desarrollar armas cibernéticas más sofisticadas, capaces de desactivar sistemas enemigos. Cuenta con la capacidad de desarrollar las defensas cibernéticas, protegiendo de ataques la infraestructura crítica. China ha integrado la computación cuántica en su estrategia de defensa nacional, reconociendo su importancia para mantener la superioridad en el ciberespacio.

3. *Desafíos y consideraciones éticas.*

La carrera tecnológica global por parte de potencias, como los Estados Unidos, es una de las variables de ese desafío lo que podría exacerbar las tensiones geopolíticas.

Existen preocupaciones éticas sobre el uso de la computación cuántica en el ciberespacio. El poder de esa tecnología ha sido utilizado para fines maliciosos como el espionaje, ciberataques o la manipulación de información, sobre todo por las potencias adversas a China.

A medida que se desarrolla la tecnología cuántica, se aprecia que existe una mayor integración de sus elementos con el ciberespacio, impulsando innovaciones en campos como la comunicación segura, la IA y la

3 Importante línea ferroviaria de alta velocidad en China, que conecta las ciudades de Beijing y Shanghai. Conocida como el Ferrocarril de Alta Velocidad, es una de las más transitadas y estratégicas. Inaugurada el 30 de junio de 2011, cubre una distancia aproximada de 1318 km.

defensa nacional. El éxito de China en esas áreas tendrá implicaciones globales, redefiniendo el futuro de la tecnología y la seguridad en el actual siglo, hacia necesarios y primordiales objetivos de desarrollo económico, político y social.

China ha reconocido la importancia del ciberespacio como un campo de batalla moderno, y ha desarrollado normativas y estrategias para proteger sus intereses en ese dominio, estableciendo leyes que exigen a las empresas y organizaciones implementar fuertes medidas de seguridad y reportar incidentes de ciberseguridad.

En tal sentido, es reconocido el potencial de la computación cuántica para transformar la defensa y la seguridad nacionales; se ha dedicado esa computación a la simulación de conflictos y al análisis de escenarios complejos en el ámbito militar.

El rápido desarrollo de la Internet de las cosas plantea desafíos. La interconexión de dispositivos crea vulnerabilidades, que pueden ser explotadas por ciberataques a redes eléctricas y sistemas de transporte, entre otros, lo que podría tener consecuencias devastadoras.

China reconoció esos riesgos e implementó medidas para fortalecer la seguridad cibernética. En 2017, el gobierno promulgó la Ley de Ciberseguridad, que establece requisitos estrictos para la protección de datos y la seguridad de las redes.

En el aspecto comunicacional, las autoridades se han esmerado en que se conozcan, no solo las posibilidades tecnológicas de esa nación, sino tambien los elementos de su cultura. Plataformas como TikTok (conocida como Douyin), han ganado popularidad mundial, convirtiéndose en vehículos para contrarrestar narrativas negativas en los medios occidentales. Ese enfoque ha encontrado eco en otros países, especialmente en los del denominado Sur Global, con los que China ha establecido alianzas estratégicas en el ámbito tecnológico.

4. *El ciberespacio y la soberanía cibernética china.*

La soberanía cibernética, se refiere a que cada nación tiene el derecho y la responsabilidad de ejercer control sobre su ciberespacio, protegiendo su infraestructura digital, regulando el flujo de información, y defendiendo sus intereses nacionales en el ámbito digital. Para China, ese concepto es fundamental en su enfoque de gobernanza de Internet, y se alinea con una visión de Internet regulada y segura.

En síntesis, se define la soberanía cibernética como una condición, en la que el Estado tiene autoridad sobre el ciberespacio dentro de sus fronteras, incluyendo la capacidad de regular el acceso a Internet, controlar el contenido en línea y proteger la infraestructura digital.

Se basa en la premisa de que, el ciberespacio, es un dominio estratégico que debe ser gestionado para garantizar la seguridad nacional, la estabilidad social y el desarrollo económico.

Entre sus principios clave se encuentran:

Control estatal: El gobierno chino ejerce control estricto sobre las infraestructuras de Internet y de los contenidos en línea.

Seguridad Nacional: La protección del ciberespacio se considera una extensión de la defensa nacional.

Regulación del Contenido: Se implementan medidas para filtrar información considerada perjudicial, o contraria a los intereses del Estado.

Autonomía tecnológica: China busca reducir su dependencia de tecnologías extranjeras y promover el desarrollo de soluciones locales.

Marco legal y político

Ley de Ciberseguridad (2017): Establece normas para la protección de datos, la seguridad de la infraestructura y la regulación del contenido en línea.

Sobre las aplicaciones prácticas de la soberanía cibernética china, está la posibilidad de ejercer la vigilancia, o sea, el uso de tecnologías avanzadas para monitorear y controlar el flujo de información:

Promoción de plataformas locales: Fomento de alternativas chinas a servicios globales (ejemplo: Wechat en lugar de WhatsApp, Baidu en lugar de Google).

Desarrollo de estándares tecnológicos: Creación de normas propias para tecnologías como el 5G y la Internet de las cosas, con el fin de reducir la dependencia de los estándares internacionales.

Implicaciones Internacionales

Modelo alternativo de gobernanza: China promueve su enfoque de soberanía cibernética como una alternativa al modelo occidental de Internet abierto y libre.

Influencia global: Por medio de iniciativas como la Ruta de la Seda Digital, China brinda la posibilidad de ampliar su modelo de gobernanza digital y tecnologías a otros países.

Tensiones internacionales: Disputas con otros países por el control de tecnologías críticas y la influencia en el ciberespacio global.

Equilibrio entre seguridad e innovación: El control estricto puede limitar la creatividad y el emprendimiento en el sector tecnológico.

La soberanía cibernética es un eslabón importante de la estrategia digital china, reflejando su enfoque de control estatal y de seguridad nacional en el ciberespacio. Ese concepto ha permitido que la nación asiática desarrolle un modelo único de gobernanza digital, caracterizado por la regulación, la promoción de tecnologías locales, y la proyección de influencia global.

Gobernanza de Internet

China ha adoptado un enfoque único hacia la gobernanza de Internet, basado en el principio de soberanía nacional. A diferencia del modelo de Internet abierto, promovido por los Estados Unidos, el país asiático defiende un modelo en el que cada nación tiene el derecho de regular y controlar su propia infraestructura de Internet. Ese enfoque se refleja, entre otros aspectos, en la adopción de políticas que restringen el acceso a sitios webs extranjeros, en defensa del contenido propio de sus intereses.

Ha promovido iniciativas internacionales para establecer normas de gobernanza digital que respalden su visión de soberanía cibernética. Un ejemplo lo constituye el "Código de Conducta para la Seguridad de la Información Internacional", presentado ante la Organización de Naciones Unidas (ONU), y que aboga por el respeto a la soberanía nacional en el ciberespacio, y por la no interferencia en los asuntos internos de otros países.

Como respuesta a las amenazas percibidas de los Estados Unidos y otras potencias, China fortaleció las capacidades defensivas en el ciberespacio. Una de las iniciativas más importantes es la creación de una unidad, perteneciente al Ejército Popular de Liberación, especializada en operaciones cibernéticas.

Denunció las actividades de vigilancia de la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en inglés). La rivalidad promovida por los Estados Unidos, obedece al desarrollo acelerado chino en el tratamiento de redes, y a la proliferación de empresas como Huawei, líderes globales en tecnología.

El país asiático ha pretendido contrarrestar la influencia estadounidense en el ciberespacio, mediante alianzas estratégicas con otros países, a la vez que busca la armonía diplomática y tecnológica. Ha colaborado con Rusia en políticas conjuntas de ciberseguridad, y ha desarrollado su visión de gobernanza de Internet en foros internacionales, como la Organización de Cooperación de Shanghai (OCS).

La agresividad estadounidense en el ámbito digital por intentar contrarrestar el avance chino, podría llevar a una fragmentación de la tecnología de la Información, sobre todo en cuanto a la trasmisión de datos, como parte de la cual, diferentes regiones pudieran adoptar estándares y regulaciones contradictorias.

Ese escenario conocido como "Balcanización de Internet", traería consecuencias negativas para la innovación y la cooperación internacional, razón por la cual China se empeña, desde sus propias políticas internas, y en los foros internacionales, por el mantenimiento de un equilibrio en cuanto al empleo del ciberespacio internacional, y a la manera efectiva en que se deben abordar las tecnologías digitales.

Mientras algunos políticos y académicos (Friedberg, Pillsbury) intentan argumentar que el poder económico y militar chino devendrá en una China irracional, en cuanto al uso del ciberespacio, otros (Shaambaugh, Steinfeld) defienden que China está cada vez más integrada a las instituciones internacionales y a la economía global. Subrayan, además, la creciente y sostenida preocupación del gobierno chino por la estabilidad internacional.

Las autoridades chinas han tenido la oportunidad de hacer valer que, salvo el afán agresivo estadounidense, existen intereses comunes entre ambas naciones, en cuanto a la defensa del ciberespacio y la ciberseguridad.

Para los dos países, el mantenimiento de la ciberseguridad es vital para la estabilidad y el desarrollo social. Sus enfoques estratégicos se cimentan en la satisfacción de sus intereses nacionales, por lo que los respectivos gobiernos enarbolan sus estrategias acerca del ciberespacio, como arquetipos a emular.

Tanto China como los Estados Unidos, consideran que la información estratégica debe ser manejada cuidadosamente, para el buen funcionamiento de la administración pública y la seguridad nacional. China apoya la perspectiva estadounidense sobre un enfoque de gobernabilidad de la ciberseguridad, que pone el peso de la implementación y ejecución de tareas y responsabilidades, bajo un esquema de múltiples partes interesadas (multistakeholder approach), entre agentes gubernamentales, privados civiles y militares.

Determinados sectores reaccionarios en los Estados Unidos se esmeran en apartar las posibilidades de entendimiento común. En 2018, el Departamento de Justicia estadounidense promulgó la "Iniciativa China", para contrarrestar lo que se percibió como actividades de espionaje económico y robo de propiedad intelectual, supuesta y fundamentalmente por los ciudadanos estadounidenses de origen chino.

Esa Iniciativa tuvo varias repercusiones geopolíticas:

1. Tensión en las relaciones sino-estadounidenses: Considerada una medida discriminatoria, encaminada solamente a contener el ascenso económico y tecnológico chino.
2. Impacto en la cooperación bilateral: Aumentó la desconfianza, afectando áreas de cooperación como el comercio, la inversión y la colaboración en ciencia y tecnología.
3. Preocupaciones sobre derechos civiles: Criticada por grupos defensores de los derechos humanos y por académicos, ya que apuntaba discriminatoriamente hacia estadounidenses de origen chino, lo que provocó que investigadores y académicos de ascendencia china sintieran un clima de miedo y autocensura, lo que provocó, en algunos casos, la pérdida de colaboraciones internacionales.

En 2021, la administración de Joe Biden anunció el fin de esa iniciativa, reconociendo lo improcedente y las críticas, pero en 2023, surgieron nuevamente denuncias que involucraron a ciudadanos chinos acusados, en ese caso, de estimular el sobrevuelo de supuestos globos espías sobre el espacio aéreo de instalaciones militares de los Estados Unidos.

Una campaña difamatoria pretendía crear una chinofobia, los medios de comunicación una vez más se prestaron para ello. Mientras el Ministerio de Relaciones Exteriores chino planteaba desconocer el asunto, en los Estados Unidos, el presidente llamaba a la presidencia de la Junta de jefes del Estado Mayor Conjunto a deliberar, y movilizó, entre otras importantes fuerzas del componente estratégico, al Comando Cibernético (US CyberCom).

Varios analistas de inteligencia estadounidenses, entre ellos Christopher Johnson, reconocieron que los Estados Unidos espían a China; la chinofobia persiguió el objetivo de justificar, ante la opinión pública, la búsqueda de información vital por los Estados Unidos, acerca de los intereses estratégicos de China, fundamentalmente, de aquellos vinculados con la transformación digital y el ciberespacio.

En 2024, el ejecutivo de la nación norteña anunció que, para 2025, incrementaría en dos veces los aranceles sobre los semiconductores chinos, incrementando las acusaciones acerca de que Beijing fuerza la transferencia de tecnología, y roba la propiedad intelectual.

Consideraciones finales

El ciberespacio y la gobernanza digital forman parte de una guerra, a partir de la especial dimensión cultural de la hegemonía del poder contemporáneo, la que se aviva ante los nexos existentes entre medios de comunicación y cultura, y su influencia sobre el conjunto de las relaciones de dominación. Se mantiene la guerra fría, en términos de lucha por la mente de los individuos, a la vez que resalta su carácter ideológico (Expósito, 2022).

Con el desarrollo de las ciencias, la guerra psicológica se ha desarrollado gracias, en parte fundamental, a las nuevas tecnologías de la información y las comunicaciones.

Ante la fuerte injerencia estadounidense, se identifica a la guerra psicológica, en relación muy especial, con la justificación para dominar el ciberespacio, como una guerra también política, entendida como diplomacia de crisis, guerra de nervios o diplomacia de intimidación dramática, con lo que la nación norteamericana se empeña en contraponerse al notable avance chino en el desarrollo económico comercial, y específicamente tecnológico.

Para cumplir con los fines anteriores, el directorio de Inteligencia de los Estados Unidos contrata a consultores de relaciones públicas, a cargo de operaciones psicológicas complejas, en el ámbito de la información comunicacional.

Una de las tareas fundamentales, validar que, en la producción de la información con fines propagandísticos, las estrategias y tácticas de la comunicación militar, se vinculan y simultáneamente se hacen partícipes de las formas de operación mediática, en la que los medios funcionan como empresas oligopólicas.

Información según los aparatos de inteligencia estadounidense, como búsqueda de contenidos, para convencer a la opinión pública, sin importar la veracidad (ejemplo: las continuas acusaciones a supuestos espías chinos en el interior de los Estados Unidos).

Comunicación como promoción de los intereses del que comunica, o sea, la manera efectiva de lograr que un mensaje, con un interés puramente propagandístico, se apegue a los intereses políticos, a conveniencia de lo que dicten el ejecutivo, y las empresas transnacionales de la comunicación en los Estados Unidos, sin dejar de analizar los intereses propios y particulares del departamento de Estado y del departamento de Defensa.

Con un mensaje "prefabricado" se menciona al ciberespacio (concepto aún no completamente tenido en cuenta por el ciudadano común), como elemento de estímulo al desarrollo de diferentes programas relacionados con el ciberespacio en los Estados Unidos: Cicada; Trippwire, entre otros. Y la República Popular China se convierte, por tanto, en el sujeto del experimento social estadounidense, por medio del cual ese sujeto, mediante la explotación, muchas veces falsificada, facilita el enriquecimiento de las citadas grandes empresas transnacionales de la comunicación, una de las formas que desarrollan los Estados Unidos para mantener su hegemonía.

Las autoridades estadounidenses, en su labor conjunta con el sector corporativo, defienden, hasta ahora sin el éxito esperado, el traslado de la informatización de las redes hacia el multidominio, entendido desde la Tierra, hasta el espacio y el ciberespacio. Y que esto se produzca mediante una interrelación estrecha de los elementos que lo componen, para lo cual se necesita entrenar al componente técnico y logístico correspondiente.

Las limitaciones impuestas por los Estados Unidos a la industria de semiconductores chinos, tiene el objetivo evidente de obstaculizar a China en su desarrollo, puesto que la nación asiática depende aún, en alguna medida, de determinado componente de fabricación estadounidense o de los aliados, por lo que las restricciones impuestas mediante las Leyes CHIPS y Science Act, de 2022, limitan el acceso chino a tecnologías avanzadas de fabricación de chips, como los equipos de Litografía Ultravioleta Extrema (LUVE), necesarios para producir chips de última generación.

Téngase en cuenta que, los chips y el ciberespacio chino, tienen una relación estrecha, ya que los chips son componentes fundamentales para la infraestructura tecnológica que sostiene el ciberespacio. En síntesis, son la base tecnológica que permite el funcionamiento, la expansión y la seguridad del ciberespacio chino, y su desarrollo es estratégico para la autonomía y la competitividad china en el ámbito digital global.

La vinculación entre el aspecto comunicacional y el ciberespacio en la República Popular China, es un reflejo de su modelo de desarrollo, y de su visión de gobernanza. Promueve la cohesión social.

Por medio de la utilización de tecnologías avanzadas y la implementación de políticas, China ha logrado mantener un alto nivel de control sobre su entorno digital, promoviendo así sus intereses nacionales.

La estrategia de seguridad y defensa de China en cuanto al ciberespacio, refleja su interés de convertirse en una potencia global en el ámbito digital. Mediante un enfoque basado en la soberanía nacional, China busca proteger sus intereses y contrarrestar las amenazas de los Estados Unidos y otras potencias.

En un mundo cada vez más interconectado, es necesario que las naciones encuentren formas de cooperación en el ámbito de la ciberseguridad, estableciendo normas y estándares que promuevan la estabilidad y la confianza en el ciberespacio. China, como una de las principales potencias digitales, mantiene su compromiso en el papel crucial que puede desempeñar, por un equilibrio del orden internacional.

La relación entre la computación cuántica, el ciberespacio, y las normativas militares chinas de seguridad y defensa, es compleja y multifacética. La computación cuántica tiene el potencial de revolucionar la forma en que se procesa la información, y se protege la seguridad, China ha sido pionera en la integración de la computación cuántica en sus estrategias de seguridad y defensa, lo que tiene implicaciones importantes para la seguridad global.

La iniciativa Internet plus constituyó un catalizador clave para la transformación digital de China, posicionando al país como líder global en innovación tecnológica.

Al mencionarse la estrecha interdependencia entre el ciberespacio y la computación cuántica, podemos percatarnos de cómo las tecnologías emergentes están transformando al mundo. China ha demostrado un compromiso sólido con el desarrollo de la computación cuántica, reconociendo su potencial para fortalecer su posición en el ciberespacio, y por las implicaciones globales que redefinirán el futuro tecnológico y la seguridad en el siglo XXI.

El ciberespacio viene convirtiéndose, desde hace años, en parte del contenido ignoto de la propaganda desatada por lo que se denomina gran prensa, o sea, es utilizado, no solo como ente importante que se debe proteger a favor de la soberanía y la seguridad de las naciones, sino también como elemento de *show* mediático, con vistas a ubicar en esa prensa el contenido de los mensajes deseados por los ejecutivos políticos y económicos de naciones como los Estados Unidos, en las que, unido a la real necesidad de defenderlo, como elemento intrínseco de la estabilidad político-social, también el ciberespacio es utilizado como vehículo para justificar cuantiosas sumas de dinero, que se aportan en nombre de la integridad nacional, y que en realidad pasan a engrosar las arcas del Complejo Militar Industrial.

Referencias bibliográficas

Expósito, J. (2022, enero 19). China en el ciberespacio. Revista Ejércitos. http://www.ejercitos.com

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

Lewis, J. A. (2022). Chinas Cyber Strategy: A Comprehensive Analysis. Center for Strategic and International Studies. En www.centerforstrategicstudies.

Ministerio de Defensa Nacional de la República Popular China (2023). Libro Blanco de Defensa Nacional. Beijing: Editorial del Pueblo.

Patiño Orozco, G. A. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. OASIS, 34, pp. 107-126. https://doi.org/10.18601/16577558.n34.07

Perera Pena, E. "El llamado globo chino y algunas de sus derivaciones estratégicas". En Revista *Cuadernos de Nuestra América*. CIPI. La Habana. Cuba. ISSN: 2959-9849.

Pillsbury, M. (2015). The Hundred Year Marathon. Chinas Secret Strategy to Replace Americas as the Global Superpower. Nueva York: Henry Holt.

Segal, A. (2020). The Hacked World Order:How Nations Fight, Trade, Manueuver, and Manipulate in the Digital Age. New York.Public Affairs.

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

Spanish.news.cn 16.3.2023. *Libro Blanco*. China explora activamente nuevos modelos de "ciberjusticia". En: www.spanish.xinhunet.com

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

Zhang, L. (2021). Chinas Quantum Supremacy. Beijing: Tsinghua University Press.