CARI / CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

Comentarios Estratégicos

Ciberseguridad, inteligencia estratégica y diplomacia digital: desafíos para la seguridad internacional en América Latina en la era de la inteligencia artificial

Virginia Nehme Rodríguez

Ciberseguridad, inteligencia estratégica y diplomacia digital: desafíos para la seguridad internacional en América Latina en la era de la inteligencia artificial

Virginia Nehme Rodríguez

Comentarios Estratégicos
N.º 56
ABRIL 2026
ISSN 3008-9956

Corrección: María Fernanda Rey
Diseño: Trenders
Maquetación: Mario Modugno
Imagen de tapa: iStock.com/Mak_Art

CARI Consejo Argentino para las Relaciones Internacionales
Uruguay 1037, piso 1.º, C1016ACA Buenos Aires, República Argentina
Teléfono: (+5411) 4811-0071 al 74 / Fax: (+5411) 4815-4742
Correo electrónico: direccioneditorial@cari.org.ar / Sitio web: www.cari.org.ar

Ciberseguridad, inteligencia estratégica y diplomacia digital: desafíos para la seguridad internacional en América Latina en la era de la inteligencia artificial

Virginia Nehme Rodríguez*

Introducción

El siglo XXI ha consagrado al ciberespacio como un dominio decisivo de poder, competencia y vulnerabilidad. La expansión de las tecnologías digitales, sumada al desarrollo acelerado de la inteligencia artificial (IA), está transformando la seguridad internacional y reconfigurando los instrumentos tradicionales de la política exterior. La información, los datos y los algoritmos se han convertido en activos estratégicos, capaces de alterar equilibrios de poder sin recurrir al uso convencional de la fuerza (Kello, 2017; Nye, 2011).

En este contexto, América Latina enfrenta este proceso desde una posición estructuralmente desventajosa. La región presenta marcadas asimetrías tecnológicas, dependencia de proveedores externos y una débil institucionalidad en materia de ciberseguridad e inteligencia estratégica. Los Estados latinoamericanos no solo deben adaptarse a nuevas formas de conflicto híbrido, sino que también debe fortalecer sus capacidades diplomáticas y analíticas para actuar en un entorno global interconectado, volátil y altamente automatizado, donde la IA comienza a

* Licenciada en Relaciones Internacionales. Magíster Scientiarum en Negociaciones Económicas Internacionales. Investigadora en diplomacia digital y del uso estratégico de las narrativas y la IA en las relaciones internacionales. Correo de contacto: virginianehme20@gmail.com

incidir directamente en la toma de decisiones estratégicas (United Nations Institute for Disarmament Research [UNIDIR], 2023).

La seguridad internacional contemporánea exige integrar tecnología, inteligencia y diplomacia como un solo campo estratégico, especialmente para regiones con brechas estructurales como América Latina.

1. El ciberespacio como nuevo dominio de la seguridad internacional

El ciberespacio se ha consolidado como el quinto dominio de la seguridad internacional, junto con la tierra, el mar, el aire y el espacio ultraterrestre. En él se desarrollan no solo ataques a infraestructuras críticas o espionaje cibernético, sino también operaciones de influencia, manipulación informativa y competencia narrativa entre Estados y actores no estatales. Estas dinámicas configuran una modalidad de confrontación permanente, ambigua y difícil de atribuir, que desafía los marcos tradicionales del derecho internacional y la disuasión estratégica (Kello, 2017; International Institute for Strategic Studies, 2023).

La inteligencia artificial acelera y amplifica este escenario. El uso de algoritmos para analizar grandes volúmenes de datos, automatizar respuestas y generar contenidos sintéticos —incluidos *deepfakes* y campañas de desinformación— multiplica el impacto de las amenazas digitales. La IA no solo reduce los costos de entrada a este tipo de operaciones, sino que también incrementa su sofisticación y alcance, erosionando la confianza pública y afectando procesos políticos y diplomáticos (World Economic Forum, 2024).

Para América Latina, el riesgo es doble. Por un lado, la región se encuentra expuesta a interferencias digitales provenientes de actores externos con mayores capacidades tecnológicas. Por otro, la ausencia de estrategias integrales de ciberseguridad limita la capacidad de anticipación y respuesta frente a ataques que pueden comprometer infraestructuras críticas, sistemas financieros y estabilidad institucional (Organization of American States [OAS], 2020). Sin capacidades propias en el dominio cibernético, América Latina corre el riesgo de convertirse en un espacio vulnerable dentro de la competencia estratégica global.

2. Inteligencia estratégica en la era de la inteligencia artificial

Los servicios de inteligencia constituyen uno de los instrumentos centrales del poder estatal. En la era digital, su función se ha transformado profundamente: ya no se limita a la obtención de información confidencial, sino que incluye el análisis estratégico de datos, la anticipación de riesgos complejos y la evaluación prospectiva de escenarios globales. La ciberseguridad y la IA han redefinido la noción misma de inteligencia estratégica (Buchanan, 2017).

La incorporación de herramientas algorítmicas y de *big data* permite mejorar la capacidad analítica, pero también introduce desafíos significativos. Los sesgos automatizados, la opacidad de los sistemas de IA y la concentración de información sensible plantean dilemas éticos, legales y democráticos. Garantizar el control civil, la rendición de cuentas y el respeto por los derechos fundamentales se vuelve esencial para legitimar el rol de la inteligencia en sociedades democráticas (Organisation for Economic Co-operation and Development [OECD], 2022; UNIDIR, 2023).

En América Latina, estos desafíos se agravan por debilidades estructurales persistentes. La fragmentación institucional, la escasa coordinación interagencial y la limitada inversión en capacidades tecnológicas reducen la eficacia de los sistemas de inteligencia. A ello se suma la falta de articulación entre inteligencia, política exterior y estrategia digital, lo que impide una visión integral de la seguridad internacional (OAS, 2020).

La inteligencia estratégica del siglo XXI debe ser digital, prospectiva y democráticamente gobernada para contribuir efectivamente a la seguridad regional.

3. Ciberseguridad y diplomacia digital: una convergencia necesaria

La diplomacia digital se ha convertido en un instrumento clave para la gestión de la seguridad internacional. A través de ella, los Estados negocian normas, construyen confianza, coordinan respuestas y proyectan narrativas estratégicas en el ciberespacio. En un entorno marcado por la competencia tecnológica, la diplo-

macia digital amplía el concepto tradicional de poder blando, integrándolo con capacidades técnicas y estratégicas (Nye, 2011; Armitage & Nye, 2007).

Sin embargo, América Latina permanece rezagada en la construcción de una agenda regional de diplomacia digital. La falta de coordinación entre cancillerías, organismos de seguridad y actores tecnológicos limita la capacidad de la región para incidir en los debates globales sobre gobernanza del ciberespacio, regulación de la IA y estándares internacionales de ciberseguridad. Mientras otras regiones consolidan posiciones comunes, América Latina aparece fragmentada y reactiva (Council of the European Union, 2023; OAS, 2020).

La convergencia entre ciberseguridad, inteligencia estratégica y diplomacia digital no es opcional, sino necesaria. Sin diplomacia digital, la seguridad tecnológica carece de legitimidad y proyección internacional; sin inteligencia estratégica, la diplomacia pierde capacidad de anticipación y coherencia. La diplomacia digital es el puente indispensable entre seguridad tecnológica, inteligencia estratégica y proyección internacional.

4. Cooperación regional y gobernanza digital en América Latina

A pesar de sus limitaciones, América Latina cuenta con una tradición de diálogo político y concertación regional que podría servir de base para una arquitectura cooperativa de ciberseguridad e inteligencia estratégica. Foros como la OEA, la CELAC o el Mercosur ofrecen marcos institucionales que, con voluntad política, podrían impulsar mecanismos de confianza, intercambio de información y coordinación estratégica, en línea con los principios promovidos por Naciones Unidas en el ciberespacio (United Nations General Assembly, 2021).

Una agenda regional de gobernanza digital debería priorizar el fortalecimiento de capacidades nacionales, la interoperabilidad técnica, la formación de recursos humanos especializados y la adopción de principios éticos en el uso de tecnologías de IA. Asimismo, resulta fundamental promover una participación latinoamericana activa en los foros multilaterales donde se definen las reglas del orden digital global (OECD, 2022; UNIDIR, 2023).

La cooperación regional no implica homogeneidad, sino coordinación estratégica. Permitiría reducir vulnerabilidades compartidas y fortalecer la posición negociadora de la región frente a actores con mayor poder tecnológico: es la vía más eficaz para transformar la vulnerabilidad tecnológica en capacidad estratégica compartida.

Conclusiones

La convergencia entre ciberseguridad, inteligencia estratégica y diplomacia digital define uno de los principales desafíos de la seguridad internacional contemporánea. En un entorno global atravesado por la automatización, la desinformación y la competencia tecnológica, los Estados que no integren estas dimensiones quedarán expuestos a dinámicas que erosionan su autonomía y capacidad de decisión (Kello, 2017; Nye, 2011).

Para América Latina, el reto es doble: fortalecer capacidades internas y construir una agenda regional que permita incidir en la gobernanza global del ciberespacio. Ello requiere liderazgo político, inversión sostenida y una visión estratégica que conciba la tecnología no solo como herramienta, sino como dimensión central de la política exterior y la seguridad internacional (World Economic Forum, 2024; United Nations General Assembly, 2021).

Integrar seguridad, inteligencia y diplomacia digital no implica militarizar el espacio tecnológico, sino ejercer soberanía democrática y cooperación estratégica. El futuro de la región dependerá de su capacidad para anticipar, coordinar y proyectar una visión propia en la era de la inteligencia artificial. En resumen, la autonomía estratégica latinoamericana en el siglo XXI se juega en el terreno de la información, la inteligencia y la diplomacia digital.

Referencias

Armitage, R. L. y Nye, J. S. (2007). *CSIS Commission on Smart Power: A smarter, more secure America*. CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csissmartpowerreport.pdf

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

Council of the European Union. (2023). *Cyber defence*. https://www.consilium.europa.eu/en/policies/cyber-defence/

International Institute for Strategic Studies. (2023). *Cyber capabilities and national power: A net assessment*. Routledge.

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

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

Organisation for Economic Co-operation and Development. (2022). *Digital security risk management*. https://www.oecd.org/digital/security/

Organization of American States. (2020). *2020 Cybersecurity Report: Risks, progress and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

United Nations General Assembly. (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace* (A/76/135). https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

United Nations Institute for Disarmament Research. (2023). *AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures*. https://unidir.org/publication/ai-and-international-security-

understanding-the-risks-and-paving-the-path-for-confidence-building-measures/

World Economic Forum. (2024). *Global Cybersecurity Outlook*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

CARI / CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES