

Más allá de las fronteras

El ciberespacio como nuevo escenario del poder geopolítico

DOI: 10.29236/sistemas.n180a7

Resumen

El ciberespacio dejó de ser un soporte técnico de la vida social para convertirse en un escenario donde se disputa el poder entre Estados. Este artículo sostiene que la digitalización no anula la geografía política: la estratifica. Bajo la aparente desterritorialización de los flujos de datos persiste una geografía densa —cables submarinos, puntos de aterrizaje, centros de datos, cadenas de suministro de semiconductores— cuyo control produce dependencia y, por lo tanto, poder. A partir de una revisión de literatura especializada, doctrina militar, instrumentos de gobernanza internacional y evidencia empírica del periodo 2022-2026, se propone un modelo de análisis articulado en tres vectores de ciberpoder: infraestructural, normativo y cognitivo. El modelo se aplica al caso colombiano, una potencia media bioceánica con nueve puntos de aterrizaje de cable submarino, alta dependencia tecnológica externa y capacidades institucionales en consolidación. Se concluye que el ciberespacio no inaugura una guerra distinta, sino una gramática distinta del conflicto: persistente, ambigua y situada por debajo del umbral del ataque armado. Para las potencias medias, la autonomía estratégica dependerá menos de la fuerza acumulada que de la capacidad de anticipación.

Palabras clave

Geopolítica; ciberespacio; ciberpoder; soberanía digital; infraestructura crítica cibernética.

Introducción

Durante más de un siglo, la geopolítica pensó el poder desde la geografía. Mahan situó la clave del predominio en el control de las líneas de comunicación marítima; Mackinder (1904) la desplazó al corazón continental euroasiático; Spykman la reubicó en los bordes. Distintas como son, estas tradiciones comparten una intuición: el poder no se distribuye de manera uniforme sobre el espacio, sino que se concentra en aquellos lugares por donde necesariamente deben pasar los flujos que sostienen la vida económica y militar de las naciones.

El ciberespacio parecía haber roto esa lógica. La promesa fundacional de la red era la de un dominio instantáneo, ubicuo y desterritorializado, ajeno a la soberanía de los Estados. "Los gobiernos del mundo industrial —escribía Barlow (1996)— no son bienvenidos entre nosotros.

No tienen soberanía donde nos reunimos". Tres décadas después, el diagnóstico se invirtió. Los Estados regresaron al ciberespacio, no como intrusos, sino como sus principales arquitectos: legislan sobre datos, subsidian semiconductores, tienden cables, patrullan lechos marinos y desarrollan capacidades militares específicas para el dominio (Perafán Del Campo et al., 2021). Lo que parecía un espacio

sin geografía resultó ser un espacio con una geografía nueva, superpuesta a la anterior y no menos disputada, donde emergen "fronteras virtuales" que no coinciden con las líneas del mapa, pero organizan identidades, flujos y lealtades (García-Jiménez et al., 2010).

Este artículo sostiene una tesis deliberadamente contraintuitiva: la digitalización no anula la geografía política, la estratifica. La aparente inmaterialidad de los datos descansa sobre una infraestructura físicamente localizada, jurídicamente sometida a jurisdicciones concretas y económicamente concentrada en pocas manos. Quien controla esa infraestructura no domina un territorio, pero sí determina las condiciones de posibilidad de la actividad ajena. Esa es, en sentido estricto, una forma de poder geopolítico.

La pregunta que anima este número —si las tecnologías de la información inauguran una nueva perspectiva de la guerra— admite una respuesta matizada. El argumento que aquí se desarrolla es que el ciberespacio no produce una guerra distinta, sino una gramática distinta del conflicto: persistente en el tiempo, ambigua en la atribución y deliberadamente situada por debajo del umbral que activa las respuestas del derecho internacional. Menos una nueva guerra que una

nueva manera de competir sin declararla.

El texto avanza en cinco movimientos: el marco conceptual y el modelo de los tres vectores de ciberpoder, la materialidad del dominio, el debate sobre su carácter bélico, la disputa por las reglas globales y la aplicación al caso colombiano.

De Mackinder al Heartland cibernético: tres vectores de ciberpoder

La doctrina militar describe el ciberespacio como un dominio operacional compuesto por tres capas interdependientes: una capa física —cables, servidores, dispositivos, con coordenadas y propietarios—, una capa lógica —protocolos, direccionamiento, software— y una capa ciber-persona, donde residen las identidades digitales de individuos y organizaciones (United States Joint Staff, 2018). Esta arquitectura estratificada es más que una convención técnica: es el punto de partida de cualquier análisis geopolítico serio, porque cada capa habilita un tipo distinto de poder y admite un tipo distinto de disputa.

Prado (2018) propuso leer esta configuración en clave mackinderiana y hablar de un *Heartland* cibernético: el conjunto de nodos cuyo control confiere ventaja estructural sobre la red. La analogía es fértil, pero exige una precisión. El Heartland euroasiático era un dato de la naturaleza; el cibernético es un artefacto que se construye, se financia, se

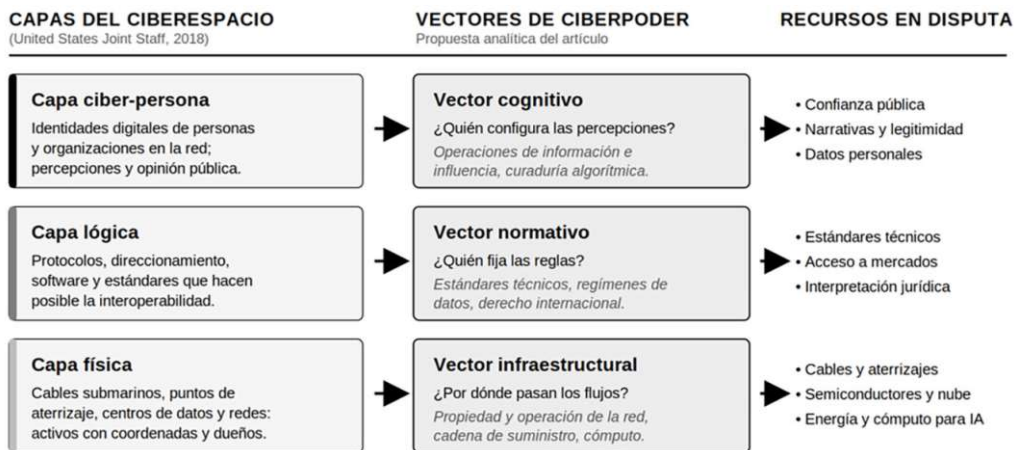
traslada y a veces se destruye. Esa reversibilidad es justamente lo que lo convierte en objeto de política pública y de estrategia, y no solo de descripción.

Sobre esta base es posible ordenar analíticamente el ciberpoder —la capacidad de un actor de obtener resultados preferidos mediante el uso de recursos electrónicamente interconectados (Nye, 2011)— en tres vectores complementarios, que constituyen la propuesta analítica de este artículo y se sintetizan en la Figura 1. La agregación de estos vectores es lo que los índices comparados intentan capturar cuando ordenan a los Estados por capacidad e intención cibernéticas (Voo et al., 2022), y lo que la literatura latinoamericana reciente ha discutido bajo las categorías de ciberpoder, cibersoberanía y ciberdiplomacia (Bartolomé, 2023).

El **vector infraestructural** opera sobre la capa física y responde a la pregunta por dónde pasan los flujos: propiedad de cables submarinos y puntos de aterrizaje, localización de centros de datos, control de la cadena de suministro de semiconductores y disponibilidad de cómputo para inteligencia artificial. Es el vector más cercano a la geopolítica clásica y, por eso mismo, el más subestimado por los análisis que insisten en la inmaterialidad de lo digital.

El **vector normativo** opera sobre la capa lógica y responde a la pre-

Figura 1. Modelo de análisis geopolítico del ciberespacio: capas, vectores de ciberpoder y recursos en disputa.



Nota. Elaboración propia a partir de la arquitectura de capas de United States Joint Staff (2018) y del concepto de ciberpoder de Nye (2011).

gunta quién fija las reglas: estándares técnicos, regímenes de protección de datos, condiciones de acceso a mercados digitales, posición de cada Estado sobre el derecho internacional aplicable y presencia en los foros donde eso se negocia. Bradford (2020) mostró que la capacidad regulatoria se proyecta extraterritorialmente sin coerción alguna: basta con controlar el acceso a un mercado suficientemente grande para que las normas propias se vuelvan estándar ajeno.

El **vector cognitivo** opera sobre la capa ciber-persona y responde a la pregunta quién configura las percepciones: operaciones de información e influencia, manipulación algorítmica de la conversación pública y uso de la desinformación como herramienta de política exte-

rior. Es donde la asimetría es mayor: actores con recursos modestos generan efectos desproporcionados sobre sociedades altamente conectadas.

Estos vectores no son compartimentos estancos: su valor analítico reside en la interacción. El sabotaje de un cable submarino (infraestructural) resulta rentable porque la ambigüedad jurídica sobre su calificación (normativo) impide una respuesta contundente, mientras la incertidumbre alimenta narrativas de vulnerabilidad (cognitivo). El ciberpoder efectivo es el producto, no la suma, de los tres.

La materialidad del poder: cables, chips y nubes

Nada revela mejor la persistencia de la geografía que la infraestructu-

ra submarina. Aproximadamente el 99 % del tráfico mundial de internet viaja por más de quinientos sistemas de cable de fibra óptica tendidos sobre el lecho marino, no por satélite; solo en 2024 se instalaron cerca de 200.000 kilómetros de cable nuevo, y en 2025 se ejecutaron más de 170 reparaciones, un promedio cercano a cuatro fallas por semana (Unión Internacional de Telecomunicaciones, 2025).

Esta arquitectura reproduce, con notable fidelidad, los cuellos de botella de la geografía marítima clásica: el mar Rojo, el estrecho de Malaca, el canal de Sicilia o el golfo de Finlandia concentran haces de cables cuya interrupción simultánea produce efectos regionales inmediatos.

Los años recientes convirtieron esa vulnerabilidad teórica en un problema operacional. Entre el 17 y el 18 de noviembre de 2024, los cables BCS East-West Interlink (Lituania-Suecia) y C-Lion1 (Finlandia-Alemania) fueron seccionados en el mar Báltico; las investigaciones señalaron al buque *Yi Peng 3*, que había apagado su sistema de identificación automática durante siete horas y media al cruzar la zona del incidente. En febrero de 2025 se registraron nuevos daños en la misma cuenca. La respuesta fue instructiva: en enero de 2025 la OTAN activó la misión *Baltic Sentry* para la protección de infraestructura crítica submarina, desplegando medios navales, aéreos y sistemas

no tripulados en una tarea que hasta hace poco se habría considerado ajena a una alianza militar (Organización del Tratado del Atlántico Norte, 2025). La protección de un cable de telecomunicaciones se volvió, literalmente, una misión de defensa colectiva.

Lo relevante de estos episodios no es el daño causado —los cables fueron reparados en días o semanas— sino su gramática: acciones de bajo costo, ejecutadas por medios civiles, jurídicamente ambiguas, difícilmente atribuibles y con efectos económicos y psicológicos desproporcionados. Es el patrón característico de la conflictividad contemporánea en el ciberespacio.

El vector infraestructural no se agota en los cables. La disputa por los semiconductores avanzados —donde un puñado de empresas concentra diseño, fabricación y maquinaria litográfica— convirtió los controles de exportación en instrumento de política exterior de primer orden, y algo análogo ocurre con el cómputo para inteligencia artificial y la nube, cuya concentración hipoteca la autonomía de Estados enteros. La Ruta de la Seda Digital china y las iniciativas occidentales de conectividad segura compiten por equipar las redes del Sur global, incluida América Latina, sabiendo que quien instala la infraestructura fija los estándares y accede a los datos durante décadas (Rivas, 2021; Mata-Sánchez, 2023).

Para las potencias medias la implicación es incómoda: la conectividad, presentada como bien público y factor de desarrollo, es a la vez un vector de dependencia. No hay soberanía digital sin respuesta explícita a quién construye, opera y puede interrumpir la infraestructura sobre la que descansa la economía nacional.

¿Una nueva perspectiva de la guerra?

La pregunta por el carácter bélico del ciberespacio tiene ya dos décadas de debate. Rid (2013) argumentó que ninguna operación cibernética conocida satisface los tres criterios clausewitzianos de la guerra —violencia, instrumentalidad y carácter político atribuido— y que lo observado es sabotaje, espionaje y subversión potenciados por medios digitales. Kello (2017) replicó que esa conclusión, técnicamente correcta, oscurece el fenómeno relevante: un estado intermedio de "paz inestable" que erosiona el orden internacional sin cruzar el umbral de la guerra. Valeriano y Maness (2015) documentaron un patrón de contención: los Estados usan estas capacidades con moderación calculada, porque su valor coercitivo depende de no emplearlas de forma catastrófica.

La evidencia reciente respalda una lectura sintética. La operación contra la red satelital KA-SAT de Viasat, ejecutada el 24 de febrero de 2022 —día de la invasión rusa a Ucrania— mediante el *wiper* Acid-

Rain, inutilizó al menos 27.000 módems y dejó fuera de servicio durante semanas 5.800 aerogeneradores en Alemania; fue atribuida oficialmente a Rusia por la Unión Europea, el Reino Unido y Estados Unidos el 10 de mayo de 2022 (CCDCOE, 2022). Es el ejemplo más nítido de una ciberoperación integrada a una campaña militar convencional: preparó el terreno, degradó comunicaciones y generó efectos transfronterizos no deseados sobre terceros Estados neutrales, lo que ilustra con precisión los dilemas jurídicos que plantea el uso de la fuerza en el ciberespacio (Llorens, 2017; García Vázquez, 2021). Pero también muestra los límites del instrumento: no decidió la campaña ni sustituyó al fuego.

Más inquietante para el análisis geopolítico es un fenómeno distinto: el preposicionamiento. Las campañas asociadas a los actores designados como *Volt Typhoon* y *Salt Typhoon* revelaron accesos persistentes en infraestructura crítica y en redes de telecomunicaciones de Estados Unidos y de otros países, sin objetivos de extracción inmediata evidentes (Congressional Research Service, 2025). Su lógica no es el ataque, sino la opción de ataque: la construcción anticipada de una capacidad que solo se activaría en una crisis futura. Esto altera la naturaleza del problema estratégico. La disuasión clásica supone capacidades visibles y umbrales claros; el preposicionamiento opera sobre lo invis-

ble y genera un dilema de seguridad permanente, en el que cada actor debe asumir que sus redes ya están comprometidas.

A ello se suma la inteligencia artificial como acelerador del ciclo ofensivo. Las proyecciones para 2026 anticipan una carrera armamentística algorítmica, con automatización creciente del reconocimiento, la explotación de vulnerabilidades y la ingeniería social, y una correlativa automatización de la defensa (Google Cloud, 2025). El efecto neto no es necesariamente más

ataques exitosos, sino una comprensión drástica del tiempo para decidir.

El resultado es una conflictividad con reglas propias, que la Tabla 1 contrasta con la guerra interestatal clásica. No se trata de una guerra nueva, sino de una competencia estratégica continua, deliberadamente calibrada para permanecer bajo el umbral del artículo 2(4) de la Carta de las Naciones Unidas, donde el derecho internacional sigue aplicándose —así lo reconoce el consenso reflejado en el *Manual*

Tabla 1. Gramáticas comparadas del conflicto: guerra interestatal clásica y conflictividad ciberespacial.

Dimensión	Guerra interestatal clásica	Conflictividad en el ciberespacio
Umbral	Declaración formal o acto de fuerza reconocible bajo el artículo 2(4) de la Carta de la ONU.	Calibrada deliberadamente por debajo del umbral del uso de la fuerza y del ataque armado.
Temporalidad	Episódica: inicio, desarrollo y terminación identificables.	Persistente: competencia continua, sin estado final ni armisticio.
Atribución	Directa e inmediata; el autor suele ser evidente.	Técnica, lenta y probabilística; atribuir es una decisión política costosa.
Actores	Fuerzas armadas estatales, con cadena de mando definida.	Estados, proxies, grupos criminales, empresas tecnológicas e individuos.
Efecto buscado	Destrucción de capacidades y control del territorio.	Degradación, denegación, manipulación y, sobre todo, dependencia.
Terreno	Geografía física: dada, estable y de titularidad pública.	Infraestructura construida: reversible, deslocalizable y mayoritariamente privada.
Disuasión	Basada en capacidades visibles y umbrales explícitos.	Erosionada por la opacidad de las capacidades y el preposicionamiento.
Reversibilidad	Daño físico permanente y costoso de revertir.	Efectos con frecuencia reversibles, pero repetibles a muy bajo costo.

Nota. Elaboración propia a partir de Rid (2013), Valeriano y Maness (2015), Kello (2017), Schmitt (2017) y United States Joint Staff (2018).

de Tallin 2.0 (Schmitt, 2017)— pero donde su aplicación práctica se enfrenta al problema de la atribución.

La disputa por las reglas: gobernanza, fragmentación y modelos en competencia

Si el vector normativo es tan decisivo como el infraestructural, los foros donde se negocian las reglas son escenarios geopolíticos de pleno derecho, y el periodo 2024-2026 fue particularmente denso en ese frente.

El Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre seguridad en el uso de las tecnologías de la información concluyó su mandato el 11 de julio de 2025 con la adopción de un informe final por consenso, y dio paso a un **Mecanismo Global** de carácter permanente, cuya sesión organizativa debía celebrarse a más tardar en marzo de 2026 (Naciones Unidas, 2025). El acuerdo consolidó el Directorio Global de Puntos de Contacto y priorizó la implementación de las normas voluntarias ya existentes sobre la creación de otras nuevas —una señal clara de que el consenso alcanzable se agotó, por ahora, en el terreno declarativo. Paralelamente, el 25 de octubre de 2025 se abrió a la firma en Hanói la Convención de las Naciones Unidas contra la Ciberdelincuencia, suscrita ese día por 65 Estados, entre ellos Colombia, y que entrará en vigor noventa días después del depósito

del cuadragésimo instrumento de ratificación (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2025).

Estos avances conviven con una fragmentación creciente. Tres modelos de ordenamiento compiten por definir el ciberespacio del futuro, y la elección entre ellos —o la negativa a elegir— constituye hoy una decisión de política exterior. El primero, de matriz estadounidense, privilegia la libertad de flujo de datos y la autorregulación del mercado. El segundo, de matriz china, articula la doctrina de la cibersoberanía: el ciberespacio como extensión del territorio nacional, sujeto a control estatal pleno sobre contenidos, datos e infraestructura (Vargas-Chaparro, 2022). El tercero, europeo, construye una tercera vía basada en derechos fundamentales y proyección regulatoria extraterritorial (Bradford, 2020).

Para una potencia media, la disyuntiva no es adherir a un bloque, sino evitar quedar atrapada en la infraestructura de uno y en la regulación de otro sin haberlo decidido.

El riesgo de esta competencia no es la victoria de un modelo, sino la consolidación de bloques tecnológicos incompatibles —el fenómeno descrito como *splinternet*—, con estándares, cadenas de suministro y regímenes de datos divergentes.

Para países que dependen simultáneamente de tecnología de ambos

polos, la fragmentación no es una abstracción: es un costo directo de transacción y una restricción a la autonomía.

Conviene, no obstante, evitar el determinismo. El Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (2024) documenta un progreso agregado significativo: 139 países cuentan con equipos de respuesta a incidentes —frente a 109 en 2021—, 132 tienen estrategias nacionales y 177 regulan la protección de datos. La capacidad estatal se está difundiendo, de manera desigual pero real, y eso reduce el margen de las grandes potencias para imponer reglas por defecto.

Colombia: geopolítica cibernética de una potencia media

Colombia ofrece un caso analíticamente valioso porque combina una posición geográfica privilegiada con una dependencia tecnológica estructural. Su condición bioceánica se traduce, en el vector infraestructural, en aproximadamente diez sistemas de cable submarino activos y nueve puntos de aterrizaje distribuidos entre Buenaventura, Tolú, Cartagena, Puerto Colombia, Barranquilla, Parque Isla Salamanca, Santa Marta, San Andrés y Riohacha (Portafolio, 2023). Esa dotación, notable para la región, es a la vez activo estratégico y superficie de exposición: la conectividad internacional depende de pocas instalaciones costeras cuya protección involucra a autoridades maríti-

mas, operadores privados y fuerzas militares, sin un régimen integrado de responsabilidad. La experiencia báltica sugiere que conviene cerrar esa brecha antes, y no después, del primer incidente.

En el plano de las amenazas, las cifras oficiales muestran una evolución favorable, pero requieren lectura cuidadosa. Colombia gestionó 1.427 incidentes cibernéticos en 2024 y 697 en 2025, una reducción del 48,84 %, en un periodo en el que el ColCERT amplió su capacidad de vigilancia de 31 a cerca de 1.300 entidades y logró por primera vez el monitoreo de infraestructura crítica en los 32 departamentos (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2026). El fraude concentró el 79,83 % de los casos del bienio, con el *phishing* (835 casos) y el acceso no autorizado a cuentas de correo (784 casos) como vectores dominantes. Ahora bien, una caída de incidentes gestionados en un contexto de expansión del perímetro de monitoreo admite dos lecturas: mejora real de la postura defensiva o cambio en los criterios de registro. El propio informe advierte un incremento de amenazas persistentes avanzadas sobre sectores estratégicos —energía, salud, defensa, transporte, finanzas y telecomunicaciones—, lo que sugiere sustitución de volumen por sofisticación. Geopolíticamente esa es la transición decisiva: del cibercrimen oportunista a la presencia de actores con patrocinio estatal.

En el vector normativo, el país ha construido una arquitectura institucional apreciable. Los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020 establecieron sucesivamente los marcos de ciberseguridad, gestión de riesgo y confianza digital (Departamento Nacional de Planeación, 2020); el Decreto 338 de 2022 definió la gobernanza de la seguridad digital (Presidencia de la República de Colombia, 2022); y la Estrategia Nacional de Seguridad Digital 2025-2027 (Presidencia de la República de Colombia, 2025) organiza la acción estatal en torno a cuatro objetivos: gobernanza, resiliencia nacional, talento y adecuación regulatoria. A ello se suman la adhesión al Convenio de Budapest mediante la Ley 1928 de 2018 (Congreso de la República de Colombia, 2018), la firma de la Convención de Hanói en 2025 y, particularmente relevante para el análisis geopolítico, la publicación de la Posición Nacional sobre la Aplicación del Derecho Internacional al Ciberespacio (Ministerio de Relaciones Exteriores de Colombia, 2025), que sitúa al país entre el grupo todavía reducido de Estados que han fijado públicamente su interpretación jurídica del dominio. El desafío, señalado desde hace años por la literatura especializada, no está en la producción normativa sino en su implementación efectiva y en la articulación entre instrumentos de política, capacidades técnicas y decisión estratégica (Saavedra & Parraguez, 2018). Publicar una

posición nacional no es un gesto declarativo: es un acto de ciberdiplomacia que aumenta la previsibilidad y reduce el margen de ambigüedad (Patiño Orozco, 2019; Rioridan, 2019).

Las brechas persisten en tres frentes. La dependencia tecnológica: casi todo el hardware, el software de base y los servicios de nube que sostienen la infraestructura crítica nacional son de origen extranjero, lo que limita la autonomía en detección, respuesta y análisis forense (Cabuya-Padilla et al., 2022). El talento: la demanda de perfiles especializados supera con amplitud la oferta formativa y el sector público compite en desventaja por retenerlos (Cujabante Villamil et al., 2020). Y la capacidad de anticipación, menos discutida: la producción científica regional en modelamiento y simulación aplicados a la ciberdefensa es limitada y las herramientas propias para explorar escenarios de crisis son incipientes (Cabuya-Padilla & Castañeda-Marroquín, 2024). Los modelos de propagación de ciberataques sobre infraestructura marítima (Cabuya-Padilla et al., 2025b) y los ejercicios híbridos de mesa apoyados en simulación matemática (Cabuya-Padilla et al., 2025a) apuntan en esa dirección: permiten ensayar decisiones estratégicas antes de que la crisis obligue a improvisarlas.

Frente a estas brechas, Colombia dispone de márgenes de maniobra

reales. En lo regional, su trayectoria institucional le permite aspirar a referente en política pública de seguridad digital y en la cooperación operativa entre CSIRT nacionales. En lo multilateral, su participación en el Mecanismo Global y su condición de firmante temprano de la Convención de Hanói le dan legitimidad para promover una agenda de creación de capacidades útil al conjunto de las potencias medias. En lo interno, la cooperación cívico-militar —rasgo distintivo del modelo colombiano (Cujabante Villamil et al., 2020)— es un activo replicable, siempre que se acompañe de salvaguardas democráticas explícitas sobre el uso de capacidades cibernéticas.

Reflexiones finales

El ciberespacio no derogó la geografía: produjo una geografía adicional, superpuesta a la física y regida por lógicas propias. Bajo la retórica de la nube persisten cables, puntos de aterrizaje, jurisdicciones y cadenas de suministro cuya distribución es tan desigual —y tan políticamente significativa— como la de los estrechos marítimos que ocuparon a la geopolítica clásica. Reconocer esa materialidad es la primera condición de cualquier estrategia seria de soberanía digital.

A la pregunta que da título a este número, la respuesta que aquí se ha sostenido es negativa en la forma y afirmativa en el fondo. El ciberespacio no ha producido una

guerra nueva: las operaciones cibernéticas, por sí solas, no han decidido ningún conflicto ni han sustituido al empleo de la fuerza. Pero sí ha producido una nueva perspectiva sobre la guerra, en tres sentidos precisos. Primero, ha extendido la competencia estratégica a un tiempo continuo, sin distinción nítida entre paz y guerra. Segundo, ha desplazado el centro de gravedad del conflicto desde la destrucción hacia la dependencia: hoy importa menos lo que un adversario puede destruir que aquello de lo cual puede privarnos. Tercero, ha convertido la ambigüedad en un recurso deliberado, lo que erosiona los mecanismos de disuasión contruidos sobre la claridad de umbrales y atribuciones.

Para una potencia media como Colombia, esto define un margen de acción específico. No puede competir en acumulación de capacidades ofensivas ni aspirar a la autosuficiencia tecnológica en el horizonte previsible, pero sí en tres terrenos donde la asimetría de recursos pesa menos. En resiliencia, con protección integrada de sus infraestructuras críticas cibernéticas y atención prioritaria a los puntos de aterrizaje de cable submarino, hoy en zona gris de responsabilidad. En diplomacia, con voz activa en el Mecanismo Global y posiciones regionales que eleven el costo político de las operaciones contra Estados pequeños. Y en anticipación, invirtiendo en modelamiento, simulación y juegos de gue-

rra que permitan probar decisiones estratégicas antes de que la crisis las imponga.

La lección de fondo es que la geopolítica del ciberespacio no premia la fuerza, sino la comprensión. En un dominio donde las capacidades se deprecian con cada parche y las alianzas se reconfiguran con cada cambio tecnológico, la ventaja duradera pertenece a quien entiende mejor el sistema que habita. Para los Estados que no pueden dominar el terreno, entenderlo es la forma más realista de ejercer poder sobre él.

Referencias

- Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. <https://www.eff.org/es/cyberspace-independence>
- Bartolomé, M. (2023). *Ciberseguridad, geopolítica y relaciones internacionales* (Global Strategy Report 5/2023). Global Strategy, Universidad de Granada.
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Cabuya-Padilla, D. E., Alvarado Carvajal, C. F., Carrascal Ortiz, R. A., Escandón Bernal, S. P., Riola Rodríguez, J. M., & Fajardo-Toro, C. H. (2022). Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990-2021. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, (E49), 197-210.
- Cabuya-Padilla, D. E., & Castañeda-Marroquín, C. A. (2024). Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. *DYNA*, 91(231), 169-179. <https://doi.org/10.15446/dyna.v91n231.109774>
- Cabuya-Padilla, D. E., Díaz-López, D., & Castañeda-Marroquín, C. (2025a). Hybrid tabletop exercise (TTX) based on a mathematical simulation-based model for the maritime sector. En *Actas de las X Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2025)* (pp. 37-44). Universidad de Zaragoza.
- Cabuya-Padilla, D. E., Díaz-López, D., Martínez-Páez, J., Hernández, L., & Castañeda-Marroquín, C. (2025b). SERDUX-MARCIM: Maritime cyber-attack simulation using dynamic modeling, compartmental models in epidemiology and agent-based modeling. *International Journal of Information Security*, 24(3), 122. <https://doi.org/10.1007/s10207-025-00985-6>
- CCDCOE. (2022). *Viasat KA-SAT attack (2022)*. Cyber Law Toolkit, NATO Cooperative Cyber Defence Centre of Excellence. [https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_\(2022\)](https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022))
- Congressional Research Service. (2025). *Salt Typhoon hacks of telecommunications companies and federal response implications* (CRS Report IF12798). Library of Congress.
- Congreso de la República de Colombia. (2018). *Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado en Budapest el 23 de noviembre de 2001*. Diario Oficial No. 50.664.
- Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible

modelo a seguir en las relaciones civil-militares. *Revista Científica General José María Córdova*, 18(30), 357-377. <https://doi.org/10.21830/19006586.588>

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995: Política nacional de confianza y seguridad digital*. Consejo Nacional de Política Económica y Social.

García Vázquez, B. (2021). El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: la ciberguerra. *Revista Chilena de Derecho y Tecnología*, 10(2), 43-68. <https://doi.org/10.5354/0719-2584.2021.57077>

García-Jiménez, A., Beltrán Orenes, P., & Núñez Puente, S. (2010). Una aproximación al concepto de frontera virtual. Identidades y espacios de comunicación. *Revista Latina de Comunicación Social*, (65), 214-221. <https://doi.org/10.4185/RLCS-2010-894-214-221>

Google Cloud. (2025). *Cybersecurity forecast 2026*. Google Cloud Security.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Llorens, M. P. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, 17, 785-816. <https://doi.org/10.22201/ijj.24487872e.2017.17.11052>

Mackinder, H. J. (1904). The geographical pivot of history. *The Geographical Journal*, 23(4), 421-437. <https://doi.org/10.2307/1775498>

Mata-Sánchez, G. (2023). Relaciones internacionales y geopolítica: conflicto y poder en el ciberespacio. *Relações Internacionais no Mundo Atual*, 3(41).

Ministerio de Relaciones Exteriores de Colombia. (2025). *Posición nacional de Colombia sobre la aplicación del derecho internacional al ciberespacio*. Gobierno de Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2026, 2 de abril). *Colombia fortalece su soberanía digital: durante 2025 logró reducir en un 48 % los incidentes cibernéticos*. MinTIC. <https://www.mintic.gov.co/portal/715/w3-article-433511.html>

Naciones Unidas. (2025). *Final report of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*. Asamblea General de las Naciones Unidas.

Nye, J. S. (2011). *The future of power*. PublicAffairs.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2025). *Convención de las Naciones Unidas contra la Ciberdelincuencia*. UNODC.

Organización del Tratado del Atlántico Norte. (2025). *Baltic Sentry: NATO steps up patrols in the Baltic Sea to safeguard critical undersea infrastructure*. Allied Maritime Command. <https://mc.nato.int/media-centre/news/2025>

Patiño Orozco, G. A. (2019). El sistema internacional cibernético: elementos de análisis. *Oasis*, (30), 163-186. <https://doi.org/10.18601/16577558.n30.10>

Perafán Del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E., & Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi et Iudicandi*, 16(1). <https://doi.org/10.15332/19090528.6480>

- Portafolio. (2023, 6 de marzo). *Así está el mapa de los cables submarinos que llegan al país*. Portafolio. <https://www.portafolio.co/innovacion/cables-submarinos-este-es-el-panorama-en-colombia-579498>
- Prado, B. (2018). Geopolítica del ciberespacio: hacia el Heartland cibernético. *Revista Geografía y Sistemas de Información Geográfica (GeoSIG)*, 10, 1-13.
- Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022, por el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital*. Diario Oficial No. 51.973.
- Presidencia de la República de Colombia. (2025). *Estrategia nacional de seguridad digital de Colombia 2025-2027*. Gobierno de Colombia.
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
- Riordan, S. (2019). *Cyberdiplomacy: Managing security and governance online*. Polity Press.
- Rivas, S. M. (2021). El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos. *Revista Relaciones Internacionales*, 3(1), 89-107.
- Saavedra, B., & Parraguez, L. (2018). La ciberseguridad: análisis político y estratégico. *Fuerzas Armadas*, (243), 44-51. <https://doi.org/10.25062/0120-0631.737>
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2.^a ed.). Cambridge University Press.
- Unión Internacional de Telecomunicaciones. (2024). *Global cybersecurity index 2024*. ITU Publications.
- Unión Internacional de Telecomunicaciones. (2025). *Submarine cable resilience*. ITU. <https://www.itu.int/en/mediacentre/backgrounders/Pages/submarine-cable-resilience.aspx>
- United States Joint Staff. (2018). *Cyberspace operations* (Joint Publication 3-12). Department of Defense.
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.
- Vargas-Chaparro, N. E. (2022). La cibergeopolítica de China: un interés estratégico de Estado. *Estudios en Seguridad y Defensa*, 17(33), 201-222. <https://doi.org/10.25062/1900-8325.328>
- Voo, J., Hemani, I., & Cassidy, D. (2022). *National cyber power index 2022*. Belfer Center for Science and International Affairs, Harvard Kennedy School. 

Diego Edison Cabuya Padilla. Capitán de Fragata de la Armada de Colombia y Doctor en Ciencias del Mar de la Escuela Naval de Cadetes "Almirante Padilla", con investigación doctoral en ciberseguridad y ciberdefensa marítima. Magíster en Ciberseguridad y Ciberdefensa, en Gestión de la Información (Universitat Politècnica de València, España) y en Logística; ingeniero electrónico y profesional en ciencias navales. Ha servido en el Comando Conjunto Cibernético de las Fuerzas Militares y fue visiting scholar Fulbright en el William J. Perry Center for Hemispheric Defense Studies (National Defense University). Actualmente es Director de Investigación de la Academia Naval de Estudios Estratégicos. ORCID: 0000-0001-5338-9943.