El ciberpoder como capacidad estratégica para consolidar la soberanía digital

Cómo citar este artículo [Chicago]: Realpe Diaz, Milena Elizabeth y Javier Alberto Ayala Amaya. "El ciberpoder como capacidad estratégica para consolidar la soberanía digital". *Novum Jus* 20, no. 2 (2026): 79-105. https://doi.org/10.14718/NovumJus.2026.20.2.3

Milena Elizabeth Realpe Diaz /
Javier Alberto Ayala Amaya

Código: 1335295270 • Autor: istockphoto.com

https://doi.org/10.14718/NovumJus.2026.20.2.3

El ciberpoder como capacidad estratégica para consolidar la soberanía digital

Milena Elizabeth Realpe Diaz[*]
Javier Alberto Ayala Amaya[**]

Recibido: 5 de agosto de 2025 **| Evaluado:** 16 de septiembre de 2025 **| Aceptado:** 2 de febrero de 2026

Resumen

El presente artículo tiene como objetivo determinar de qué manera la consolidación de la soberanía digital de un Estado, dada su capacidad de ejercer control autónomo sobre sus recursos digitales, sistemas de información y plataformas tecnológicas, se configura como la expresión máxima de ciberpoder estatal. Para ello, se analizan los elementos constitutivos de la soberanía digital —infraestructura crítica, flujos de datos, marcos normativos, tecnologías emergentes e insumos estratégicos— y se argumenta que todos ellos pueden ser protegidos o vulnerados a través del despliegue del ciberpoder. Asimismo, se examina la relación entre Estados y corporaciones tecnológicas transnacionales, evidenciando tensiones estructurales y escenarios de subordinación normativa. El estudio concluye que el ciberpoder, más allá de su función defensiva, debe ser comprendido como una herramienta activa de gobernanza digital, capaz de incidir en la formulación normativa, la protección de infraestructuras, la acción diplomática y el desarrollo tecnológico soberano. En este marco, la soberanía digital se redefine como una construcción dinámica, disputada y dependiente de la articulación estratégica de capacidades cibernéticas nacionales.

Palabras clave: ciberpoder; soberanía digital; hegemonía tecnológica; ciberseguridad; gobernanza digital.

[*] Coronel, Ejército Nacional de Colombia. PhD (c) en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra General Rafael Reyes Prieto. Magíster en Ciberseguridad y Ciberdefensa por la Escuela Superior de Guerra. Magíster en Seguridad de la Información por la Universidad de Los Andes. Especialista en Seguridad de Redes de Computadores por la Universidad Católica de Colombia. Especialista en Seguridad Física y de la Informática por la Escuela de Comunicaciones del Ejército Nacional. Especialista en Seguridad de la Información por la Universidad de los Andes. Ingeniera de Sistemas por la Universidad Cooperativa de Colombia. ORCID: https://orcid.org/0000-0003-4345-6182. Correo: milena.realpe@esdeg.edu.co.

[**] Autor póstumo (1968-2026). Mayor General (R) del Ejército Nacional de Colombia. Se desempeñaba como rector en propiedad de la Universidad Militar Nueva Granada (UMNG) al momento de su fallecimiento, ocurrido el 1 de junio de 2026. Este manuscrito constituye una de sus últimas contribuciones académicas en los campos del ciberpoder y la soberanía digital. Posdoctor en Costituzione e Diritto Civile negli Ordinamenti Europei e Latino-Americani por la Università degli Studi di Messina (Italia); Ph. D. en Derecho por la Universidad Sergio Arboleda; Ph. D. en Derecho Internacional por la Universidad Alfonso X el Sabio (España); magíster en Seguridad y Defensa por la Universidad de Nebrija (España) y por la Escuela Superior de Guerra; especialista en Alta Gerencia Internacional por la Universidad de los Andes; abogado por la Universidad Autónoma de Bucaramanga y profesional en Ciencias Militares por la Escuela Militar de Cadetes "General José María Córdova". ORCID: https://orcid.org/0000-0003-4345-6182. Correo: javier.ayala@unimilitar.edu.co.

https://doi.org/10.14718/NovumJus.2026.20.2.3

Cyberpower as a Strategic Capability for Consolidating Digital Sovereignty

Milena Elizabeth Realpe Diaz
Javier Alberto Ayala Amaya

Received: August 5, 2025 **| Evaluated:** September 16, 2025 **| Accepted:** February 2, 2026

Abstract

This article aims to determine how the consolidation of a State's digital sovereignty, given its capacity to exercise autonomous control over its digital resources, information systems, and technological platforms, constitutes the highest expression of state cyberpower. To this end, it analyzes the constituent elements of digital sovereignty—critical infrastructure, data flows, regulatory frameworks, emerging technologies, and strategic inputs—and argues that all of them may be protected or compromised through the deployment of cyberpower. It also examines the relationship between States and transnational technology companies, revealing structural tensions and scenarios of regulatory subordination. The study concludes that cyberpower, beyond its defensive function, should be understood as an active tool of digital governance capable of influencing regulatory formulation, infrastructure protection, diplomatic action, and sovereign technological development. Within this framework, digital sovereignty is redefined as a dynamic and contested construct that depends on the strategic articulation of national cyber capabilities.

Keywords: cyberpower; digital sovereignty; technological hegemony; cybersecurity; digital governance

Introducción

En la era de la hiperconectividad global, el ciberespacio ha emergido como un nuevo dominio estratégico donde se redefinen las formas del poder y la soberanía estatal. A diferencia de los dominios tradicionales de tierra, mar, aire y espacio, el ciberespacio no se encuentra delimitado geográficamente, sino que se configura por infraestructuras digitales, flujos de datos y marcos normativos que trascienden fronteras físicas. Esta característica convierte al ciberpoder en una herramienta clave para los Estados que buscan preservar o recuperar su propia soberanía digital, entendida como la capacidad para ejercer control autónomo sobre sus recursos digitales, sistemas de información y plataformas tecnológicas[1]. El Senado de Francia[2], por su parte, sitúa su discusión sobre el hecho de que la soberanía digital en el ciberespacio, lejos de ser una utopía igualitaria, se ha convertido en un lugar de enfrentamiento mundial.

En dicho escenario, el presente artículo propone una tesis: cuando el ciberpoder es configurado y desplegado estratégicamente, se vuelve un instrumento decisivo para la consolidación de la soberanía digital, al habilitar capacidades técnicas, normativas, defensivas y diplomáticas que permiten contrarrestar la hegemonía tecnológica ejercida por actores dominantes en el ciberespacio.

El objetivo general que guía la investigación es determinar cómo influye el ciberpoder en la consolidación de la soberanía digital de los Estados. Para ello se han definido tres objetivos específicos. El primero es identificar los elementos constitutivos de la soberanía digital que son susceptibles de control mediante capacidades cibernéticas. El segundo es analizar la relación entre actores privados y estatales en función de su incidencia sobre la soberanía digital. El tercero es describir cómo el ciberpoder actúa sobre dichos elementos para consolidar la soberanía digital a favor de determinados actores. Estos objetivos permitirán una exploración sistemática de las dinámicas de poder que se despliegan en el ciberespacio, así como de los desafíos que enfrentan

[1] Milena Realpe, "La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de la soberanía digital", *Novum Jus* 18, núm. 2 (2024): 279-304; Juan Aguilar, "China Y Estados Unidos: Antagonismos Y Liderazgos En El Ciberespacio Frente a América Latina", *URVIO. Revista Latinoamericana De Estudios De Seguridad*, núm. 36 (mayo 2024): 66-84.

[2] Francia, Senado, Rapport d'information fait au nom de la commission d'enquête sur la souveraineté numérique [Informe de información realizado en nombre de la comisión de investigación sobre la soberanía digital], núm. 7 (2019-2020).

los Estados de menor desarrollo tecnológico para proteger su autonomía digital frente a potencias y corporaciones con capacidades cibernéticas superiores[3].

En el artículo se abordarán en primer lugar los componentes básicos de la soberanía digital: infraestructura crítica, flujos de datos, ciberseguridad, regulación y autonomía normativa, y se destacará cómo esas dimensiones pueden ser vulneradas o fortalecidas por el uso estratégico del ciberpoder. Posteriormente se examinará la asimetría entre actores estatales y corporativos; sobre todo, en regiones como América Latina, donde la dependencia tecnológica y la debilidad de las capacidades cibernéticas obstaculizan el ejercicio efectivo de la soberanía digital[4]. Finalmente, se analizarán casos y mecanismos mediante los cuales los Estados pueden fortalecer su propio ciberpoder como herramienta de autodeterminación digital.

En los actuales escenarios geopolíticos, el ciberespacio ha dejado de ser solo un entorno de interacción informacional para convertirse en un verdadero campo de batalla donde los Estados ejercen poder y proyectan influencia. La relevancia que adquiere el ciberespacio, como lo advierte Ayala, "no se limita solamente a potencializar las redes, sino a tornarse en un modo prevalente para la organización de las actividades humanas transformando, a partir de su lógica, todos los dominios de la vida social y económica"[5]. Esta lógica transforma la noción tradicional de soberanía, al depender esta ahora de la capacidad estatal de ejercer control y protección sobre su infraestructura crítica digital y sus flujos de información.

La relación existente entre ciberpoder y soberanía digital reproduce fielmente las tensiones y, por qué no decirlo, batallas que en el ciberespacio se libran a título de actores particulares con claras intenciones de generar impactos significativos en diversos escenarios del dominio físico. Por definición, estas son operaciones *no cinéticas* que, como lo señala Vea[6], no se perciben dando un paseo por la calle. Sus efectos son difíciles de atribuir a un autor y suele ser el usuario de la tecnología el primero en advertir que algo está pasando. Se manifiestan en interrupciones del

[3] Kevin Parker, "El uso del ciberpoder", *Military Review*, ed. hispanoamericana, mayo-agosto (2014): 50-63; Joseph Nye, "Cyber power" (Cambridge: Universidad de Harvard, Escuela gubernamental John F. Kennedy, Centro Belfer para la Ciencia y Asuntos Internacionales, mayo de 2010).

[4] Juan Aguilar, "Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030", *Revista Seguridad y Estrategia* 1, núm. (2023): 40-55; Carmen Cîrnu y Alexandru Georgescu, "A complex system governance theory", *Studies in Informatics and Control* 32, núm. 2 (2023): 127-136.

[5] Javier Ayala, *Los ciberconflictos a la luz del Derecho Internacional Humanitario* (Bogotá: Grupo Editorial Ibáñez, 2018), 20.

[6] Javier Vea, "Introducción a la guerra no cinética", *Revista de aeronáutica y astronáutica*, núm. 915 (2022): 708-719.

servicio, alteraciones en el acceso a la información, manipulación de narrativas o fallos técnicos inexplicables, que evidencian una disrupción anómala del entorno digital. Estas operaciones no suelen dejar un agujero humeante en el suelo, no producen sonidos violentos y no ocasionan derramamiento de sangre civil colateral. Son operaciones precisas, discretas y esquivas, pero con una contundente capacidad de influencia que no debe subestimarse.

En el contexto contemporáneo, las operaciones *no cinéticas* en el ciberespacio y en diferentes escenarios son cada vez más frecuentes e insidiosas. Las grandes potencias, como Estados Unidos, China y Rusia, libran una competencia estratégica multidimensional que va más allá del plano militar tradicional e incorpora la guerra informativa, la ciberseguridad, la supremacía tecnológica y la influencia geopolítica mediante el control de datos y algoritmos. Esta lucha se manifiesta en conflictos indirectos por el dominio del ciberespacio, campañas de desinformación, ataques cibernéticos dirigidos a infraestructuras críticas, espionaje digital y el uso de tecnologías emergentes con fines estratégicos[7]. En el escenario descrito, el ciberpoder es desplegado como una herramienta de disuasión, coerción y proyección de poder blando y duro en el entorno digital.

Además de esta pugna cibernética, se desarrolla una guerra comercial y tecnológica orientada a controlar los flujos económicos y los recursos críticos para el desarrollo de tecnologías estratégicas como la inteligencia artificial (IA), la computación cuántica y la fabricación de semiconductores. Estados Unidos y sus aliados han impuesto restricciones comerciales a empresas chinas como Huawei y SMIC, mientras que China invierte agresivamente en asegurarse el acceso a tierras raras y minerales estratégicos como el litio, el cobalto y el neodimio, esenciales para la fabricación de dispositivos electrónicos y componentes militares[8].

Rusia, por su parte, ha fortalecido su soberanía tecnológica mediante alianzas estratégicas y desarrollo de capacidades nacionales. Esta lucha por los insumos tecnológicos fundamentales configura una nueva forma de competencia sistémica que redefine los límites de la soberanía estatal y exige a los países periféricos construir ciberpoder soberano para no quedar subordinados a las potencias dominan-

[7] Aguilar, "Retos de América Latina"; Keir Giles, *Handbook of Russian Information Warfare* (NATO Defense College, 2016).

[8] Unión Europea, *Comisión Europea, Critical raw materials resilience: Charting a path towards greater security and sustainability* [Resiliencia de las materias primas fundamentales: Trazando un camino hacia una mayor seguridad y sostenibilidad], COM(2020) 474 final (Bruselas: Comisión Europea, 2 de septiembre de 2020); Yan Xuetong, *Leadership and the rise of great powers* (Princeton University Press, 2019).

tes. En este marco, la literatura académica reciente ha subrayado la necesidad de conceptualizar el ciberpoder como una dimensión transversal de las capacidades estatales. Según Nye[9], el ciberpoder puede expresarse como la habilidad de un actor para obtener resultados mediante recursos del ciberespacio, lo cual incluye tanto medios coercitivos (*hard power*) como instrumentos de atracción y legitimación (*soft power*). Esta concepción ha sido retomada por diversos autores para señalar que el poder en el ciberespacio opera mediante la manipulación de datos, el control de plataformas digitales y la imposición de estándares tecnológicos, y configura así una nueva arquitectura de influencia global[10].

Visto lo anterior, si la guerra no cinética (*non-kinetic warfare* [NKW]) se entiende como el empleo de herramientas informativas, psicológicas, diplomáticas, económicas, sociales y tecnológicas por parte del Estado para alcanzar objetivos estratégicos, afectando o condicionando la voluntad nacional del adversario[11], resulta lógico reconocer que el ciberespacio ha sido instrumentalizado con fines hostiles por actores como Rusia y China. Los ciberataques rusos son ilustrativos; en 2015 los ataques informáticos denominados *BlackEnergy* e *Industroyer* dejaron sin electricidad a miles de personas en Ucrania; en 2017 el ciberataque NotPetya se propagó globalmente y causó daños por más de 10.000 millones de USD[12]. Asimismo, la censura, propaganda global y desinformación chinas[13] permiten entrever cómo se utiliza el ciberespacio para alcanzar supremacía, así como para manipular, engañar e intimidar a sus oponentes, en clara manifestación de las formas contemporáneas de agresión propias de la NKW.

En este escenario, la noción de *soberanía digital* se revela como una construcción frágil, particularmente para aquellos Estados que carecen de ciberpoder suficiente para proteger y proyectar su autonomía en el espacio digital. Cuanto mayor es el ciberpoder de un Estado, mayor es su capacidad de autodeterminación y, en consecuencia, más sólida es su soberanía digital. Por el contrario, las asimetrías tecnológicas existentes degradan la posibilidad de que los países con menos recur-

9 Joseph Nye, "Cyber power"; Nye, *The future of power* (Nueva York: PublicAffairs, 2011).

10 Realpe, "La ciberdiplomacia"; Daniel Kuehl, "From cyberspace to cyberpower: Defining the problem", en *Cyberpower and national security,* ed. Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009).

11 Vea, "Introducción a la guerra".

12 Joe Tidy, "Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente", *BBC News,* 24 de marzo de 2022.

13 Dan, Blumenthal y Linda Zhang, "Censura, propaganda y desinformación en China", American Enterprise Institute (AEI), 10 de julio de 2020.

sos logren consolidar capacidades diferenciales en el ciberespacio, con lo que se perpetúa su dependencia y vulnerabilidad.

Frente al mencionado escenario, América Latina presenta un rezago estructural en materia de ciberseguridad, infraestructura digital y formulación de políticas públicas para el desarrollo del ciberpoder. Según indicadores como el Global Cybersecurity Index[14] y el National Cyber Security Index[15], la mayoría de los países latinoamericanos se ubican por debajo del promedio mundial en términos de capacidades cibernéticas, lo que revela una situación de vulnerabilidad estructural frente a amenazas externas y limita las posibilidades de ejercer una soberanía digital efectiva[16]. Para superar esa condición, resulta necesario desarrollar una estrategia nacional de ciberpoder que articule inversión en infraestructura, fortalecimiento de las capacidades humanas y técnicas, marcos normativos adaptativos, cooperación internacional y participación en foros multilaterales. Dicha estrategia debe considerar, además, el papel de las empresas tecnológicas globales, cuyo poder de facto sobre los flujos de información y las plataformas digitales desafía la autoridad de los Estados y requiere mecanismos de regulación y control desde una perspectiva soberana[17].

Este artículo adopta un enfoque cualitativo e interpretativo, guiado por el paradigma constructivista, que entiende la realidad como una construcción social producto de las interacciones entre actores, normas e instituciones[18]. Por medio de una revisión documental de literatura académica, informes técnicos y documentos de organismos multilaterales, se analizan las dinámicas que configuran el ciberpoder y su impacto sobre la soberanía digital. Más que medir variables, este estudio busca comprender cómo los Estados y otros actores, como las corporaciones tecnológicas y las organizaciones internacionales, disputan el control del ciberespacio mediante estrategias normativas, tecnológicas y diplomáticas. El marco teórico se sustenta en la teoría del poder de Nye[19], cuyas nociones de *hard, soft* y *smart power* permiten interpretar el ciberespacio como un escenario de competencia política y geoestratégica, más allá de lo puramente técnico.

---

14 Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index 2020* [Índice global de ciberseguridad 2020] (Ginebra: Unión Internacional de Telecomunicaciones, junio de 2021).

15 Academia de e-Gobernanza de Estonia, "NCSI Index", National Cyber Security Index, consultado el 19 de mayo de 2026.

16 Aguilar, "Retos de América Latina".

17 André Barrinha y Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age", *Global Affairs* 3, núms. 4-5 (2017): 353-364; Patrick. J. Blount, *Reprogramando el mundo: el ciberespacio y la geografía del orden global* (Bristol: Prensa de e-Relaciones Internacionales, 2019).

18 Peter Berger y Thomas Luckman, *La construcción social de la realidad* (Amorrortu, 1997).

19 Nye, "Cyber power"; Nye, *The future of power*.

En virtud de lo anterior, la comprensión del ciberpoder como fenómeno emergente requiere abordar su configuración discursiva, normativa, tecnológica y política en contextos dinámicos e interdependientes[20]. Desde esta perspectiva, la soberanía digital no es entendida como una condición dada, sino como una construcción en disputa, atravesada por relaciones asimétricas de poder, gobernanza tecnológica y apropiación normativa del ciberespacio[21]. En esta línea, los conceptos de *hegemonía digital, soberanía normativa* y *cibergobernanza global* son considerados productos discursivos que deben ser desentrañados en sus contextos de producción, reproducción y disputa[22].

A través de esta lente, el análisis de actores como Estados Unidos, China y Rusia, al igual que el de organismos como Naciones Unidas o la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus iniciales en inglés), se abordará no solo desde sus capacidades técnicas, sino también desde la legitimidad que otorgan a sus prácticas de poder digital. El análisis se basa en categorías emergentes del material revisado, aplicando un enfoque inductivo que permite generar interpretaciones fundadas y contextualizadas[23]. Esta estrategia metodológica proporciona herramientas conceptuales y analíticas para demostrar la tesis principal: que el ciberpoder constituye una capacidad estratégica determinante para que los Estados ejerzan soberanía digital efectiva en el nuevo orden internacional digital.

Elementos constitutivos de la soberanía digital susceptibles de control e influencia por parte del ciberpoder

La *soberanía digital* puede entenderse como la capacidad de los Estados para ejercer control autónomo sobre su infraestructura tecnológica, datos, normas y contenidos digitales. Según Braun y Hummel[24], este concepto implica una combinación de poder absoluto, encarnado e institucional, a fin de mantener la libertad y proteger

[20] Ruth Sautu, *El método biográfico. La reconstrucción de la sociedad a partir del testimonio* (Ediciones Lumiere, 2023); Uwe Flick, *Introducción a la investigación cualitativa* (Ediciones Morata, 2004).

[21] Berger y Luckman, *La construcción social*.

[22] Guzzini Stefano, "A reconstruction of constructivism in international relations", *European Journal of International Relations* 6, núm. 2 (2000): 147-182; Ted Hopf, "The promise of constructivism in international relations theory", *International Security* 23, núm. 1 (1998): 171-200.

[23] Sautu, *El método biográfico*; Flick, *Introducción a la investigación*.

[24] Matthias Braun y Patrik Hummel, "Is Digital Sovereignty Normatively Desirable?", *Information, Communication & Society*, (2024): 1–14.

frente a vulnerabilidades en entornos digitales. En el ámbito europeo, Mügge[25] precisa que dicha soberanía implica dominio sobre las capas física, lógica y de contenido digital, que incluye datos, algoritmos y estándares, como forma de autonomía estratégica frente a potencias como Estados Unidos y China. Flonk et al.[26] evidencian que en la Unión Europea se ha pasado del enfoque de libre acceso al de control de contenido como instrumento de soberanía, especialmente frente a la desinformación y el discurso de odio.

Desde una perspectiva latinoamericana, Ayala[27] señala que la soberanía digital también es una herramienta de defensa ante amenazas híbridas y actores no estatales en el ciberespacio, que demanda normas que protejan tanto al Estado como a la población. En ese sentido, la soberanía digital se configura como una extensión del poder estatal en el dominio digital y, como tal, es objeto de disputa geopolítica y económica. El ciberpoder se presenta, entonces, como la herramienta estratégica mediante la cual los Estados, corporaciones y actores híbridos buscan intervenir o consolidar dicha soberanía.

Entre los elementos centrales que componen la soberanía digital se encuentran: la infraestructura crítica de telecomunicaciones; la capacidad de almacenamiento y procesamiento de datos; el control sobre los flujos de datos transfronterizos; los marcos jurídicos que rigen la protección de datos y la privacidad, y la autonomía en el desarrollo y uso de tecnologías emergentes como la IA y los sistemas operativos. Como señala Kittichaisaree[28], la soberanía digital requiere un equilibrio entre la posesión material de infraestructuras (cables, servidores, satélites) y la autonomía funcional para operar sistemas digitales propios. El control de la infraestructura digital es un componente esencial, porque define la capacidad de un país para sostener de manera autónoma y segura la propia conectividad digital. De acuerdo con Realpe[29], sin control soberano sobre dicha infraestructura, los Estados acaban siendo vulnerables a interrupciones del servicio, espionaje, dependencia tecnológica y pérdida de autonomía regulatoria. Así, el ciberpoder se manifiesta en la posibilidad de asegurar, controlar o intervenir estas infraestructuras.

[25] Daniel Mügge, "EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?", *Journal of European Public Policy* 31, núm. 8 (2024): 2200-2225.

[26] Daniëlle Flonk, Markus Jachtenfuchs y Anke Obendiek, "Controlling Internet Content in the EU: Towards Digital Sovereignty", *Journal of European Public Policy* 31, núm. (2024): 2316–2342.

[27] Ayala, *Los ciberconflictos*.

[28] Kriangsak Kittichaisaree, *Public International Law of Cyberspaces* (Springer, 2017).

[29] Realpe, "La ciberdiplomacia".

Además de la infraestructura, el tratamiento y soberanía sobre los datos constituye uno de los frentes más sensibles. En un entorno global donde los datos personales, económicos, de seguridad y de inteligencia circulan por redes que atraviesan múltiples jurisdicciones, el control sobre estos flujos se convierte en una cuestión de soberanía. China, por ejemplo, ha promovido el concepto *cibersoberanía* para justificar la localización de datos y el control estatal sobre la información que circula en su ciberespacio nacional[30]. A través del ciberpoder, los Estados buscan imponer sus propias reglas sobre el manejo de datos, lo cual los convierte tanto en un bien estratégico como en elementos de disputa o, mejor, convierte el procedimiento de protección en una acción hostil, dada la localización dispersa de dichos datos.

Un elemento clave es el marco normativo que sustenta el entorno digital. Dicha arquitectura se compone de estándares técnicos, protocolos de comunicación, legislación en materia de ciberseguridad, derechos digitales y mecanismos de gobernanza. La imposición de determinados estándares por parte de empresas o países con mayor influencia digital puede convertirse en un mecanismo indirecto de subordinación normativa e inequidad en el libre uso del ciberespacio. Tal como apunta Blount[31], la "geografía del orden digital" no está determinada por límites geográficos, sino por la distribución del poder normativo en el ciberespacio.

También resulta fundamental la capacidad para desarrollar y controlar tecnologías críticas, como la IA, la computación cuántica y los sistemas operativos. Estas tecnologías permiten ejercer control funcional sobre redes, datos y usuarios; por tanto, constituyen una dimensión estratégica de la soberanía digital. El acceso soberano a estas capacidades determina en gran medida la autonomía digital de un país. Como han advertido Realpe y Nye[32], la dependencia de soluciones extranjeras crea vulnerabilidades estructurales que pueden ser explotadas en contextos de tensión política, económica o militar.

La Figura 1 presenta un análisis comparativo de los principales elementos que componen la soberanía digital, según tres enfoques académicos destacados: los de Mügge, Braun y Hummel, así como el de Flonk et al[33]. Esa sistematización permite identificar coincidencias y divergencias conceptuales entre los autores respecto al

30 Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace", *NBR Special Report* núm. 87 (2020).

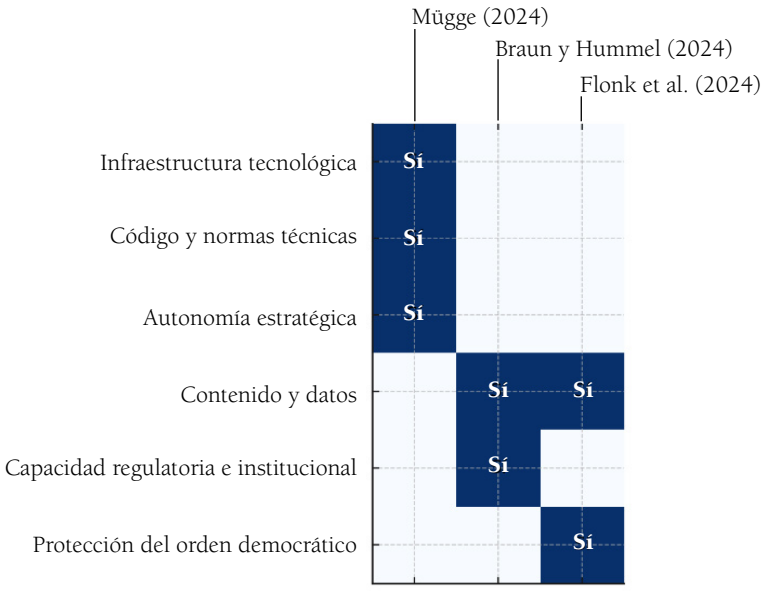
31 Blount, "*Reprogramando el mundo*".

32 Realpe, "La ciberdiplomacia"; Nye, "Cyber power".

33 Mügge, "EU AI Sovereignty"; Braun y Hummel, "Is Digital Sovereignty"; Flonk, Jachtenfuchs y Obendiek, "Controlling Internet".

control estatal sobre la infraestructura tecnológica, las normas técnicas, los flujos de datos, la capacidad regulatoria y la protección del orden democrático.

Figura 1. Coincidencias en elementos de soberanía digital por autor



Fuente: elaboración propia, a partir de Mügge, Braun y Hummel, Flonk et al[34].

El ciberpoder actúa a través de diversas formas: desde el desarrollo de capacidades nacionales para proteger infraestructuras hasta la proyección de poder ofensivo mediante ciberataques o la manipulación de sistemas extranjeros. Como lo plantean Betz y Stevens[35], el ciberpoder puede manifestarse tanto en la amenaza como en el uso efectivo de recursos cibernéticos para lograr objetivos estratégicos, y configura así nuevas formas de coerción o disuasión digital.

En contextos de ciberdependencia, donde los Estados delegan funciones clave del entorno digital en empresas extranjeras, se produce una erosión de la soberanía, entendida dicha merma como el debilitamiento de la capacidad del Estado para ejercer control efectivo sobre los recursos, datos, normas, infraestructuras y dinámicas sociales que se desarrollan en el entorno digital. Esa vulnerabilidad

[34] Mügge, "EU AI Sovereignty"; Braun y Hummel, "Is Digital Sovereignty"; Flonk, Jachtenfuchs y Obendiek, "Controlling Internet Content".

[35] David Betz y Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (Routledge, 2011).

puede ir desde el uso de plataformas extranjeras para servicios públicos hasta la contratación de soluciones privadas de ciberseguridad. Tales relaciones de dependencia trasladan el poder efectivo de decisión desde las autoridades nacionales hacia actores transnacionales, lo que dificulta el ejercicio pleno de soberanía digital[36].

Lo anterior es una práctica común que incrementa las vulnerabilidades. Basta recordar el caso del ciberataque con un *ransomware* sufrido por la empresa IFX Networks en 2023, que comprometió la infraestructura digital de más de 760 organizaciones en América Latina, incluyendo al menos 50 entidades públicas en Colombia. Entre las instituciones afectadas estuvieron el Ministerio de Salud, la Superintendencia Nacional de Salud, el Consejo Superior de la Judicatura y el Instituto Colombiano Agropecuario (ICA). Este incidente provocó la interrupción de servicios esenciales, como la plataforma MIPRES, del Ministerio de Salud, usada para la prescripción de tratamientos médicos, y diversos sistemas judiciales, lo que llevó a la suspensión de términos procesales en la Rama Judicial. Además, se calcula que más de 55 millones de datos del sector salud quedaron expuestos, lo cual encendió una alerta nacional sobre la vulnerabilidad de las infraestructuras críticas frente a amenazas cibernéticas[37].

Asimismo, el acceso a los recursos físicos necesarios para operar en el ciberespacio, como los minerales estratégicos para fabricar chips, es otro aspecto del ciberpoder que afecta la soberanía digital. Países con capacidad para controlar las cadenas de suministro global de tierras raras, como China, obtienen una ventaja estratégica que les permite condicionar la autonomía tecnológica de otros actores[38]. Así, el poder sobre los insumos digitales materiales constituye un vector clave de influencia geoeconómica.

La *ciberdiplomacia* surge como mecanismo complementario para proteger o disputar los mencionados elementos de soberanía. A través de acuerdos internacionales, normas multilaterales o alianzas estratégicas, los Estados intentan posicionarse en el debate global sobre gobernanza del ciberespacio buscando proteger su autonomía normativa y tecnológica. Esa dimensión del ciberpoder blando permite ejercer influencia en escenarios internacionales como la ONU, la ICANN o el Grupo de los 20 (G20) digital[39].

36 Cîrnu y Georgescu, "A complex system governance".
37 Portafolio, "IFX Networks sufrió ciberataque: estas son las entidades afectadas en Colombia", *Portafolio*, 13 de septiembre de 2023.
38 Comisión Europea, *Critical raw materials resilience*.
39 Barrinha y Renard, "Cyber-Diplomacy".

En América Latina, los déficits en infraestructura, regulación y capacidades técnicas limitan significativamente el ejercicio soberano en el entorno digital. La dependencia tecnológica de empresas extranjeras, la baja inversión en ciberseguridad y la escasa participación en los foros globales de gobernanza digital hacen que la región sea vulnerable a influencias externas y al ejercicio de ciberpoder foráneo[40]. Esas brechas deben ser reconocidas como desafíos estratégicos que requieren una respuesta integral basada en el desarrollo de capacidades soberanas.

Es importante destacar que la soberanía digital no se ejerce de manera absoluta ni unilateral, sino que se articula en un entramado global de interdependencias. Como señalan Braun y Hummel[41], la soberanía digital debe entenderse como un poder distribuido entre múltiples actores, incluidos Estados, empresas y ciudadanos, lo cual implica que ninguna entidad puede ejercer control absoluto sobre el entorno digital sin considerar las tensiones y ambivalencias inherentes al ecosistema global. Ello implica que incluso los Estados más poderosos deben negociar su espacio de autonomía digital frente a corporaciones, organismos internacionales y redes transnacionales. En el contexto descrito, la resiliencia normativa y técnica se vuelve un indicador de ciberpoder soberano[42].

En síntesis, el análisis de los elementos constitutivos de la soberanía digital, como infraestructura, datos, normas, tecnología e insumos estratégicos, permite concluir que todos ellos son susceptibles de ser controlados, protegidos o vulnerados por el ciberpoder. Dicha capacidad de incidencia configura un nuevo escenario estratégico, en el cual los Estados deben redefinir sus propias capacidades soberanas para evitar la subordinación a lógicas de dominación tecnológica ejercidas por actores externos; particularmente, grandes corporaciones tecnológicas y potencias hegemónicas[43]. Sin embargo, tal situación también representa una oportunidad: a mayor capacidad de proyección de ciberpoder, mayor será la posibilidad de ejercer soberanía digital de forma efectiva a nivel tanto nacional como internacional[44]. Por tanto, las estrategias estatales que busquen alinear y potenciar los elementos constitutivos del ciberpoder con los pilares de la soberanía digital contribuirán de manera mutua al fortalecimiento, sostenibilidad y autonomía tecnológica del Estado[45].

40 Aguilar, "Retos de América Latina".
41 Braun y Hummel, "Is Digital Sovereignty".
42 Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security* 38, núm. 2 (2013): 7-40.
43 Mügge, "EU AI Sovereignty".
44 Ayala, *Los ciberconflictos*.
45 Braun y Hummel, "Is Digital Sovereignty".

La Tabla 1 plantea un marco lógico donde se identifican relaciones entre poder digital y soberanía, y se proponen rutas estratégicas para que los Estados fortalezcan sus capacidades sin comprometer su autonomía. Como se ha señalado, el problema radica en la disolución y degradación del ciberpoder por la no asignación de recursos, ante la injerencia de actores nacionales y supranacionales. Esta vulnerabilidad se acentúa, asimismo, por la pérdida de control sobre infraestructura física, conectividad y protocolos, la desconfianza en las capacidades tecnológicas cibernéticas, o a la implantación de marcos regulatorios inadecuados. En concreto, es necesario mantenerse atentos a las relaciones que en la Tabla 1 se describen, además de poner especial cuidado a las acciones estratégicas recomendadas.

Tabla 1. Relación entre ciberpoder y soberanía digital y acciones recomendadas para generar sinergias

Elementos del ciberpoder	Elementos de la soberanía digital afectados	Tipo de relación	Acciones recomendadas para generar sinergia
Capacidades técnicas ofensivas y defensivas	Seguridad de redes nacionales y protección de activos digitales	Protección/ amenaza	Fortalecer capacidades nacionales en ciberdefensa y detección proactiva mediante la inversión en talento y tecnología.
Ciberdiplomacia y poder normativo	Autonomía normativa y participación en la gobernanza global	Legitimación/ imposición normativa	Impulsar la participación activa en foros multilaterales (ONU, ITU, ICANN) y promover acuerdos de gobernanza soberana.
Desarrollo y control de tecnologías emergentes	Autonomía tecnológica y desarrollo soberano de IA y sistemas críticos	Autonomización/ dependencia tecnológica	Establecer programas de investigación y desarrollo (I+D) nacionales y alianzas regionales para el desarrollo de tecnología propia.
Dominio sobre infraestructuras críticas digitales	Control sobre la conectividad nacional e integridad del tráfico de datos	Control soberano/ intervención externa	Promover la infraestructura digital estatal y esquemas de "soberanía compartida" con empresas bajo una regulación clara.
Acceso a insumos estratégicos (minerales, *hardware*)	Independencia de las cadenas de suministro tecnológicas	Autosuficiencia/ vulnerabilidad estructural	Diversificar proveedores, desarrollar capacidades locales de transformación y asegurar contratos estratégicos.
Capacidades de vigilancia, recolección y análisis de datos	Protección de datos personales y de la soberanía informacional	Resguardo de la privacidad/ vigilancia masiva	Establecer marcos robustos de protección de datos y exigencias de transparencia para plataformas digitales.

Fuente: elaboración propia, con base en referencias de Libicki y Aguilar[46].

[46] Martin Libicki, *Conquest in Cyberspace-National Security and Information Warfare* (Cambridge University Press, 2007); Aguilar, "Retos de América Latina".

La relación entre actores estatales y privados: hegemonía tecnológica y soberanía digital

En la arquitectura del ciberespacio la soberanía digital ha dejado de ser una prerrogativa exclusiva del Estado nación, para convertirse en un campo de disputa entre múltiples actores con capacidades desiguales. Aunque históricamente los Estados han detentado el monopolio del poder soberano, en el entorno digital deben compartir esa autoridad con corporaciones tecnológicas transnacionales que, al controlar infraestructuras críticas, flujos masivos de datos y sistemas algorítmicos de decisión, ejercen un poder fáctico comparable al de muchos gobiernos, o incluso superior[47]. Esa reconfiguración del poder socava los marcos tradicionales de gobernanza y plantea desafíos críticos para la legitimidad, la autonomía regulatoria y la capacidad de acción soberana en el ciberespacio. Esta realidad da pie a una tensión estructural entre el principio de soberanía y la lógica de mercado global, donde la titularidad del ciberpoder no obedece a reglas estatales, sino a capacidades tecnológicas y económicas concentradas[48].

Autores como Nye[49] han advertido que el poder en el entorno digital se difunde más ampliamente que en los dominios tradicionales, y ello dificulta a los Estados mantener el monopolio de las funciones soberanas. En ese marco, empresas como Google, Meta, Amazon, Microsoft o Huawei no solo ofrecen servicios tecnológicos, sino que modelan ecosistemas digitales, condicionan la regulación de datos, intermedian en la provisión de ciberseguridad y controlan flujos globales de información, y así erosionan la capacidad estatal para ejercer un control autónomo sobre los elementos esenciales de su soberanía digital[50].

A su vez, el ascenso de las potencias tecnológicas ha dado lugar a formas de competencia geoeconómica que transforman el ciberespacio en un campo de batalla por la hegemonía digital. Estados Unidos, China y Rusia protagonizan una carrera por el dominio de tecnologías emergentes —IA, computación cuántica, redes 5G— con una marcada estrategia de aseguramiento de insumos estratégicos como tierras raras, litio y semiconductores. Dicha pugna no solo tiene implicaciones económicas, sino que redefine la arquitectura del poder mundial, pues las capacidades tecnológicas permiten ejercer formas de influencia, vigilancia y control que trascienden las

47 Braun y Hummel, "Is Digital Sovereignty"; Mügge, "EU AI Sovereignty".
48 Blount, *"Reprogramando el mundo"*.
49 Nye, "Cyber power".
50 Realpe. "La ciberdiplomacia".

fronteras físicas[51]. En ese sentido, la soberanía digital de los países del Sur Global —y en particular, la de América Latina— se ve comprometida por su limitada capacidad de producción tecnológica, su dependencia de infraestructuras foráneas y su rezago en normativas de protección de datos. Tal como plantea Realpe[52], la ciberdiplomacia emerge como herramienta clave para mediar estas tensiones promoviendo la creación de estándares internacionales que respeten la soberanía digital y fortalezcan las capacidades nacionales frente a los actores tecnológicos dominantes.

Las plataformas digitales privadas ejercen una forma de "soberanía algorítmica" estableciendo de facto normas de comportamiento, moderación de contenidos, privacidad y seguridad sin mayor participación de los Estados. Tal situación genera un desbalance que cuestiona la legitimidad de los marcos jurídicos nacionales. La colaboración entre actores estatales y privados es, por eso mismo, ambivalente: por un lado, permite proveer capacidades tecnológicas; por otro, puede derivar en una cesión de soberanía si no hay de por medio mecanismos regulatorios sólidos[53]. A ello se suma, a su vez, la dificultad de imponer normas globales en un espacio tan fragmentado. Mientras algunas potencias promueven un "internet soberano" y otras defienden un "ciberespacio abierto", la falta de consensos multilaterales facilita que las grandes corporaciones actúen conforme a intereses comerciales y, por tanto, subordinen derechos como la privacidad, la autonomía y la equidad digital. Esa divergencia ha motivado propuestas para una gobernanza policéntrica, basada en el multilateralismo y en principios de justicia digital[54].

Además, la fragmentación normativa permite que los Estados con mayor ciberpoder impongan sus reglas a través de acuerdos bilaterales, cláusulas extraterritoriales o tecnologías con estándares predeterminados. Ello afecta en especial a países sin capacidad para desarrollar soluciones propias, que terminan adoptando sistemas con *backdoors*, lógicas de extracción de datos o dependencias de mantenimiento externo. Esa es una nueva forma de neocolonialismo digital, según ha sido señalado por enfoques críticos desde el Sur Global[55].

51 Beatriz Tiusabá, "La Transformación del Concepto de Ciberespacio en Estados Unidos: la Importancia de la Ciberseguridad y la Implementación del Ciberpoder" (Tesis de maestría, Universidad Militar Nueva Granada, 2023).

52 Realpe. "La ciberdiplomacia".

53 Tiusabá, "La Transformación del Concepto".

54 Amel Attatfa, Karen Renaud y Stefano De Paoli, "Cyber Diplomacy: A Systematic Literature Review", *Procedia Computer Science* 176 (2020): 60-69.

55 Tiusabá, "La Transformación del Concepto".

Por otra parte, hay casos en los que los Estados han delegado funciones de interés estratégico en empresas privadas, como en la provisión de ciberseguridad, servicios en la nube o gestión de infraestructuras críticas. Si bien eso puede mejorar la eficiencia operativa, también expone vulnerabilidades ante conflictos de intereses, amenazas internas o intervenciones externas. La estrategia debe, por tanto, buscar un equilibrio entre colaboración público-privada y garantía de control estatal soberano[56].

Hay, además, razones objetivas por las cuales es imperativo ejercer control, regulación y soberanía sobre el ciberespacio y los datos que son propiedad de ciudadanos y comunidades sociales y políticas, así como sobre la información de empresas privadas, a la par que se siguen y fijan normas mínimas, pero eficaces, para el uso del ciberespacio, tendientes a disminuir las inequidades y posiciones hegemónicas y de poder de algunos actores. La soberanía digital, desde esta perspectiva tradicional, presupone la acción intencional de personas, organizaciones o instituciones que buscan participar, influir o, de alguna manera, adquirir parte del control orgánico que reside en el entorno tecnológico. Sin embargo, ante la aceleración en el desarrollo de la IA, se suma un agente que puede tener poca intención de cooperar y cambie las vías legítimas de ejercer soberanía, o que, incluso, transforme sus elementos constitutivos. Al respecto, en su artículo "La violencia de los algoritmos", Owen[57] expresaba desde 2015 su preocupación por Palantir, un programa espía novedoso para la época. El autor explicaba que, aunque el sistema fuera programado por humanos, contenía riesgos de que los *outputs* fueran interpretados mal por el algoritmo, o de que las decisiones acerca de a quién declarar terrorista o enemigo del Estado recayeran exclusivamente en la máquina, lo que conduciría a una preocupante automatización de la violencia:

> Palantir es una ventana a la reflexión del Estado sobre la tecnología. Amenazados por el creciente poder de actores digitales percibidos como nefastos, los estados occidentales han buscado controlar la propia red para, como afirman en documentos filtrados por Edward Snowden, «Recopilarlo todo; Procesarlo todo; Explotarlo todo; Asociarlo todo; Olfatearlo todo; Saberlo todo». Cada vez más, estas herramientas, y los algoritmos que las impulsan, se utilizan para automatizar la violencia[58].

En síntesis, el papel de los actores privados en el ecosistema digital es decisivo, pero problemático. Su potencial para contribuir al fortalecimiento del ciberpoder

[56] Realpe. "La ciberdiplomacia".
[57] Taylor Owen, "The violence of algorithms", *Foreign Affairs Magazine,* 25 de Mayo de 2015.
[58] Owen, "The violence of algorithms".

estatal debe estar condicionado a un marco regulatorio claro, políticas de soberanía tecnológica, mecanismos de transparencia y un enfoque en cooperación estructurada. El desafío es diseñar alianzas que no comprometan la autonomía, sino que la refuercen estableciendo salvaguardas para evitar la captura de funciones soberanas por intereses corporativos globales[59]. A la par, debe regularse la creciente automatización y responsabilidad delegada en la IA, pues, *a priori*, resulta evidente la observación de que mientras más control tenga la IA, habrá menos gobernanza y soberanía legítima sobre el ciberespacio.

Dinámicas del ciberpoder sobre la soberanía digital: mecanismos de acción y consolidación estratégica

Si bien ya fue establecida la relación de fuerte interdependencia entre ciberpoder y soberanía digital, y aunque es recomendable, incluso, promover la sinergia funcional entre los componentes de ambos, también es cierto que el ciberpoder es el dinamizador y gestor legítimo de las actividades que configuran la soberanía en el ciberespacio, como, por ejemplo, el marco regulatorio. Además, quien detenta el poder y la autoridad oficial o delegada para consolidar el ciberpoder estatal es quien puede incidir directa y formalmente sobre la estrategia a través de la cual se extiende el control y se consolida la gobernanza digital en cada país; en virtud de ello, se argumentará en torno a esa relación preponderante y cómo se despliegan las acciones para obtener ventaja en dicho escenario contendido.

El ciberpoder constituye, no una noción abstracta, sino una realidad operativa con capacidad tangible para transformar estructuras de poder y redefinir competencias soberanas. Su ejercicio demanda la articulación estratégica de capacidades técnicas, normativas, diplomáticas y militares, las cuales permiten a los Estados incidir en el entorno digital, salvaguardar sus intereses nacionales y proyectar su autoridad sobre dominios intangibles, como el flujo de datos, la infraestructura crítica y la opinión pública digital. De esta forma, el ciberpoder actúa de forma directa sobre los elementos constitutivos de la soberanía digital, como la autonomía tecnológica, la capacidad normativa y la gobernanza de infraestructuras digitales[60].

Uno de los principales mecanismos mediante los cuales el ciberpoder incide sobre la soberanía es la *proyección de influencia estratégica en la formulación de normas*

[59] Nye, "Cyber power"; Blount, "*Reprogramando el mundo*".
[60] Realpe, "La ciberdiplomacia".

internacionales. A través de la ciberdiplomacia, los Estados con mayores capacidades buscan legitimar sus intereses en el diseño de esquemas de ciberseguridad, protección de datos, gobernanza de internet y regulación de contenidos. Esa dimensión normativa del ciberpoder permite moldear el entorno digital global de acuerdo con intereses nacionales y consolida así una forma de soberanía difusa, pero efectiva[61].

La *construcción de capacidades nacionales de ciberdefensa y ciberseguridad* constituye otro vector del ciberpoder. Estados como Israel, China y Estados Unidos han desarrollado ecosistemas robustos de defensa digital que no solo previenen ataques, sino actúan como instrumentos de disuasión y proyección internacional. El caso colombiano, por ejemplo, fija la ciberdefensa como un componente estratégico para salvaguardar la soberanía, entendida como la capacidad estatal para anticipar y contrarrestar amenazas digitales que afecten la integridad nacional[62].

Asimismo, el *control de la infraestructura crítica de conectividad y almacenamiento de datos* ha adquirido un carácter soberano. La localización de servidores, el desarrollo de nubes nacionales, la encriptación estatal y el diseño de protocolos propios son prácticas que ilustran cómo el ciberpoder se emplea para evitar la dependencia tecnológica y asegurar el control de la información estratégica. Países como China, con su política de "cibersoberanía", han ejemplificado la posibilidad de consolidar un ecosistema digital propio como medio de defensa ante la intromisión de actores externos[63].

El *dominio sobre los flujos de información y los contenidos digitales* constituye otra dimensión crítica. A través de mecanismos de IA, vigilancia algorítmica y manipulación de narrativas, algunos Estados despliegan ciberpoder para incidir en las percepciones públicas tanto internas como externas, y reforzar así la cohesión nacional o erosionar la legitimidad de sus adversarios. Dicha dimensión se asocia con la guerra cognitiva y la influencia informacional como elementos clave del poder nacional[64].

---

61 Realpe, "La ciberdiplomacia"; Daniel Dumitru y Cristina Bodoni, "Extension of international humanitarian law order in the information area through digital diplomacy", *Strategic Impact* 80, núm. 4 (2021): 86-102.

62 Colombia, Departamento Nacional de Planeación, Lineamientos de política para ciberseguridad y ciberdefensa, CONPES 3701 (Bogotá: DNP, 14 de julio de 2011).

63 Johan Eriksson y Giacomello Giampiero, "Cyberspace in space: Fragmentation, vulnerability, and uncertainty", en *Cyber security politics Socio-Technological Transformations and Political Fragmentation*, ed. Myriam Dunn Cavelty y Andreas Wenger (Routledge, 2022), 95-107.

64 Tiusabá, "La Transformación del Concepto".

Por otro lado, el *fortalecimiento de capacidades institucionales internas* a través de agencias especializadas, protocolos de gestión de incidentes y programas de formación digital también permite consolidar soberanía. El ciberpoder se expresa aquí como capacidad para ordenar el ciberespacio nacional, establecer responsabilidades claras y reaccionar con eficacia frente a contingencias, ataques o crisis en el dominio digital[65].

En el contexto descrito, la *interdependencia entre ciberpoder y ciberdiplomacia* resulta estratégica. La capacidad de una nación para participar en escenarios multilaterales, definir posiciones sobre las normas, apoyar capacidades de terceros y formar alianzas selectivas refuerza su posición soberana y le permite actuar no solo en defensa, sino en ofensiva diplomática. Promover acuerdos sobre ciberseguridad, cooperación tecnológica y gobernanza digital se convierte, entonces, en una extensión legítima del ciberpoder[66].

Por último, la *apropiación crítica de tecnologías emergentes*, como la IA, la *blockchain* y la computación cuántica debe entenderse como un imperativo soberano. Si bien dichas tecnologías pueden fortalecer el ciberpoder de los Estados, también plantean riesgos si son adoptadas sin control, dependiendo de proveedores externos o sin marcos éticos. La consolidación de la soberanía digital pasa por la capacidad para diseñar, adaptar y regular estos desarrollos desde una lógica nacional[67].

En suma, el ciberpoder se manifiesta como un conjunto de capacidades activas, estratégicamente organizadas para actuar sobre los elementos que constituyen la soberanía digital. No se trata de tan solo proteger infraestructuras o impedir ataques, sino de construir proactivamente la arquitectura reglamentaria, institucional y tecnológica que permita a los Estados ejercer control autónomo, influir en el orden digital global y preservar la integridad de sus decisiones soberanas en un entorno cada vez más interdependiente. Así, la postura que reconoce la necesidad de generar sinergias entre ciberpoder y soberanía digital se contrasta y complementa con otra que reconoce la mayor influencia del ciberpoder, en un escenario donde ambas son funcionales y pueden operar alternativamente en contextos determinados, según como las circunstancias lo indiquen.

65 Realpe, "La ciberdiplomacia"; Jorge Vega, "Ciberdiplomacia en América Latina: niveles, enfoques y velocidades", *Real Instituto Elcano,* núm. 38 (2023).

66 Realpe, "La ciberdiplomacia"; Barrinha y Renard, "Cyber-Diplomacy".

67 Tiusabá, "La Transformación del Concepto".

Conclusiones

El problema que orientó la presente investigación se centró en la dificultad conceptual y estratégica de establecer una relación unívoca entre ciberpoder y soberanía digital. A diferencia de otros dominios del poder estatal, el ciberespacio no permite aplicar de manera directa categorías tradicionales de soberanía, ya que los límites territoriales, jurídicos y políticos se disuelven en una red global regida por infraestructuras distribuidas, actores no estatales y estándares transnacionales. En ese contexto, la relación entre ciberpoder y soberanía digital es mediada por dinámicas de interdependencia tecnológica y normativas impuestas por actores con capacidades hegemónicas, lo que transforma la soberanía en un ejercicio condicionado por la arquitectura del poder digital global.

La tesis según la cual cuando el ciberpoder se configura como capacidad estratégica integral permite consolidar la soberanía digital fue demostrada analizando los elementos estructurales sobre los que este poder actúa. Se evidenció que el ciberpoder, lejos de ser tan solo una herramienta de defensa frente a amenazas externas, puede y debe ser orientado a construir un espacio digital soberano mediante el dominio de infraestructuras críticas, el control normativo, la proyección diplomática y la apropiación tecnológica. En consecuencia, la soberanía digital no puede ejercerse de forma efectiva sin un ciberpoder robusto, articulado y adaptativo.

En relación con el primer objetivo específico, se identificó que los elementos estructurales de la soberanía digital —infraestructura, datos, regulación y tecnología— se hallan expuestos a intervenciones directas del ciberpoder, tanto en su dimensión protectora como en su capacidad de control. Dicha exposición no es accidental, sino estructural, ya que se relaciona con la naturaleza misma del entorno digital, en el que la dependencia técnica, la circulación transfronteriza de datos y la gobernanza externa reducen la autonomía estatal si no existen capacidades propias para actuar sobre dichos elementos.

En cuanto al segundo objetivo específico, se demostró que los actores privados —en especial, las corporaciones tecnológicas globales— poseen capacidades que sobrepasan las de muchos Estados en términos de procesamiento de datos, control de infraestructuras, influencia normativa y desarrollo de tecnologías críticas. Esa situación configura una asimetría estructural en la que el ejercicio de soberanía digital

por parte de los Estados se ve condicionado por marcos regulatorios, tecnologías y plataformas diseñadas fuera de su jurisdicción. Tal dependencia compromete la autonomía política, jurídica y estratégica, y constituye, por ende, una forma de subordinación digital.

Respecto al tercer objetivo específico, se encontró que el ciberpoder se manifiesta por medio de mecanismos concretos que inciden sobre la soberanía digital: el control de infraestructuras nacionales, la formulación normativa, la defensa cibernética, la acción diplomática en foros internacionales y la adopción crítica de tecnologías emergentes. Cuando dichos mecanismos van articulados a una estrategia de Estado, permiten determinar márgenes efectivos de soberanía, no como aislamiento técnico, sino como capacidad autónoma de decisión, regulación y protección de los intereses nacionales en el entorno digital.

Un aspecto particular que merece resaltarse es la incorporación acelerada de la IA en los sistemas digitales, que redefine profundamente tanto la configuración del ciberpoder como las condiciones para ejercer soberanía digital. La automatización de procesos críticos —como la detección de amenazas, la clasificación de datos, la toma de decisiones operativas y la vigilancia algorítmica— introduce nuevos vectores de poder que ya no requieren mediación humana constante. En ese marco, el control sobre los algoritmos, la infraestructura computacional y los modelos de IA se convierte en una condición indispensable para ejercer ciberpoder soberano. A su vez, la falta de capacidad para auditar, desarrollar o adaptar de forma autónoma dichas tecnologías amplía la brecha entre Estados dominantes y dependientes, y transfiere el eje de soberanía desde el control territorial al control del código, del dato y de la automatización.

Finalmente, artículo demostró que el ciberpoder no es una amenaza intrínseca a la soberanía, sino un recurso clave para su afirmación. La soberanía digital no se reduce al aislamiento técnico ni al proteccionismo informático, sino que implica una gobernanza activa del entorno digital, sustentada en capacidades propias, normas claras, marcos éticos y alianzas multilaterales inteligentes. El gran desafío para los Estados no es solo defenderse de ciberamenazas externas, sino transformarse internamente para ejercer poder legítimo y autónomo en un entorno transnacional, descentralizado e interconectado, que incluye actores no estatales relevantes como las empresas privadas, las cuales también deben integrarse bajo un solo liderazgo y conformar un ecosistema digital identitario.

Bibliografía

Academia de e-Gobernanza de Estonia. "NCSI Index". National Cyber Security Index. https://ncsi.ega.ee/ncsi-index/ (fecha de consulta: 19 de mayo de 2026).

Aguilar, Juan. "China y Estados Unidos: Antagonismos Y Liderazgos En El Ciberespacio Frente a América Latina". *URVIO. Revista Latinoamericana De Estudios De Seguridad*, núm. 36 (2024): 66-84. https://doi.org/10.17141/urvio.36.2023.5845.

Aguilar, Juan. "Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030". *Revista Seguridad y Estrategia* 1, núm. 2 (2023): 40-55. https://ciberprisma.org/2023/08/19/retos-de-america-latina-para-la-construccion-de-una-politica-nacional-de-ciberseguridad-una-apuesta-a-2030/

Attatfa, Amel, Karen Renaud y Stefano De Paoli. "Cyber Diplomacy: A Systematic Literature Review". *Procedia Computer Science* 176 (2020): 60-69. https://doi.org/10.1016/j.procs.2020.08.007

Ayala, Javier. *Los ciberconflictos a la luz del Derecho Internacional Humanitario.* Bogotá: Grupo Editorial Ibáñez, 2018.

Barrinha, André y Thomas Renard. "Cyber-Diplomacy: The Making of an International Society in the Digital Age". *Global Affairs* 3, núms. 4-5 (2017): 353-364. doi:10.1080/23340460.2017.1414924.

Berger, Peter y Thomas Luckmann. *La construcción social de la realidad.* Amorrortu, 1997.

Betz, Daniel y Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power.* Routledge, 2011.

Blount, Patrick J. *Reprogramando el mundo: el ciberespacio y la geografía del orden global.* Bristol: Prensa de e-Relaciones Internacionales, 2019.

Blumenthal, Dan y Linda Zhang. "Censura, propaganda y desinformación en China". American Enterprise Institute (AEI), 10 de julio de 2020. https://www.aei.org/articles/chinas-censorship-propaganda-disinformation/

Braun, Matthias y Patrik Hummel. "Is Digital Sovereignty Normatively Desirable?". *Information, Communication & Society,* (2024): 1–14. doi:10.1080/1369118X.2024.2332624.

Cîrnu, Carmen y Alexandru Georgescu. "A complex system governance theory". *Studies in Informatics and Control* 32, núm. 2 (2023): 127-136. https://doi.org/10.24846/v32i2y202312

Colombia, Departamento Nacional de Planeación. *Lineamientos de política para ciberseguridad y ciberdefensa.* CONPES 3701. Bogotá: DNP, 14 de julio de 2011. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Dumitru, Daniel y Cristina Bodoni. "Extension of international humanitarian law order in the information area through digital diplomacy". *Strategic Impact* 80, núm. 4 (2021): 86-102.

Eriksson, Johan y Giacomello, Giampiero. "Cyberspace in space: Fragmentation, vulnerability, and uncertainty". En *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*, editado por Myriam Dunn Cavelty y Andreas Wenger, 95-107. Routledge, 2022.

Flick, Uwe. *Introducción a la investigación cualitativa*. Ediciones Morata, 2004.

Flonk, Daniëlle, Markus Jachtenfuchs y Anke Obendiek. "Controlling Internet Content in the EU: Towards Digital Sovereignty". *Journal of European Public Policy* 31, núm. 8 (2024): 2316-2342. doi:10.1080/13501763.2024.2309179.

Francia, Senado. *Rapport d'information fait au nom de la commission d'enquête sur la souveraineté numérique* [Informe de información realizado en nombre de la comisión de investigación sobre la soberanía digital]. Núm. 7 (2019-2020). Por Gérard Longuet. París: Senado, 2019. (fecha de consulta: 19 de mayo de 2026).

Giles, Keir. *Handbook of Russian Information Warfare*. NATO Defense College, 2016. https://www.ndc.nato.int/news/news.php?icode=1186

Guzzini, Stefano. "A reconstruction of constructivism in international relations". *European Journal of International Relations* 6, núm. 2 (2000): 147-182. https://doi.org/10.1177/1354066100006002001

Hopf, Ted. "The promise of constructivism in international relations theory". *International Security* 23, núm. 1 (1998): 171-200. https://doi.org/10.2307/25392671998.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft". *International Security* 38, núm. 2 (2013): 7-40. http://www.jstor.org/stable/24480929

Kittichaisaree, Kriangsak. *Public International Law of Cyberspaces*. Springer, 2017.

Kuehl, Daniel. "From cyberspace to cyberpower: Defining the problem". En *Cyberpower and national security*, editado por Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz, 24-42. National Defense University Press, 2009.

Libicki, Martin. *Conquest in cyberspace: National security and information warfare*. Cambridge University Press, 2007.

Mügge, Daniel. "EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?". *Journal of European Public Policy* 31, núm. 8 (2024): 2200-2225. doi:10.1080/1350 1763.2024.2318475.

Nye, Joseph, "Cyber power". Cambridge: Universidad de Harvard, Escuela gubernamental John F. Kennedy, Centro Belfer para la Ciencia y Asuntos Internacionales, mayo de 2010. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf

Nye, Joseph. *The future of power*. Nueva York: PublicAffairs, 2011.

Owen, Taylor. "The violence of algorithms". *Foreign Affairs Magazine*, 25 de Mayo de 2015. https://www.foreignaffairs.com/world/violence-algorithms

Parker, Kevin L. "El uso del ciberpoder". *Military Review*, ed. hispanoamericana, mayo-agosto (2014): 50-63. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20140831_art009SPA.pdf (fecha de consulta: 19 de mayo de 2026).

Portafolio. "IFX Networks sufrió ciberataque: estas son las entidades afectadas en Colombia". *Portafolio,* 13 de septiembre de 2023. https://www.portafolio.co/negocios/ifx-networks-sufrio-ciberataque-estas-son-las-entidades-afectadas-en-colombia-595171

Realpe, Milena. "La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de intereses nacionales". *Novum Jus* 18, núm. 2 (2024): 279-304. https://doi.org/10.14718/NovumJus.2024.18.2.11

Sautu, Ruth. *El método biográfico. La reconstrucción de la sociedad a partir del testimonio.* Ediciones Lumiere, 2023.

Segal, Adam. "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace". *NBR Special Report* núm. 87 (2020). https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

Tidy, Joe. "Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente". *BBC News*, 24 de marzo de 2022. https://www.bbc.com/mundo/noticias-60850173

Tiusabá, Beatriz. "La Transformación del Concepto de Ciberespacio en Estados Unidos: la Importancia de la Ciberseguridad y la Implementación del Ciberpoder" (Tesis de maestría, Universidad Militar Nueva Granada, 2023).

Unión Europea, Comisión Europea. *Critical raw materials resilience: Charting a path towards greater security and sustainability* [Resiliencia de las materias primas fundamentales: Trazando un camino hacia una mayor seguridad y sostenibilidad]. COM(2020) 474 final. Bruselas: Comisión Europea, 2 de septiembre de 2020. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0474

Unión Internacional de Telecomunicaciones. *Global Cybersecurity Index 2020* [Índice global de ciberseguridad 2020]. Ginebra: Unión Internacional de Telecomunicaciones, junio de 2021. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

Vea, Javier. "Introducción a la guerra no cinética". *Revista de aeronáutica y astronáutica,* núm. 915 (2022): 708-719. https://dialnet.unirioja.es/servlet/articulo?codigo=9800514

Vega, Jorge. "Ciberdiplomacia en América Latina: niveles, enfoques y velocidades". *Real Instituto Elcano,* núm. 38 (2023). https://media.realinstitutoelcano.org/wp-content/uploads/2023/05/ari38-2023-vega-ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades.pdf

Xuetong, Yan. *Leadership and the rise of great powers.* Princeton:Princeton University Press, 2019.