Revista Iberoamericana de la Educación, Vol - 10 No. 2, April - June 2026
e-ISSN: 2737-632x
Pgs 238-251

Fronteras Digitales: Ciberseguridad, Soberanía y los Nuevos Paradigmas del Poder Geopolítico

Digital Frontiers: Cybersecurity, Sovereignty, and the New Paradigms of Geopolitical Power

Fronteiras Digitais: Cibersegurança, Soberania e os Novos Paradigmas do Poder Geopolítico

Juan Rigoberto Castillo Serracín*
Odessa Aranda*
Francisco Farnum Castro*
Javier Miguel Gómez Solís*

How to cite:
Castillo, J., Aranda, O., Farnum, F., Gómez, J. (2026). Fronteras Digitales: Ciberseguridad, Soberanía y los Nuevos Paradigmas del Poder Geopolítico. *Revista Iberoamericana De educación,* 9 (2).

http://www.revista-iberoamericana.org/index.php/es

* Universidad de Panamá, Panamá.
juan.castillos@up.ac.pa
https://orcid.org/0009-0006-5821-7028
** Universidad de Panamá, Panamá.
odessa.aranda@up.ac.pa
https://orcid.org/0000-0002-3698-1141
*** Universidad de Panamá, Panamá.
francisco.farnum@up.ac.pa
https://orcid.org/0000-0002-5879-2296

**** Universidad de Panamá, Panamá.
javier.gomez@up.ac.pa.
https://orcid.org/0009-0000-4583-5157

Abstract

Cyberspace has become a domain of power and conflict, challenging traditional geopolitics. This study analyzes how digital dependence redefines sovereignty, borders, and power. The general objective was to develop a conceptual framework for understanding new paradigms of 21st-century conflict and cooperation. Using qualitative documentary analysis of state cybersecurity doctrines, international reports, and academic literature, the research confirms the central hypothesis: cyberspace has fractured traditional paradigms. States are not adapting international law but actively building digital sovereignties through infrastructure control and data localization. Additionally, gray-zone operations—cyber espionage, disinformation, and infrastructure attacks—are normalized as legitimate foreign policy tools within a normative vacuum that fosters competition over cooperation. This leads to the proposal of hybrid sovereignty as the new axis of state authority in the 21st century.

Keywords: Computer security, sovereignty, geopolitics, international security, information policy.

Resumen

El ciberespacio se ha consolidado como un dominio de poder y conflicto que desafía la geopolítica tradicional. Este estudio

analiza cómo la dependencia digital redefine soberanía, frontera y poder, con el objetivo de desarrollar un marco conceptual para los nuevos paradigmas de conflicto y cooperación en el siglo XXI. Mediante una metodología cualitativa y análisis documental de doctrinas estatales, informes internacionales y literatura académica, los resultados confirman la hipótesis central: el ciberespacio ha fracturado los paradigmas tradicionales. Los Estados no adaptan el derecho internacional, sino que priorizan soberanías digitales mediante control de infraestructuras y localización de datos. Asimismo, se evidencia la normalización de operaciones en zona gris (ciberespionaje, desinformación, ataques a infraestructuras tecnológicas) como herramientas legítimas de política exterior, en un entorno de vacío normativo que fomenta la competencia sobre la cooperación. Finalmente, se propone el concepto de soberanía híbrida como nuevo eje de autoridad estatal en el siglo XXI.

Palabras clave: Seguridad informática, soberanía, geopolítica, seguridad internacional, política de la información.

Resumo

O ciberespaço consolidou-se como um domínio de poder e conflito que desafia a geopolítica tradicional. Este estudo analisa como a dependência digital redefine soberania, fronteira e poder, com o objetivo de desenvolver um quadro conceptual para compreender os novos paradigmas de conflito e cooperação no século XXI. Por meio de uma metodologia qualitativa e análise documental de doutrinas estatais, relatórios internacionais e literatura académica, os resultados confirmam a hipótese central: o ciberespaço fraturou os paradigmas tradicionais. Os Estados não estão adaptando o direito internacional, mas sim priorizando a construção de soberanias digitais mediante o controle de infraestruturas e a localização de dados. Da mesma forma, evidencia-se a normalização de operações na zona cinzenta (ciberespionagem, desinformação, ataques a infraestruturas tecnológicas) como ferramentas legítimas de política externa, num ambiente de vazio normativo que fomenta a competição acima da cooperação. Por fim, propõe-se o conceito de soberania híbrida como novo eixo de autoridade estatal no século XXI.

Palavras-chave: ciberespaço; cibersegurança; soberania digital; geopolítica; poder; zona cinzenta; soberania híbrida.

INTRODUCCIÓN

En las últimas décadas, el escenario de las relaciones internacionales ha experimentado una transformación profunda, marcada por la irrupción de un nuevo dominio de poder y conflicto: el ciberespacio. Este entorno digital, que alguna vez fue visto principalmente como un motor para la globalización, se ha consolidado como un campo de batalla estratégico.

La dependencia de las naciones de infraestructuras tecnológicas para el funcionamiento de su economía, gobierno y defensa ha creado una superficie de confrontación sin precedentes (Singer & Friedman, 2014, pp. 1–12). Esta digitalización acelerada ha traído consigo una consecuencia crítica: la creación de una vulnerabilidad estratégica a escala nacional. Estados e infraestructuras críticas se han convertido en objetivos directos para una nueva clase de actores hostiles.

La integración de la Inteligencia Artificial en el arsenal de ciberataques ha acelerado el ciclo de conflicto, permitiendo una automatización de la desinformación y del descubrimiento de vulnerabilidades que desafía la capacidad de respuesta institucional en tiempo real.

El aumento de ciberataques patrocinados por diferentes Estados, el espionaje a gran escala y las campañas de desinformación demuestran una brecha fundamental: la interconexión global ha avanzado mucho más rápido que los paradigmas para gobernarla y protegerla (Singer & Friedman, 2014, pp. 1–12; Reuters Institute, 2024).

En este contexto, los conceptos tradicionales de la geopolítica, como soberanía, frontera y poder, resultan insuficientes. La soberanía ya no puede garantizarse únicamente mediante el control del territorio físico.

Las fronteras se vuelven porosas y el poder se redefine, permitiendo a actores con menos recursos convencionales desafiar a potencias mundiales en el dominio digital. Esta reconfiguración no solo involucra a Estados, sino que otorga un rol protagónico a las corporaciones tecnológicas (Big Tech), las cuales custodian la infraestructura crítica y los datos, convirtiéndose en actores geopolíticos con capacidad de

mediación o sabotaje que, en ocasiones, supera la de los Estados tradicionales (Goldsmith & Wu, 2006).

La presente investigación se justifica por la necesidad imperante de actualizar los marcos de análisis de la política exterior y la seguridad nacional para el contexto del siglo XXI. Este estudio es particularmente urgente y oportuno para la República de Panamá, considerando que su infraestructura tecnológica, específicamente el hub de cables submarinos que convergen en el istmo, lo posiciona como un nodo crítico de la arquitectura digital global.

Esta convergencia no es solo una ventaja logística, sino una servidumbre estratégica: el control físico de estos conductos representa el control sobre el flujo vital de la información global. Para Panamá, la neutralidad histórica de su posición geográfica enfrenta hoy el riesgo de verse comprometida en la disputa por el control de los datos, reactivando la importancia de la geografía física en un dominio supuestamente inmaterial.

En el escenario global actual, la ciberseguridad ha trascendido su concepción técnica original para erigirse como un eje rector de la alta política internacional. Esta transformación estratégica se consolidó cuando se reconoció formalmente al ciberespacio como un dominio operativo de guerra, situándolo al mismo nivel de importancia que los dominios tradicionales de tierra, mar, aire y espacio (OTAN, 2016).

A pesar de que las naciones continúan operando bajo conceptos de soberanía westfaliana, persisten debilidades estructurales en su capacidad para gobernar y defender un entorno donde los actores pueden proyectar su poder de forma anónima e instantánea. A diferencia de los paradigmas de disuasión del siglo XX, la dificultad de atribución en el ciberespacio incentiva una carrera de armamentos constante, convirtiendo al Estado-nación en una entidad vulnerable.

A la luz de esta desconexión, surgen análisis entorno a la irrupción del ciberespacio y la dependencia de infraestructuras críticas transnacionales están forzando una redefinición de los conceptos clásicos de soberanía y poder estatal en la actual competencia geopolítica.

Para abordar esta complejidad, la investigación tiene como objetivo general analizar de qué manera el ciberespacio está reconfigurando los conceptos tradicionales de soberanía, frontera y poder, con la finalidad de desarrollar un marco

conceptual que permita comprender los nuevos paradigmas del conflicto y la cooperación geopolítica en el siglo XXI.

MATERIALES Y MÉTODOS

Para el desarrollo de esta investigación se adoptó un enfoque cualitativo con un diseño no experimental, de carácter bibliográfico y documental. La naturaleza del estudio es descriptivo-analítica, orientada a caracterizar la transición de los paradigmas geopolíticos en el ciberespacio a través de un marco de interpretación crítico.

Para garantizar la rigurosidad y replicabilidad del estudio, se aplicó una técnica de análisis de contenido cualitativo sobre un corpus documental seleccionado mediante un muestreo intencional, basado en criterios de relevancia geopolítica y vigencia temporal.

Las unidades de análisis se categorizaron y procesaron en tres niveles fundamentales que integran literatura académica indexada en repositorios de prestigio para la arquitectura del marco teórico y la fundamentación del fenómeno, informes estratégicos de organismos internacionales y centros de pensamiento especializados.

Todo ello se realiza para la extracción de datos empíricos y tendencias sobre ciberataques globales, así como documentos doctrinales y marcos legales nacionales, tales como estándares, leyes y estrategias, que definen las posturas soberanas de potencias y actores clave en la región.

La ruta operativa de la investigación consistió en la codificación temática de estos textos, utilizando como categorías analíticas los conceptos de soberanía digital y territorialidad, infraestructura crítica y ciberguerra cinética, extraterritorialidad jurídica corporativa y operaciones en zona gris.

Estas categorías permitieron estructurar la discusión de resultados de manera sistémica, contrastando las doctrinas estatales con los incidentes técnicos y los marcos legales emergentes.

El procedimiento de análisis se fundamentó en un enfoque hermenéutico, permitiendo interpretar los eventos tratados a partir de la construcción teórica emergente.

Finalmente, se realizó una triangulación de datos y metodológica para contrastar las doctrinas políticas declaradas con los incidentes técnicos reportados en la industria. Este proceso de validación garantizó la confiabilidad de los

resultados al cruzar fundamentos teóricos con evidencia pragmática, asegurando que los hallazgos deriven de una síntesis sistemática y multidisciplinaria capaz de ser replicada por otros investigadores bajo condiciones similares.

RESULTADOS

El análisis documental y el estudio de casos confirman la hipótesis central de esta investigación: la irrupción del ciberespacio ha provocado una fractura fundamental en los paradigmas de la geopolítica tradicional. Los resultados demuestran que, en lugar de una gobernanza global unificada, los Estados están priorizando la construcción de soberanías digitales y la proyección de poder en entornos no convencionales. La discusión se estructura a través de los cuatro paradigmas analizados:

1. El Paradigma Físico y el Umbral de la Ciberguerra (Caso Stuxnet)

El estudio del caso Stuxnet revela el momento en que el conflicto digital trascendió lo virtual. Descubierto en 2010 y presuntamente desarrollado bajo la operación Juegos Olímpicos (Sanger, 2012), este malware no buscaba el espionaje, sino la destrucción física de la planta nuclear de Natanz en Irán.

Según el análisis de Langner (2013), al manipular los controladores lógicos (PLC) de Siemens para alterar la frecuencia de las centrifugadoras de uranio, Stuxnet validó la existencia de la ciberguerra cinética al cruzar el umbral de lo virtual a lo material.

Más allá del sabotaje, este evento demostró la ineficacia del aislamiento físico (*air-gap*) como medida de protección absoluta y planteó un desafío sistémico al derecho internacional debido a la ambigüedad en la atribución del ataque. Este precedente ha obligado a las naciones a redefinir sus infraestructuras críticas (energía, salud, agua) como objetivos militares legítimos, elevando la ciberseguridad a una condición *sine qua non* de la supervivencia estatal.

2. El Paradigma Doctrinal y la Fragmentación (Caso China) El análisis confirma que los Estados están divergiendo activamente del modelo de gobernanza abierto y descentralizado (Goldsmith & Wu, 2006). China lidera esta tendencia mediante la

institucionalización de la doctrina *Wangluo Zhuquan* o Ciber-Soberanía, la cual propone un giro del modelo *multistakeholder* hacia un multilateralismo estado-céntrico expresado en:

- Control Territorial y Proyección Geopolítica: Pekín sostiene que el ciberespacio es un reflejo del territorio físico donde el Estado debe ejercer soberanía plena (Creemers, 2020). Esta visión no es puramente defensiva; a través de la Ruta de la Seda Digital (Digital Silk Road), China exporta infraestructura crítica y estándares técnicos a terceras naciones, facilitando la expansión de su modelo de gobernanza autoritaria y creando esferas de dependencia tecnológica (Lee, 2022).

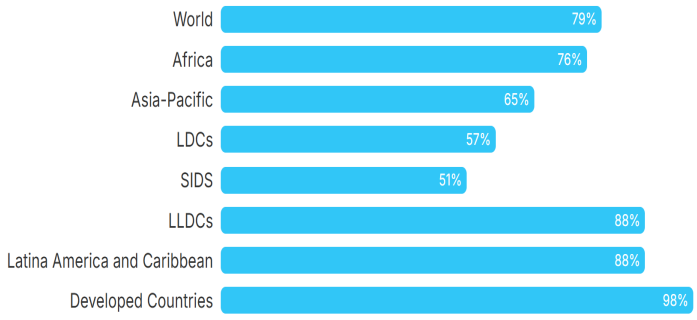
- Soberanía de Datos y Seguridad Nacional: Este modelo, materializado en el Gran Cortafuegos y la Ley de Ciberseguridad de 2017, trasciende la censura para tratar los datos como un activo estratégico.

Al exigir que los datos de los ciudadanos se almacenen domésticamente, práctica replicada por Rusia (Chander & Le, 2015), China redefine la información como un recurso bajo tutela soberana, blindando su ecosistema digital frente a la influencia y el monitoreo de potencias occidentales.

A continuación, se analizan los aspectos vinculados a la legislación mundial sobre protección de datos y su privacidad, expresados en un porcentaje de países con legislación en materia de privacidad y protección de datos, los cuales se muestran en la siguiente figura 1 y la figura 2 en su geolocalización.

Figura 1

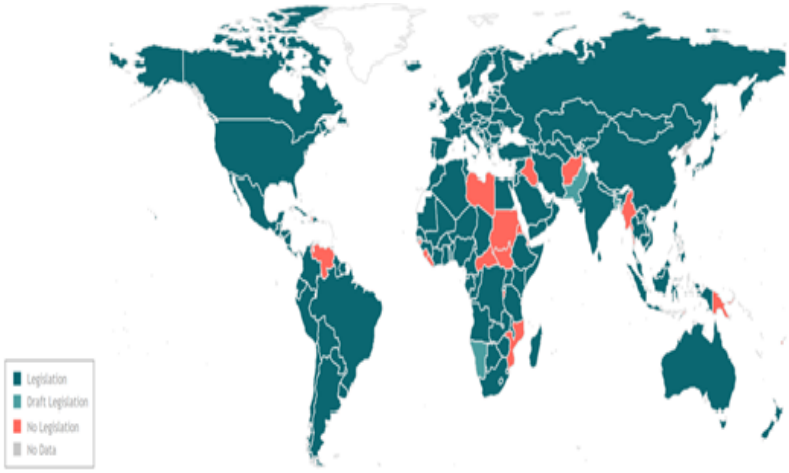
Legislación mundial sobre protección de datos y privacidad. Porcentaje de países con legislación en materia de privacidad y protección de datos.



Fuente: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Figura 2

Legislación mundial sobre protección de datos y privacidad.



Fuente: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

3. El Paradigma Extraterritorial y el Alcance Corporativo (Caso EE. UU.)

A diferencia del control territorial estricto, Estados Unidos ejerce su soberanía mediante la proyección extraterritorial de su poder jurídico, un modelo que desafía la noción clásica de soberanía westfaliana vinculada al espacio físico. El instrumento paradigmático de esta doctrina es la Ley CLOUD (Clarifying Lawful Overseas Use of Data) expresándose mediante los siguientes criterios:

- Desterritorialización de la Justicia: Esta legislación faculta a las agencias federales para exigir la entrega de datos a proveedores de servicios de computación en la nube bajo jurisdicción estadounidense (como Microsoft, Amazon o Google), independientemente de que los servidores se ubiquen físicamente en terceros países. Este enfoque sustituye la geografía por el vínculo corporativo, estableciendo una soberanía funcional donde el Estado sigue a los datos a través de sus empresas nacionales.

- Colisión Jurisdiccional y el Dilema de Cumplimiento: Esta doctrina genera un conflicto sistémico con regímenes de protección de datos, como el GDPR de la Unión Europea.

Según el análisis conjunto de la EDPB y el EDPS (2019), la Ley CLOUD crea un vacío de seguridad jurídica para las organizaciones, que se ven atrapadas en un dilema de cumplimiento: obedecer el mandato estadounidense o respetar el derecho fundamental a la privacidad europeo.

Esta fricción evidencia la transformación de la infraestructura digital en un campo de batalla jurisdiccional, donde las potencias tecnológicas actúan como intermediarios y ejecutores de la autoridad estatal, diluyendo las fronteras nacionales en favor de una jurisdicción corporativa global.

Por otra parte, Brasil representa la respuesta estratégica más estructurada de las naciones emergentes ante la vulnerabilidad digital expuesta por las revelaciones de espionaje masivo de la NSA en 2013 (Caso Snowden).

El país redefinió su política exterior digital bajo una doctrina de soberanía tecnológica que busca reducir la asimetría de poder frente a las potencias del norte a través de dos ejes complementarios (Jiang & Belli, 2024):

-Frente Legal y Normativo: Antes de la LGPD, Brasil sentó un precedente global con el Marco Civil da Internet (2014), considerado la Constitución de la Internet, que estableció principios de neutralidad de la red y derechos civiles en el ciberespacio como respuesta directa a la vigilancia externa.

Posteriormente, la Ley General de Protección de Datos (LGPD) de 2018 consolidó este blindaje jurídico al elevar la protección de datos a la categoría de derecho fundamental, permitiendo al Estado brasileño ejercer una autoridad normativa sobre empresas extranjeras y alinearse con los estándares de privacidad más rigurosos del mundo (Bioni, 2019).

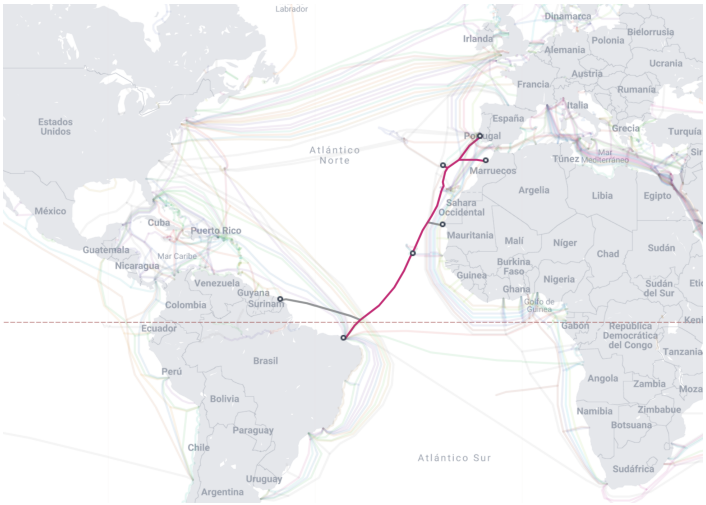
-Frente de Infraestructura y Resiliencia Física: Para garantizar una autonomía real, Brasil identificó que la independencia legal es insuficiente si no existe una soberanía sobre el sustrato físico de la red.

El impulso del cable submarino EllaLink (2021) representa una ruptura con la dependencia de ruta (path dependency) tradicional, donde casi la totalidad del tráfico de datos de la región transitaba por nodos controlados por Estados Unidos.

Al conectar directamente Fortaleza con Sines (Portugal), este proyecto no solo reduce la latencia, sino que materializa una decisión geopolítica diseñada para proteger el flujo de datos estratégicos y de defensa nacional frente a la interceptación en puntos de tránsito norteamericanos como se muestra en el mapa de cables submarinos, reflejado en la figura 3. (EllaLink, s.f.; Jiang & Belli, 2024).

Figura 3

Mapa de Cables Submarinos (EllaLink).



Fuente: https://www.submarinecablemap.com/submarine-cable/ellalink

Los resultados evidencian que el ciberespacio se ha consolidado como el vehículo predilecto para operaciones situadas en la zona gris, definida como el espacio de conflicto que permanece deliberadamente por debajo del umbral de la guerra convencional para evitar una respuesta militar a gran escala. Esta dinámica representa una fractura en la dicotomía tradicional de paz o guerra, estableciendo un estado de beligerancia persistente.

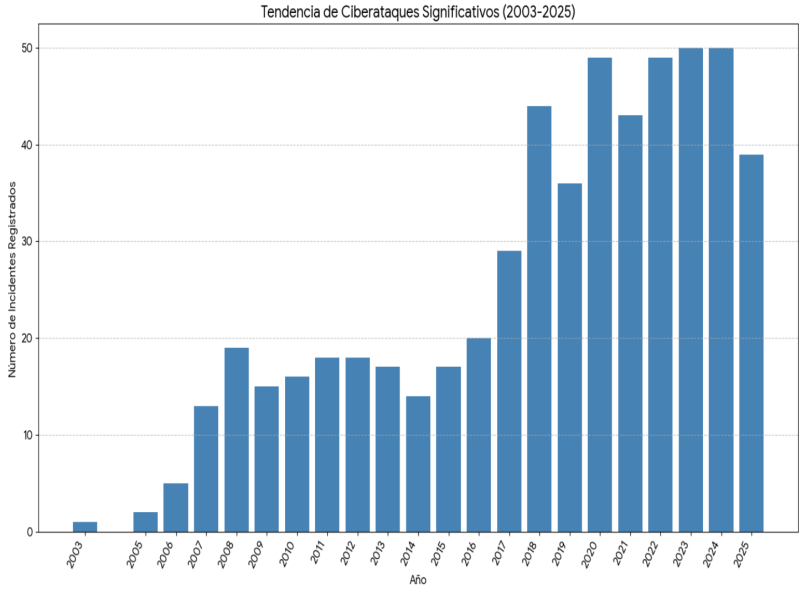
-Estratificación del Ataque a Infraestructuras: En 2024, el 57% de los incidentes cibernéticos se dirigieron contra infraestructuras críticas, lo que demuestra que el objetivo no es solo el robo de información, sino la capacidad de paralizar el funcionamiento básico de un Estado (energía, finanzas y salud) como mecanismo de presión política. Esta tendencia refleja la

adopción de doctrinas de ataque al centro de gravedad del adversario sin necesidad de despliegue de tropas físicas.

-La Ventaja de la Atribución Ambigua: Se documentan ataques continuos vinculados a actores estatales contra sectores estratégicos de defensa y energía en regiones como Medio Oriente, Australia y el sector aeroespacial. La relevancia académica de estas operaciones reside en el uso de proxies (actores por poder) o grupos de fachada, lo que permite a los Estados alcanzar objetivos geopolíticos manteniendo una negación plausible, diluyendo así la responsabilidad jurídica internacional.

-Desinformación como Arma de Erosión Institucional: Las campañas para erosionar la confianza institucional, especialmente críticas durante procesos electorales en 2024, se han normalizado como herramientas estándar de política exterior. Estas operaciones de información no buscan convencer al adversario, sino fragmentar el tejido social y deslegitimar las democracias, convirtiendo la percepción pública en un nuevo frente operativo de la geopolítica digital.

Figura 4. Tendencia de Ciberataques Significativos (2003-2025).



Fuente: Elaboración propia a partir de datos del Center for Strategic & International Studies (CSIS). Ciberataques significativos patrocinados por estados. https://www.csis.org/programs/strategic-tec

La figura ilustra la frecuencia de incidentes cibernéticos significativos registrados por año, extraídos de la base de datos del Center for Strategic and International Studies (CSIS, 2025). Se observa una clara y pronunciada tendencia al alza en el número de estos incidentes a lo largo de las últimas dos décadas.

Esta visualización sirve como evidencia empírica directa para la presente investigación y respalda de manera contundente la hipótesis central de este trabajo: la normalización de las operaciones en la zona gris. Autores como Wirtz (2017) y Mazarr (2015) definen esta zona como el espacio entre la paz y la guerra donde los actores estatales utilizan ciberataques para obtener ventajas estratégicas sin desencadenar un conflicto militar convencional. El aumento constante en la frecuencia de estos incidentes, visible en la gráfica, demuestra que estas tácticas han pasado de ser eventos aislados a herramientas comunes de la política exterior moderna (CSIS, 2025; Maness & Valeriano, 2016).

CONCLUSIONES

Esta nueva realidad ha roto para siempre los esquemas geopolíticos clásicos. El mundo no avanza hacia acuerdos globales, sino hacia una internet dividida en bloques enfrentados. China impone su control absoluto (Wangluo Zhuquan); Estados Unidos extiende su jurisdicción con la Ley CLOUD; Brasil responde con infraestructura propia como el cable EllaLink.

Países en nodos clave como Panamá deben dejar la neutralidad y gestionar activamente su soberanía digital. Las operaciones en zona gris (espionaje, desinformación, sabotaje) ya son moneda corriente en política exterior. Por eso, la ciberseguridad se vuelve condición de supervivencia estatal.

Las universidades tienen que romper el aislamiento entre carreras como Informática, Derecho y Relaciones Internacionales. Es urgente formar profesionales capaces de analizar tanto códigos como leyes extraterritoriales. Solo así se reducirá la dependencia intelectual de la región.

La defensa real exige crear una inteligencia geopolítica propia y una doctrina de infraestructura soberana. Los Estados deben diversificar sus conexiones para evitar la vigilancia masiva y

generar datos propios que midan su vulnerabilidad tecnológica. La ciencia debe guiar la política exterior y la defensa nacional en este siglo complejo.

REFERENCIAS

Bioni, B. (2019). Proteção de dados pessoais: A função e os limites do consentimento. Ed. Forense. https://www.kufunda.net/publicdocs/Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20a%20fun%C3%A7%C3%A3o%20e%20os%20limites%20do%20consentimento%20(Bruno%20Ricardo%20Bioni).pdf

Center for Strategic and International Studies (SCIS). (2025). Significant cyber incidents since 2006. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chander, A., & Le, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677–739. https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=elj

Creemers, R. (2020). China's conception of cyber sovereignty. En D. Broeders & B. van den Berg (Eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107–126). Rowman & Littlefield. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421

EllaLink. (s.f.). The first high-capacity direct connection between Europe and Latin America https://ella.link/

European Data Protection Board (EDPB) & European Data Protection Supervisor (EDPS). (2019). Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data. European Union. https://www.edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

Goldsmith, J., & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. Oxford University Press. https://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf

Jiang, M., & Belli, L. (2024). Digital sovereignty in the BRICS: A multi-dimensional approach. Journal of Cyber Policy, 1–22. https://doi.org/10.1080/23738871.2023.2290000

Langner, R. (2013). To kill a centrifuge: A technical analysis of Stuxnet's latent design. The Langner Group. https://www.langner.com/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Lee, J. (2022). China's Digital Silk Road: Strategic technological competition and exporting political illiberalism. Issues & Insights Working Paper, 22(SR2). Pacific Forum.

Maness, R. C., & Valeriano, B. (2016). *Cyber spillover conflicts: Transitions from cyber conflict to conventional foreign policy disputes?* En K. Friis (Ed.), Conflict in Cyber Space (pp. 45–64). Routledge.

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428

Organización del Tratado del Atlántico Norte (OTAN). (2016). Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Reuters Institute for the Study of Journalism. (2024). Digital news report 2024. University of Oxford. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024

Sanger, D. E. (2012). Confront and conceal: Obama's secret wars and surprising use of American power. Crown.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

United Nations Conference on Trade and Development (UNCTAD). (2024). Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Wirtz, J. J. (2017). *Life in the Gray Zone: Observations on contemporary conflict. Strategic Studies Quarterly*, 11(4), 3–14.