El Quinto Dominio en Disputa

La rivalidad entre China y Estados Unidos por el control del ciberespacio

Resumen ejecutivo

El ciberespacio se ha consolidado como el quinto dominio de la guerra, un escenario transversal a los dominios terrestre, marítimo, aéreo y espacial, cuya disputa define hoy la rivalidad estratégica entre la República Popular China y los Estados Unidos. Se trata de una rencilla que, lejos de reducirse a una cuestión tecnológica, se ha convertido en una pugna multidisciplinar, abarcando desde dimensiones geopolíticas y económicas hasta cuestiones legislativas o cognitivas. Ambas potencias han desarrollado estrategias nacionales diferenciadas. Washington mantiene una ciberdefensa activa de colaboración público-privada mientras Pekín ejerce un control centralizado del ciberespacio como extensión de su soberanía nacional. Entre los principales instrumentos destacan el ciberespionaje, los ataques a infraestructuras críticas y las campañas de desinformación. El presente artículo analiza dichas estrategias, así como los marcos normativos y las herramientas de influencia cibernética que ambas potencias utilizan. Así, se pretende identificar las implicaciones de esta rivalidad para la seguridad internacional y, para finalizar este escrito, se formulará una conclusión con recomendaciones orientadas a reducir los riesgos inherentes a este entorno.

Introducción

La geopolítica en la actualidad ha sido fruto de transformaciones irreversibles. Esto es así debido a la conexión digital que envuelve al conjunto de la sociedad contemporánea. Todo ello ocurre en un entorno artificial y multidimensional, generado por ordenadores a escala global: el ciberespacio. Dicha novedad ha resultado en un nuevo tipo de confrontación entre Estados, escapando a las categorías tradicionales del conflicto[1]. No existe contacto físico directo, la atribución de responsabilidades resulta sumamente compleja y las reglas convencionales de soberanía pierden eficacia en un escenario sin fronteras claramente delimitadas.

El Estado Mayor Conjunto de los Estados Unidos reconoció por primera vez el ciberespacio como un dominio de conflicto en su Estrategia Militar Nacional para Operaciones en el

[1]Benedikt, M. (Ed.). (1991). *Cyberspace: First steps*. MIT Press; Center for Strategic and International Studies. (2025). *Significant Cyber Incidents Since 2006*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-02/250210_Cyber_Events.pdf

Ciberespacio de 2006[2], y la OTAN lo incorporó formalmente en la Cumbre de Varsovia de 2016, equiparando los ciberataques en potencial dañino a los ataques convencionales[3]. Desde entonces, la competición entre China y Estados Unidos ha ido articulando, de manera progresiva y letal, una rivalidad que busca incidir de manera directa en la economía, instituciones, y seguridad colectiva de sus enemigos y aliados. Esto ha dado como resultado un notorio impacto en el conjunto del entramado internacional y en el equilibrio de poder global. Como el presente artículo reúne a dos potencias de modelos estratégicos diferenciados, se analizarán las técnicas que emplean para así comprender las implicaciones de esta rivalidad para la seguridad internacional.

El Ciberespacio como Escenario Estratégico

A modo de contexto, a lo largo de la historia, los escenarios donde se llevan a cabo todas las operaciones necesarias para lograr determinados objetivos se conocen como dominios, y antiguamente se dividían en el dominio terrestre, marítimo, aéreo y espacial, coincidiendo como espacios físicos per se. En la actualidad esta concepción fue revisada y se incluyeron el cognitivo y el ciberespacio, siendo este último el «transdominio» de la guerra moderna: un entorno que supera las fronteras físicas convencionales y que repercute, de forma simultánea, en los demás para amplificar las capacidades estratégicas de los actores que lo dominan[4]. Su especificidad radica en que los actores que lo habitan pueden actuar de forma anónima, beneficiándose de la denominada «denegación plausible», es decir, la capacidad de perpetrar ciberataques eludiendo la atribución de responsabilidades[5].

Las Amenazas Persistentes Avanzadas (APTs) suponen la amenaza por antonomasia, operaciones cibernéticas de alto perfil, coordinadas y financiadas por actores estatales, cuyo objetivo abarca tanto grandes corporaciones como instituciones militares y gubernamentales[6]. La sofisticación creciente de estas operaciones, que combinan técnicas de ciberespionaje,

---

[2]Chairman of the Joint Chiefs of Staff. (2006). *National Military Strategy for Cyberspace Operations*. National Security Archive. https://nsarchive.gwu.edu/document/21419-document-23

[3] NATO. (2016). Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.

[4]García Servert, R., y Calvo Albero, J. L. (2022). El dominio cognitivo en las operaciones multidominio: concepto y problemática. *Academia de las Artes y las Ciencias Militares*, 17. https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf

[5]Torres Soriano, M. R. (2017). Guerras por delegación en el ciberespacio. *Revista del Instituto Español de Estudios Estratégicos*, 9, 17-33.

[6]Hussain, S., Maaz, A., y Uddin Ghouri, S. S. (2020). Advanced Persistent Threat: A systematic review of literature and meta-analysis of threat vectors. https://doi.org/10.1007/978-981-15-4409-5_15

vulnerabilidades de día cero y campañas de desinformación, ha transformado el ciberespacio en el campo de batalla determinante del siglo XXI.

Dos Modelos, una Misma Ambición

Por un lado, China ha construido un modelo de gobernanza digital caracterizado por el control centralizado y la soberanía cibernética, pues Pekín concibe el ciberespacio como una extensión de su propia soberanía nacional, así como una herramienta de disuasión y control interno. Esta visión se consolidaría en 2014, cuando el dirigente Xi Jinping presentó el concepto de "gran potencia cibernética" (网络强国 - *wǎngluò qiángguó*), orientando la estrategia del Partido Comunista Chino (PCCh) hacia el desarrollo tecnológico autónomo y la restricción de tecnologías extranjeras en sectores sensibles como las telecomunicaciones[7]. La conocida Gran Muralla cibernética es la expresión más visible de esta arquitectura de control. Se trata de un entramado de filtrado y censura que bloquea el acceso a plataformas extranjeras como Google, Facebook o Twitter (X), y que obliga a las empresas tecnológicas que operan en territorio chino a almacenar los datos de sus usuarios dentro de las fronteras del país, reforzando así la capacidad del Estado para controlar información que circula por la red.

Estados Unidos, por su parte, posee una concepción más abierta y liberal sobre el ciberespacio, sustentada en la colaboración público-privada y la transparencia institucional. Su Estrategia de Defensa Nacional de 2022 identifica a China como el principal desafío para la seguridad nacional, reconociendo que las capacidades cibernéticas chinas amenazan la operatividad de sus Fuerzas Armadas[8]. Frente a ello, Washington ha articulado una ciberdefensa activa en torno a organismos como el *United States Cyber Command* (USCYBERCOM), la NSA y la *Cybersecurity and Infrastructure Security Agency* (CISA), junto con iniciativas de coordinación como el *Joint Cyber Defense Collaborative* (JCDC) y el *Joint Ransomware Task Force* (JRTF).

Esta contraposición que se observa a nivel tecnológico representa de manera clara la divergencia estructural entre dos modelos políticos y económicos irreconciliables. Asimismo, la guerra comercial, iniciada en 2025 y caracterizada por sanciones y barreras arancelarias cruzadas sobre productos tecnológicos, pone de manifiesto que la lucha en el ciberespacio y la competición tecnológica son dimensiones inseparables de una misma rivalidad estructural[9]. Ambas

[7]Doshi, R., De la Bruyère, E., Picarsic, N., y Ferguson, J. (2021). *China como una «gran potencia cibernética»: las dos voces de Pekín en las telecomunicaciones*. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_China_cyber_power_Spanish.pdf

[8]U.S. Department of Defense. (2022). *National defense strategy of the USA*. https://media.defense.gov

[9]Márquez de la Rubia, F. (2025). La batalla por la supremacía tecnológica: EE. UU. vs China. *Panorama Geopolítico de los Conflictos*, 11, 311-338. https://www.defensa.gob.es/documents/2073105/2361682/PGC2024_Capitulo12.pdf

competiciones se entrelazan en lo referente al control sobre tecnologías clave como semiconductores, inteligencia artificial, o redes de quinta generación, pues son clave para influir en la arquitectura global de Internet y explotar vulnerabilidades en su propio beneficio.

Marco Normativo: Dos Concepciones del Ciberespacio

El dilema regulatorio del ciberespacio radica en su naturaleza intangible por las ventajas que presenta: los actores actúan de forma encubierta, la atribución es difícil y las normas internacionales comunes son prácticamente inexistentes. A nivel nacional, ambas potencias han desarrollado marcos legislativos que reflejan sus respectivas concepciones estratégicas respecto a dicha temática. China promulgó en 2017 su Ley de Ciberseguridad (网络安全法 - *wǎngluò ānquán fǎ*), orientada a garantizar la soberanía del ciberespacio y la seguridad nacional. Esta norma se complementa con la Ley de Seguridad de Datos (DSL) y la Ley de Protección de Información Personal (PIPL), ambas en vigor desde 2021, y con el Reglamento sobre Gestión de la Seguridad de los Datos de la Red, vigente desde 2025[10]. En la cúspide institucional se sitúa la Comisión Central de Asuntos del Ciberespacio, presidida por el propio Xi Jinping. En el plano operativo, el Ejército de Liberación Popular estableció en 2024 la Fuerza de Apoyo a la Información (ISF) y la Fuerza Cibernética (CSF), dedicadas respectivamente al soporte informativo y a las operaciones activas en el ciberespacio[11].

El marco estadounidense se articula en torno a la *Cybersecurity Information Sharing Act* y la *Federal Information Security Modernization Act*, que regulan la colaboración entre el sector privado y las agencias federales en materia de amenazas cibernéticas y las evaluaciones periódicas de seguridad, respectivamente[12].

A estas se añaden órdenes ejecutivas como la EO 14028 del presidente Biden[13], orientada a reforzar la seguridad de las redes federales. La diferencia fundamental entre ambos modelos no reside únicamente en los instrumentos normativos, sino en su orientación. Es decir, se observa a una China tajante en la regulación para ejercer control sobre sus fronteras y así impedir, en la

[10]Sack, S., Chen Zeng, K., y Webster, G. (2024). *Moving data, moving target: Uncertainties remain in China's overhauled cross-border data transfer regime*. Cyber Security Center of Stanford, DigiChina. https://digichina.stanford.edu/

[11]Nouwens, M. (2024). *China's new Information Support Force*. The International Institute for Strategic Studies. https://www.iiss.org

[12] Congressional Record, Volume 161, Number 155. (2015, 22 de octubre). https://www.gpo.gov

[13] The White House. (2021, 12 de mayo). *Executive Order 14028: Improving the Nation's Cybersecurity* https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf

medida de lo posible, que existan brechas que el enemigo pueda explotar[14]. Estados Unidos, en contraposición, busca su propia regulación para proteger y habilitar la colaboración, permitiendo que las empresas puedan aportar su conocimiento y que, a la par, se encuentren amparadas bajo la misma seguridad cibernética.

Tácticas de Influencia Cibernética: Espionaje y Desinformación

Lejos de limitarse a una cuestión de servidores y algoritmos, la ciberguerra deja rastros concretos, medibles y devastadores. Se observa, por ejemplo, con el espionaje cibernético, que utiliza la red como un medio enormemente eficaz y difícilmente rastreable. Entre 2006 y 2011, una operación china de cinco años bautizada como *Shady RAT* penetró de forma silenciosa en 72 instituciones y corporaciones estadounidenses, extrayendo secretos de Estado y propiedad intelectual de alto valor sin que sus responsables pudieran ser señalados con certeza jurídica[15]. Una década más tarde, el grupo *Silk Typhoon* explotó vulnerabilidades de día cero en *Microsoft Exchange Server* para acceder remotamente a decenas de miles de servidores gubernamentales y comerciales de todo el mundo[16]. La sofisticación de estas operaciones apunta a una estrategia deliberada de largo plazo, orientada a acumular información que otorgue ventaja política, militar y económica.

Así, haciendo alusión al bando contrario de la contienda, en septiembre de 2022, China denunció que la NSA había perpetrado ciberataques contra la Universidad Politécnica del Noroeste, y en febrero de 2025 acusó a tres agentes identificados de esa misma agencia de atacar infraestructuras críticas durante los Juegos Asiáticos de Invierno[17]. Independientemente de la verificación de estas acusaciones, pues se encuentran sometidas a la opacidad que caracteriza al quinto dominio, su mera formulación pública evidencia que ambas potencias han normalizado el ciberespacio como escenario de operaciones encubiertas contra el adversario.

Otra táctica de gran uso y efectividad que conviene destacar es la desinformación. A diferencia de un ciberataque a una infraestructura, cuyo daño puede medirse en horas de servicio perdidas

---

[14] National People's Congress of the People's Republic of China. (2016, November 7). *Cybersecurity Law of the People's Republic of China.* https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

[15]Center for Strategic and International Studies. (2025). *Significant Cyber Incidents Since 2006*. https://l1nq.com/9wd3qj4

[16]Microsoft Threat Intelligence. (2025, 5 de marzo). *Silk Typhoon targeting IT supply chain*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

[17]Xinhua. (2025). Chinese police put 3 U.S. operatives on wanted list over cyberattacks. *Xinhua News Agency*. https://english.news.cn/20250415/e7acc3bf9c404e1db06f2bb678d8e98f/c.html

o datos robados, la manipulación informativa actúa sobre la percepción colectiva de la realidad[18]. La pandemia de COVID-19 ofreció al PCCh la oportunidad de desplegar esta estrategia a escala global. A través de redes de bots, diplomacia pública y medios estatales, Pekín construyó una narrativa paralela que exaltaba la eficacia de su modelo de gobierno frente al desorden democrático occidental, difundida precisamente en las plataformas que el propio régimen prohíbe dentro de sus fronteras[19]. Se observa de esta manera como China utiliza a su favor la apertura de Internet en Occidente como vector de influencia, mientras mantiene su propio espacio digital herméticamente cerrado.

TikTok forma parte de este juego cibernético. Según el *Global Engagement Center*[20], *ByteDance* mantiene listas internas para restringir el acceso a sus plataformas a personas consideradas críticas con el PCCh, convirtiendo una red social de entretenimiento en un mecanismo silencioso de control narrativo[21]. Estados Unidos, por su parte, en esta guerra de relatos actuó con la hipótesis del «Lab Leak» sobre el origen del virus, que fue promovida activamente a través de documentos oficiales, aun sin respaldo unánime de la comunidad científica internacional[22]. La línea entre información, persuasión y manipulación se vuelve deliberadamente borrosa, y es esa ambigüedad la que funciona como arma.

Conclusión y Recomendaciones

El individuo es, en última instancia, el principal afectado de la ciberguerra entre China y Estados Unidos. Cuando un ciberataque paraliza una red eléctrica o colapsa un sistema sanitario, es el ciudadano quien pierde acceso a servicios esenciales. Cuando una campaña de desinformación inunda sus redes sociales, es su percepción de la realidad la que se distorsiona. Cuando TikTok restringe contenidos o la NSA filtra datos masivamente, es su privacidad la que queda

---

[18]García Servert, R., y Calvo Albero, J. L. (2022). El dominio cognitivo en las operaciones multidominio: concepto y problemática. *Academia de las Artes y las Ciencias Militares*, 17. https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf

[19]Manantan, M. B. (2021). Unleash the Dragon: China 's strategic narrative during the COVID-19 pandemic. *The Cyber Defense Review*, 6(2), 71-90. https://www.jstor.org/stable/27021377

[20] Global Engagement Center. (2023). *How the People's Republic of China seeks to reshape the global information environment*. U.S. Department of State. https://www.state.gov/wp-content/uploads/2023/09/how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment_final.pdf

[21] García Servert, R., y Calvo Albero, J. L. (2022). El dominio cognitivo en las operaciones multidominio: concepto y problemática. Academia de las Artes y las Ciencias Militares. https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf

[22] U.S. House of Representatives, Select Subcommittee on the Coronavirus Pandemic. (2024). *After action review of the COVID-19 pandemic: The lessons learned and a path forward.* https://oversight.house.gov/wp-content/uploads/2024/12/2024.12.04-SSCP-FINAL-REPORT-ANS.pdf

comprometida. El quinto dominio atraviesa la pantalla de cada teléfono móvil y condiciona cada decisión cotidiana; por esta razón, su control y protección constituyen una prioridad ineludible para cualquier Estado en materia de seguridad nacional.

De este análisis se derivan tres líneas de actuación. En primer lugar, la dificultad estructural para atribuir un ciberataque exige avanzar hacia mecanismos internacionales de cooperación que reduzcan la impunidad en el quinto dominio, dado que la ausencia de normas comunes continúa siendo, como se ha señalado, uno de los principales obstáculos para una gobernanza compartida del ciberespacio. En segundo lugar, el modelo de colaboración público-privada articulado por organismos como el JCDC o el JRTF estadounidense demuestra que la coordinación interinstitucional resulta clave para proteger infraestructuras críticas, por lo que su fortalecimiento debería extenderse a otros actores internacionales expuestos a amenazas similares. Por último, frente a la sofisticación de las campañas de desinformación, resulta necesario reforzar la resiliencia institucional y la alfabetización digital de la ciudadanía, de modo que la opinión pública esté mejor preparada para discernir entre información veraz y manipulada.

Bibliografía

Benedikt, M. (Ed.). (1991). *Cyberspace: First steps*. MIT Press.

Center for Strategic and International Studies. (2025). *Significant Cyber Incidents Since 2006*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-02/250210_Cyber_Events.pdf

Chairman of the Joint Chiefs of Staff. (2006, diciembre). *National Military Strategy for Cyberspace Operations*. National Security Archive. https://nsarchive.gwu.edu/document/21419-document-23

Doshi, R., De la Bruyère, E., Picarsic, N., y Ferguson, J. (2021). *China como una «gran potencia cibernética»: las dos voces de Pekín en las telecomunicaciones*. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_China_cyber_power_Spanish.pdf

García Servert, R., y Calvo Albero, J. L. (2022). El dominio cognitivo en las operaciones multidominio: concepto y problemática. *Academia de las Artes y las Ciencias Militares*. https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf

Global Engagement Center. (2023). *How the People's Republic of China seeks to reshape the global information environment*. U.S. Department of State. https://www.state.gov/wp-content/uploads/

2023/09/how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment_final.pdf

Hussain, S., Maaz, A., y Uddin Ghouri, S. S. (2020). Advanced Persistent Threat: A systematic review of literature and meta-analysis of threat vectors. https://doi.org/10.1007/978-981-15-4409-5_15

Manantan, M. B. (2021). Unleash the Dragon: China's strategic narrative during the COVID-19 pandemic. *The Cyber Defense Review*, 6(2), 71-90. https://www.jstor.org/stable/27021377

Márquez de la Rubia, F. (2025). La batalla por la supremacía tecnológica: EE. UU. vs China. *Panorama Geopolítico de los Conflictos*, 11, 311-338. https://www.defensa.gob.es/documents/2073105/2361682/PGC2024_Capitulo12.pdf

Microsoft Threat Intelligence. (2025, 5 de marzo). *Silk Typhoon targeting IT supply chain*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

National People's Congress of the People's Republic of China. (2016, November 7). *Cybersecurity Law of the People's Republic of China*. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

NATO. (2016, 9 de julio). *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. https://www.nato.int/cps/ic/natohq/official_texts_133169.htm

Nouwens, M. (2024). *China's new Information Support Force*. The International Institute for Strategic Studies. https://www.iiss.org

Sack, S., Chen Zeng, K., y Webster, G. (2024). *Moving data, moving target: Uncertainties remain in China's overhauled cross-border data transfer regime*. Cyber Security Center of Stanford, DigiChina. https://digichina.stanford.edu/

The White House. (2021, 12 de mayo). *Executive Order 14028: Improving the Nation's Cybersecurity* https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf

Torres Soriano, M. R. (2017). Guerras por delegación en el ciberespacio. *Revista del Instituto Español de Estudios Estratégicos*, 9, 17-33.

U.S. Department of Defense. (2022). *National defense strategy of the USA*. https://media.defense.gov

U.S. House of Representatives, Select Subcommittee on the Coronavirus Pandemic. (2024). *After action review of the COVID-19 pandemic: The lessons learned and a path forward*. https://oversight.house.gov/wp-content/uploads/2024/12/2024.12.04-SSCP-FINAL-REPORT-ANS.pdf

Xinhua. (2025, 15 de abril). Chinese police put 3 U.S. operatives on wanted list over cyberattacks. *Xinhua News Agency*. https://english.news.cn/20250415/e7acc3bf9c404e1db06f2bb678d8e98f/c.html