LA CIBERSEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS REGIONALES COMO FACTOR CLAVE PARA LA SEGURIDAD MULTIDIMENSIONAL DEL HEMISFERIO AMERICANO. CASO PRÁCTICO: ITAIPU Y YACYRETA

Zoraya Alas Candia

LA CIBERSEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS REGIONALES COMO FACTOR CLAVE PARA LA SEGURIDAD MULTIDIMENSIONAL DEL HEMISFERIO AMERICANO. CASO PRÁCTICO: ITAIPU Y YACYRETA

Zoraya Alas Candia[a]

RESUMEN

Este trabajo, analiza el preocupante aumento de ciberataques a infraestructuras críticas en el mundo y su potencial impacto en la seguridad multidimensional del hemisferio americano. Se utilizó enfoque cualitativo, pensamiento crítico, análisis sistémico, respaldo teórico-práctico suficiente, para demostrar la importancia de detectar y corregir a tiempo las debilidades institucionales de ciberseguridad para fomentar la confianza mutua y ampliar los marcos de cooperación hemisféricos existentes. Como ejemplo práctico, presenta el caso de las Represas Hidroeléctricas Sudamericanas de Itaipu y Yacyreta, para ilustrar la aplicación de los instrumentos y mecanismos de cooperación regional a disposición de todos los países del hemisferio a través la Organización de los Estados Americanos (OEA). La Declaración sobre Seguridad de las Américas (DSA 2003), sirvió de guía a esta investigación, haciendo especial hincapié en la contribución de las Relaciones Internacionales y la Ciberdiplomacia para dirimir conflictos de Derecho Internacional y mantener la paz y la seguridad hemisférica.

PALABRAS CLAVE:

Seguridad multidimensional, ciberseguridad, infraestructuras hidroeléctricas críticas, derecho internacional, Relaciones Internacionales, diplomacia cibernética

Citación APA:

De Alas Candia, Z. (2025). La ciberseguridad de las infraestructuras críticas regionales como factor clave para la seguridad multidimensional del hemisferio americano. caso práctico: Itaipu y Yacyreta. *Hemisferio*, 11, [56-69]. https://doi.org/10.59848/hemisferio.87

Estilo Chicago (Bibliografía)

De Alas Candia, Zoraya. "La Ciberseguridad de las Infraestructuras Críticas Regionales como Factor Clave para la Seguridad Multidimensional del Hemisferio Americano. Caso Práctico: Itaipu y Yacyreta". *Hemisferio 11,* (2025): [56-69]. https://doi.org/10.59848/hemisferio.87

Fecha de publicación: 18/12/2025

.

[a] Es Doctora en Defensa, Desarrollo y Seguridad Estratégica Nacional (IAEE), posee cuatro maestrías, una de ellas cursada en el Colegio Interamericano de Defensa (CID), obtuvo máxima calificación en todas y recomendación de publicación de su tesis en dos de ellas. Es Abogada y Escribana Pública. Estudió dos especializaciones: en inteligencia estratégica y en didáctica superior universitaria, participó en numerosos cursos y seminarios internacionales en toda América y en Asia. Ocupó altos cargos directivos en el sector público dentro del Estado paraguayo. A nivel internacional, ha ejercido funciones diplomáticas con rango de ministra en la Misión Permanente del Paraguay ante la OEA y actualmente se desempeña como Coordinadora de la Dirección de Relaciones Externas del CID, ambas en Washington D.C.

INTRODUCCIÓN

El preocupante aumento de ciberataques a los sistemas que controlan y operan las infraestructuras críticas en el mundo, hace necesaria una mirada crítica respecto a la manera en que se articula la cultura estratégica hemisférica de ciberseguridad, en la intención de encontrar nuevas maneras de aplicar los mecanismos de cooperación regional existentes que contribuyan a mitigar la inseguridad cibernética[1].

A nivel regional, el riesgo de ser blanco de actividades maliciosas que enfrentan las infraestructuras críticas, es verdaderamente elevado, debido a que estos activos vitales para el desarrollo de los Estados, dependen 100% de las tecnologías que manejan sus sistemas operativos, lo que lamentablemente, las expone constantemente a recibir ciberataques.

Este tipo de amenazas a la seguridad cibernética regional, posee características muy complejas que operan en varios espectros al mismo tiempo, socavan la estabilidad política, económica, energética y la seguridad de los países. Paralelamente, les impide fomentar confianza cibernética mutua, ya que los ciberataques, podrían provenir de cualquier país del hemisferio e incluso, del resto del mundo; pero, en la práctica, salvo que un grupo cibercriminal se atribuya la autoría de los ciberataques, la determinación precisa de la identidad de los perpetradores, sigue siendo casi imposible.

Ante este panorama, los sistemas de ciberseguridad de los países del hemisferio se encuentran al límite de sus capacidades operativas. En virtud de ello, este estudio abordará el acuciante incremento de ciberataques a infraestructuras críticas en el mundo y su potencial impacto en el hemisferio americano, para resaltar la importancia de aplicar los instrumentos y mecanismos interamericanos existentes e incrementar la cooperación y la confianza mutua regional. A tal efecto, plantea a modo de casuística regional, un análisis de los niveles de ciberseguridad de dos Represas Hidroeléctricas Sudamericanas: Itaipu y Yacyreta.

En tal sentido, debemos reconocer que la sociedad de la información en el ciberespacio en la que vivimos inmersos, representa un universo de oportunidades de desarrollo y crecimiento para todos los países del mundo; pero al mismo tiempo, representa un gigantesco desafío para la ciberseguridad de los Estados. Esta compleja dualidad, pone constantemente a prueba sus capacidades, así como la calidad de la gestión de las instituciones nacionales y de los Organismos Internacionales encargados de reglamentar el uso responsable del quinto dominio.

"No debemos esperar la ocurrencia de un ciber 911 para empezar a actuar"

Al respecto, es menester remarcar la importancia que reviste para nuestro hemisferio proteger adecuadamente sus activos estratégicos y abordar el tema con la seriedad y rigurosidad que merece. Este análisis, realizará un escenario prospectivo respecto al impacto destructivo y las potenciales consecuencias que los ciberataques a estas infraestructuras hidroeléctricas críticas de la región sudamericana podrían provocar, para dimensionar más claramente cuánto afectaría a todo el hemisferio americano.

Para ello, se tomarán en consideración los instrumentos interamericanos sobre seguridad cibernética vigentes, que ponen el foco en la necesidad de incrementar esfuerzos conjuntos entre los países del hemisferio, para reforzar las medidas de ciberseguridad colectiva (Carta de las Naciones Unidas - 1945)[2] que permitan elevar los niveles de ciberseguridad regional para garantizar la seguridad

[1] Colegio Interamericano de Defensa, citado en Colegio Interamericano de Defensa, *Documento de posición sobre ciberseguridad hemisférica y amenazas híbridas* (Washington, D.C.: CID, 2022).

[2] Organización de las Naciones Unidas, *Carta de las Naciones Unidas y Estatuto de la Corte Internacional de Justicia* (San Francisco: ONU, 1945).

humana (Informe sobre Desarrollo Humano - PNUD 1994)[1] y la seguridad nacional de todo el hemisferio.

Como punto inicial de este estudio sobre ciberseguridad interamericana, recordemos al senador americano Joe Lieberman[2] que dijo: "No debemos esperar la ocurrencia de un ciber 911 para empezar a actuar".

Esta frase de impacto, debe hacernos reflexionar profundamente sobre ¿qué evento de ciberseguridad podría compararse a una tragedia de esas proporciones en nuestra región? La respuesta es: Los ciberataques a infraestructuras hidroeléctricas críticas.

Para ejemplificar la magnitud destructiva que un ciberataque podría ejercer sobre este tipo de activos estratégicos vitales, tomaremos como ejemplo a dos Represas Hidroeléctricas sudamericanas de las cuales se benefician Argentina, Brasil y Paraguay.

Las represas hidroeléctricas de Itaipu[3] y Yacyreta[4], fueron establecidas en base a dos Tratados internacionales binacionales independientes, ambos firmados en el año 1973. El Tratado de Itaipu, compromete a Brasil y Paraguay, mientras que el Tratado de Yacyreta, fue firmado entre Argentina y Paraguay.

La protección de estas infraestructuras hidroeléctricas críticas, reviste trascendental importancia para asegurar la soberanía energética, mantener la seguridad humana y la seguridad nacional de los tres países mencionados, pero al mismo tiempo, para garantizar la paz y la seguridad de todo el hemisferio americano.

Examinando el marco normativo que las sustenta, encontramos informaciones muy interesantes, extraídas de sus sitios webs oficiales. Por ejemplo, ambas hidroeléctricas, además de los Tratados binacionales constitutivos por las que fueron creadas, se encuentran respaldadas por políticas públicas nacionales de sus respectivos Estados, coherentes con la naturaleza del vínculo jurídico binacional que las originó.

En el mismo sentido, se pudo verificar que Argentina, Brasil y Paraguay, son signatarios del Convenio de Budapest[5] sobre ciberdelincuencia, así como de sus protocolos complementarios. Por otro lado, los tres países poseen Equipos de Respuesta a Incidentes de Ciberseguridad (CSIRTs) a nivel nacional y paralelamente, cada entidad binacional posee su propio CSIRTs individual.

Adicionalmente, siguiendo las recomendaciones de los organismos regionales especializados en ciberseguridad, en forma periódica realizan ejercicios conjuntos y coordinados de simulación de ciberataques. Sin embargo, no se han encontrado registros en fuentes abiertas, ni en consultas informales a expertos, que demuestren la existencia de un CSIRTs[6] conjunto entre ambas Hidroeléctricas, y esto, en términos de ciberseguridad, constituye una enorme debilidad estratégica que podría ser aprovechada de forma maliciosa.

América Latina, es reconocida por la abundancia de biodiversidad y recursos naturales que posee. En efecto, según el Banco de Desarrollo de América Latina y el Caribe - CAF 2018[7], la región sudamericana es privilegiada en ese aspecto, ya que alberga bajo su superficie el 30% del agua dulce del planeta, insumo prioritario para la producción de otros bienes y servicios vitales para nuestro hemisferio.

[1] Programa de las Naciones Unidas para el Desarrollo (PNUD), *Informe sobre Desarrollo Humano 1994: Nuevas dimensiones de la seguridad humana* (Nueva York: PNUD, 1994).
[2] Joe Lieberman, citado en U.S. Senate Committee on Homeland Security and Governmental Affairs, *Hearing on "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"* (Washington, D.C.: U.S. Government Printing Office, 2002).
[3] ITAIPU Binacional, *Tratado entre la República del Paraguay y la República Federativa del Brasil para el aprovechamiento hidroeléctrico del río Paraná* (Asunción-Brasilia: 1973), https://www.itaipu.gov.br/.
[4] Entidad Binacional Yacyreta, *Tratado entre la República del Paraguay y la República Argentina para el aprovechamiento hidroeléctrico del río Paraná en el sitio denominado Yacyreta-Apipé* (Asunción-Buenos Aires: 1973), https://www.eby.org.ar/.
[5] Consejo de Europa, *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*, firmado por Argentina, Brasil y Paraguay (Estrasburgo: Consejo de Europa, 2001), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
[6] CSIRT Argentina, "Centro de Respuesta a Incidentes de Seguridad en Tecnología de la Información," Ministerio de Seguridad, https://csirt.argentina.gob.ar/; CSIRT Brasil, "Centro de Tratamento e Resposta a Incidentes Cibernéticos," https://www.cert.br/; CSIRT Paraguay, "Equipo de Respuesta a Incidentes de Seguridad Informática," https://www.gov.py/csirt.
[7] Banco de Desarrollo de América Latina y el Caribe (CAF), *Gestión integrada del recurso hídrico en América Latina: desafíos institucionales, legales y políticos* (Caracas: CAF, 2018), https://scioteca.caf.com/handle/123456789/1293.

Lógicamente, los recursos naturales existentes en la región sudamericana, son aprovechados por los países que tienen la fortuna de poseerlos para impulsar su desarrollo. Una de las maneras que han encontrado para hacerlo, es a través de la construcción de monumentales represas hidroeléctricas que les permitan utilizar responsable y convenientemente la abundancia de agua y el impresionante caudal de sus ríos para generar energía eléctrica.

Este legítimo aprovechamiento de sus recursos, es el ejemplo perfecto de la dualidad a la que se hizo referencia más arriba; pues, configura al mismo tiempo una inestimable oportunidad de progreso y cooperación internacional para el desarrollo de esa subregión, y a la vez, abre las puertas a una cantidad indeterminable de riesgos y desafíos para la seguridad cibernética hemisférica.

Con base en lo anterior, se plantea la segunda pregunta de estudio: ¿por qué estas infraestructuras hidroeléctricas críticas sudamericanas podrían ser blancos potenciales de ciberataques?
Respuesta: Por el tipo de bien que generan y el nivel de daño que un ciberataque individual o simultáneo, podría causar a todo el hemisferio americano.

Como sabemos, estas infraestructuras hidroeléctricas críticas, son muy importantes para el impulso económico y la independencia energética de la región sudamericana; pero, al estar operadas por tecnologías de última generación que dependen completamente de sistemas operativos digitales, se convierten automáticamente en preciados bastiones para organizaciones internacionales de ciberdelincuencia de todo el mundo, con altísimo potencial destructivo. Recordemos que, la energía eléctrica que producen estas represas, mueve toda la actividad económica, mercantil, educativa, tecnológica y la salud pública del Cono Sur[1].

En adición a lo anterior, la ubicación geoestratégica de las referidas hidroeléctricas, en pleno corazón de América del Sur, incrementa exponencialmente el riesgo de daño potencial a gran escala que esa subregión podría sufrir, en caso de ocurrir un ciberataque[2];[3].

Por otro lado, tanto la represa hidroeléctrica de Itaipu como la de Yacyreta, se encuentran sobre el mismo cause hídrico, el caudaloso Río Paraná, a tan sólo 422 kilómetros la una de la otra. Pero, por si este escenario no fuese ya lo suficientemente complejo, se adiciona a esta peligrosa ecuación el hecho de que, una de ellas se encuentra a menos de 30 kilómetros de la Triple Frontera, conocida por las constantes sospechas de ser un centro de actividades criminales con fines de financiamiento al terrorismo internacional y la otra represa, si bien se sitúa aproximadamente 380 kilómetros más al sur, sigue perteneciendo a su zona de influencia.

Sin duda alguna, estos datos generan gran preocupación a la comunidad de ciberseguridad. Las ganancias que generan este tipo de actividades cibernéticas maliciosas, casi siempre se asocian al financiamiento de delitos conexos, lo que constituye otra de las amenazas endémicas que aquejan al mundo e influyen directamente sobre en nuestra región[4].

Prosiguiendo con el análisis, desde la perspectiva económica, encontramos que el Río Paraná, es uno de los más importantes de la región sudamericana. Forma parte de la Hidrovía Paraguay - Paraná, por cuyas aguas transita todo el comercio de importación y exportación proveniente de distintas partes del mundo[5].

Para ilustrar mejor la gravitancia hidrohegemónica que reviste el Río Paraná para esa subregión, es importante mencionar que su trayectoria inicia al sur, en la Cuenca del Plata, pasando por la Cuenca del Paraná, influyendo sobre la Cuenca del Amazonas; llegando incluso hasta la Cuenca del Orinoco, al norte del mapa hidrográfico

[1] Banco de Desarrollo de América Latina y el Caribe (CAF). *La infraestructura en el desarrollo integral de América Latina: la visión desde el sector eléctrico*. Caracas: CAF, 2019. https://scioteca.caf.com/handle/123456789/1434.
[2] ITAIPU Binacional. "Datos técnicos y geográficos." https://www.itaipu.gov.br/.
[3] Entidad Binacional Yacyreta. "Ubicación geográfica." https://www.eby.org.ar/.
[4] Organización de las Naciones Unidas contra la Droga y el Delito (UNODC), *La conexión entre el delito cibernético y la financiación del terrorismo* (Viena: ONUDD, 2021), https://www.unodc.org/unodc/es/cybercrime/terrorism.html.
[5] Comisión Económica para América Latina y el Caribe (CEPAL), *La Hidrovía Paraguay-Paraná: desafíos y perspectivas logísticas para la integración regional* (Santiago de Chile: CEPAL, 2020), https://www.cepal.org/es/publicaciones/45674-la-hidrovia-paraguay-parana-desafios-perspectivas-logisticas-la-integracion.

sudamericano (Comité Intergubernamental Hidrovía Paraguay-Paraná -1992)[1].

La posibilidad de un ciberataque a cualquiera de estas infraestructuras hidroeléctricas críticas sudamericanas, podría tener consecuencias catastróficas en todo el hemisferio americano; empezando por la interrupción inmediata y por tiempo indefinido del suministro de energía eléctrica en todo el territorio de los tres países afectados[2].

Por otro lado, los servicios de internet en la región, quedarían completamente inutilizados y fuera de servicio, lo que dejaría aisladas a sus comunidades, sin interconexión y, consecuentemente, a merced de los ciberdelincuentes especializados en detectar debilidades de seguridad cibernética dentro de los servicios de banca electrónica, tanto pública como privada.

Igualmente, a consecuencia de la pérdida de conectividad digital, se verían severamente comprometidos los controles de los comandos informáticos que operan los sistemas de apertura y cierre de las compuertas que gobiernan las esclusas de ambas hidroeléctricas.

Ante tal escenario, lo primero que ocurriría serían terribles inundaciones que afectarían gravemente a sus poblaciones. Se interrumpiría indefinidamente la navegabilidad fluvial en gran parte de Sudamérica y, por consiguiente, ocurriría una drástica caída de toda la actividad económica y mercantil a nivel regional. Pero lo más grave y triste, sería la imposibilidad de dar atención médica a sus comunidades, ante la proporción de las inundaciones y la cantidad de damnificados que esto podría provocar, inevitablemente sus sistemas de salud pública colapsarían.

La magnitud del daño que un ciberataque a estas infraestructuras hidroeléctricas criticas sudamericanas podría representar para nuestra región, es un tema que debe ser atendido con urgencia. Afrontarlo, no sólo sobrepasaría por completo las capacidades de los países afectados, sino que, además, sus consecuencias justificarían la declaración inmediata de estado de calamidad regional y, por consiguiente, se convertiría en una amenaza directa a la seguridad multidimensional de todo el hemisferio americano.

Haciendo prospección desde la perspectiva de la ciberseguridad, los CSIRTs individuales de ambas hidroeléctricas y los equipos nacionales de respuesta a incidentes cibernéticos de los tres países involucrados, con toda seguridad harían lo

"Los ciberataques a infraestructuras hidroeléctricas críticas podrían provocar, para dimensionar más claramente cuánto afectaría a todo el hemisferio americano"

imposible por recuperar el control de los sistemas operativos bajo ciberataque. Pero, lamentablemente, ante la eventual magnitud de los daños informáticos y el colapso general de los sistemas a nivel subregional, sus esfuerzos serían en vano, esto, pues se desestabilizarían por tiempo indefinido todos los servicios estatales y a causa de esto las pérdidas humanas y económicas alcanzarían proporciones dantescas.

En efecto, para afrontar un ciberataque, indefectiblemente, los países comprometidos deberán recurrir a la ayuda internacional, lo que, a su vez, absorbería las capacidades de respuesta a incidentes cibernéticos de los demás países del hemisferio, especialmente de aquellos con mejor situación económica y mayor desarrollo

[1] Comité Intergubernamental de la Hidrovía Paraguay-Paraná, *Acuerdo de Santa Cruz de la Sierra sobre Transporte Fluvial por la Hidrovía Paraguay-Paraná (Puerto Cáceres – Puerto Nueva Palmira)* (Santa Cruz, Bolivia: Comité Intergubernamental de la Hidrovía, 1992), https://www.hidrovias.org/.

[2] Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID), *Estado de la ciberseguridad en el sector energético en América Latina y el Caribe* (Washington, D.C.: OEA/BID, 2020), https://publications.iadb.org/es/estado-de-la-ciberseguridad-en-el-sector-energetico-en-america-latina-y-el-caribe.

tecnológico. Es decir, los países del hemisferio pagarían subsidiariamente los daños colaterales de un ciberataque a estas infraestructuras hidroeléctricas críticas.

La verdad es que, prácticamente, ningún país de nuestro hemisferio posee recursos suficientes ni capacidades de respuesta necesarias para sobreponerse por sí solo a un ciberataque masivo de estas características, lo que abona el terreno para seguir bregando por la adopción de mayores medidas de ciberseguridad colectiva[1].

Al resepcto, el enfoque académico, estratégico y teórico que otorga el Colegio Interamericano de Defensa (CID)[2] a este tipo de situaciones que comprometen la ciberseguridad regional, coincide con este análisis, reconociendo que, únicamente podrían ser gestionados de manera adecuada, mediante la prevención y la cooperación hemisférica coordinada.

En adición a lo anterior, la instrumentación de tales esfuerzos, debe realizarse siempre a través de las Relaciones Internacionales de los países y los objetivos de esas colaboraciones estratégicas, deben orientarse a edificar una arquitectura de ciberseguridad colectiva sólida[3].

Desde el punto de vista del Derecho Internacional, por consecuencia lógica, la ciberdiplomacia sería la encargada de conducir los debates respecto a los términos y alcances de los acuerdos multilaterales que se negocien sobre el tema, para alcanzar compromisos regionales basados en consensos que garanticen verdaderamente la protección integral de las infraestructuras hidroeléctricas críticas, para asegurar el bien común de nuestro hemisferio (CAEN)[4].

DESARROLLO

Teorías

La ciberseguridad es una especialidad relativamente nueva, sin embargo, ofrece interesantes enfoques teóricos y opiniones de diversos autores que permiten dimensionar claramente la importancia que reviste para el mundo emprender acciones de prevención individuales y colectivas, así como la cooperación regional para afrontarlas exitosamente.

En tal sentido, Henry Kissinger[5], se refiere al ciberespacio como un ámbito virtual de intercambio de información e interacción entre personas y sistemas que se encuentra permanentemente expuesto a ciberamenazas.

Tomando en consideración lo anterior, con absoluta propiedad, Nick Espinoza[6] aseguraba que en el ámbito del ciberespacio: "donde exista una vulnerabilidad, esta con toda seguridad será aprovechada" por los ciberdelincuentes.

En efecto, informaciones estadísticas elaboradas por la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA)[7], confirman que cada vez se registran más ciberataques en el mundo y su potencial destructivo también es cada vez mayor. Por ello, es imperioso que los países de la región tomen en serio las graves las amenazas cibernéticas que aquejan a sus infraestructuras críticas y las afronten de forma coordinada, colaborativa y multilateral.

En cuanto a las instituciones y herramientas jurídicas sobre ciberseguridad que se encuentran a disposición de todos los países del hemisferio, dentro del sistema interamericano, la Organización de los Estados Americanos (OEA) y sus organismos

[1] Organización de los Estados Americanos y Banco Interamericano de Desarrollo, citados en Organización de los Estados Americanos y Banco Interamericano de Desarrollo, *Estado de la ciberseguridad en el sector energético en América Latina y el Caribe* (Washington, D.C.: OEA/BID, 2020).

[2] Colegio Interamericano de Defensa (CID), *Documento de posición sobre ciberseguridad hemisférica y amenazas híbridas* (Washington, D.C.: CID, 2022), https://www.college.cid.edu/documentos/ciberseguridad-hemisferica.pdf.

[3] Organización de los Estados Americanos (OEA), *Marco de referencia para una arquitectura de ciberseguridad regional* (Washington, D.C.: OEA, 2019), https://www.oas.org/es/sms/cicte/docs/Framework-Ciberseguridad.pdf.

[4] Escuela de Altos Estudios Nacionales (CAEN), *Seguridad y defensa nacional en el ciberespacio: retos y estrategias en América Latina* (Lima: CAEN, 2021), https://www.caen.edu.pe/documentos/seguridad-cibernetica.pdf.

[5] Henry Kissinger, citado en Mariano Bartolomé, *Ciberseguridad: una mirada estratégica desde la defensa hemisférica* (Washington, D.C.: Colegio Interamericano de Defensa, 2021)

[6] Nick Espinoza, citado en Oficina de Asuntos de Desarme de las Naciones Unidas, *Desarme y ciberseguridad: amenazas y tendencias globales* (Nueva York: ONU, 2022).

[7] Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA), *Desarme y ciberseguridad: amenazas y tendencias globales* (Nueva York: ONU, 2022), https://www.un.org/disarmament/publications/more/cybersecurity-report-2022/.

especializados como la Unión Internacional de Telecomunicaciones (UIT)[1], aportan una serie de instrumentos, políticas, conceptos, salvaguardas de seguridad, así como directrices, métodos de gestión de riesgos, acciones y formación técnica que pueden combinarse entre sí para proteger de forma efectiva e integral los activos estratégicos de nuestra región.

Profundizando el conocimiento de las características de la ciberseguridad, el ex catedrático del Colegio Interamericano de Defensa, Profesor Doctor Mariano Bartolomé[2], definió la ciberseguridad como: "todo aquello que se enfoca en las amenazas y riesgos que surgen y se despliegan en el ámbito del ciberespacio". Consideraba además que, para dar respuesta efectiva al combate de las actividades maliciosas en el ciberespacio, el núcleo de la ciberseguridad siempre debía enfocarse a garantizar que los sistemas informáticos mantengan intacta la Triada CIA: Confiabilidad, Integridad y Disponibilidad.

Partiendo de lo anterior, surge una nueva incógnita: ¿por qué si se trata sólo de ciberamenazas, se consideran tan peligrosas? En primer lugar, aunque se trate sólo de una posibilidad eventual, desde la toma de conocimiento sobre su existencia, una ciberamenaza, debe considerarse como una operación maliciosa en progreso. Hoy en día, la pregunta no es si pasará, sino cuándo ocurrirá[3].

Algunos de los motivos de ese axioma, están asociados al hecho de que las operaciones maliciosas, revisten características muy particulares, por ejemplo, su bajo costo, cualquier persona con conocimientos suficientes podría ejecutarlas. Además, posee límites difusos, lo que las hace muy difíciles de detectar o prevenir, hasta que el daño ya está hecho.

Los ciberataques, casi siempre son perpetrados de forma anónima, lo que obstaculiza la atribución de la responsabilidad de los autores. Por consiguiente, los índices de impunidad respecto a este tipo de ciberdelitos son elevadísimos; ya que, en el ámbito jurídico, sin causa no hay condena y sin jurisdicción no hay justicia.

Otras de las características de las amenazas cibernéticas, es la multiplicidad y simultaneidad de blancos potenciales. Los ciberdelincuentes, pueden atacar de forma individual o en operativos tipo comando. Las operaciones, casi siempre son remotas y los métodos de recolección y análisis de información para prevenirlos o combatirlos necesitan ser mejorados constantemente, por el vertiginoso ritmo en que los delincuentes cibernéticos innovan sus técnicas maliciosas.

Respecto al alcance conceptual de la ciberseguridad, la Fuerza Aérea de los Estados Unidos (USAF)[4], responsable de la guerra y la defensa aérea, así como de las operaciones espaciales, hace una interesante disquisición entre amenazas e incidentes de ciberseguridad. Aseguran que, para que un evento de ciberseguridad se considere una ciberamenaza, deben poder identificarse al menos cuatro elementos: actores o perpetradores, herramientas o técnicas aplicadas, un blanco a atacar y un impacto destructivo e ilegal que se desea obtener.

Por su parte, según Rid[5] las ciberamenazas pueden definirse como códigos maliciosos de computadora, empleados con el objetivo de amenazar, causar daño físico o funcional a estructuras, sistemas o seres vivos.

En cuanto a los tipos de perpetradores, el Profesor Mariano Bartolomé[6], los clasifica de acuerdo a su motivación, En líneas generales, pueden ser: hacktivistas, cibercriminales, insiders, espías, terroristas o directamente tratarse de acciones desplegadas en el marco de las campañas ofensivas o defensivas en las guerras híbridas.

[1] Unión Internacional de Telecomunicaciones (UIT). *Guía de ciberseguridad: marco para políticas nacionales de ciberseguridad.* Ginebra: UIT, 2018. https://www.itu.int/en/publications/Documents/tsb/2021-Guidelines-National-Cybersecurity-Frameworks-es.pdf.

[2] Mariano Bartolomé, "Ciberseguridad: una mirada estratégica desde la defensa hemisférica," *Revista Hemisferio*, Colegio Interamericano de Defensa, no. 14 (2021): 22–25, https://www.college.cid.edu/revistah/download/revista-hemisferio-14.pdf.

[3] Oficina de Asuntos de Desarme de las Naciones Unidas, citado en Oficina de Asuntos de Desarme de las Naciones Unidas, *Desarme y ciberseguridad: amenazas y tendencias globales* (Nueva York: ONU, 2022).

[4] Fuerza Aérea de los Estados Unidos (USAF), *Cybersecurity and Cyberspace Operations Doctrine (AFDP 3-12)* (Washington, D.C.: Department of the Air Force, 2020), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/AFDP%203-12-Cyberspace%20Operations.pdf.

[5] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

[6] Mariano Bartolomé, "Ciberseguridad: una mirada estratégica desde la defensa hemisférica," *Revista Hemisferio*, Colegio Interamericano de Defensa, no. 14 (2021): 22–25, https://www.college.cid.edu/revistah/download/revista-hemisferio-14.pdf.

Pero, ¿a qué denominamos infraestructuras críticas? En palabras del precitado autor, son activos estratégicos de vital importancia para la seguridad de los Estados, la salud pública, la economía nacional y para la confianza ciudadana en sus autoridades.

PERSPECTIVA MULTIDIMENSIONAL DE LA CIBERSEGURIDAD

Analizando la ciberseguridad regional, desde la perspectiva de la Declaración sobre Seguridad en las Américas (DSA - OEA 2003)[1] instrumento internacional que sirvió de base para el presente estudio; a modo de referencia, se toma prestada la interpretación gráfica de la DSA, realizada por el Profesor Doctor Mark Hamilton, Decano del CID, denominada "Los cuatro cuadrantes de la seguridad multidimensional".

Fuente: Profesor Doctor Mark Hamilton, Decano del CID.

Este interesante cuadro, ordena de manera clara y didáctica las amenazas, preocupaciones y otros desafíos a la seguridad hemisférica contenidos en la DSA. En él, se observa que las ciberamenazas a infraestructuras críticas, se encuentran dentro del cuadrante inferior izquierdo, en el grupo de las amenazas asimétricas, compartiendo escenario con las armas de destrucción masiva y el terrorismo que, como ya fuera señalado, muy a menudo se combinan para generar financiamiento.

Por otra parte, la seguridad humana, es el primer bien público que la inseguridad cibernética amenaza. Según la ONU, para hablar de seguridad humana, deben coexistir tres libertades fundamentales y un derecho inalienable: la libertad respecto al miedo, la libertad respecto a la necesidad, y el derecho a vivir una vida digna[2].

Sobre el punto, el Instituto Interamericano de Derechos Humanos (IIDH)[3], amplía el concepto de seguridad humana, incorporando dentro de la definición general a la seguridad económica, alimentaria, la salud, el derecho a un ambiente saludable, la seguridad personal, la seguridad comunitaria y la libertad política.

"Las Relaciones Internacionales y la Ciberdiplomacia efectiva que la articula, hacen posible llegar a consensos amplios"

En igual sentido, según Fuentes, Rojas y Aravena[4], la seguridad humana, posee además tres características fundamentales, la primera es su naturaleza integradora, la segunda su carácter multidimensional y la tercera su fuerte sentido multilateralista.

El segundo bien público vulnerado por la inseguridad cibernética, es la seguridad nacional. Kennan[5] la define como la capacidad de un Estado de proseguir su desarrollo sin influencias externas. En este orden de ideas, es claro que, la ausencia de ciberseguridad subyuga la soberanía de los Estados, por consiguiente, la seguridad nacional no puede consolidarse.

Si bien, la Carta de las Naciones Unidas, no define expresamente el término seguridad nacional, sin embargo, se considera reconocida tácitamente,

[1] Organización de los Estados Americanos (OEA), *Declaración sobre Seguridad en las Américas* (México, D.F.: Conferencia Especial sobre Seguridad, 2003), https://www.oas.org/es/sms/docs/DeclaracionSeguridad2003.pdf.
[2] Programa de las Naciones Unidas para el Desarrollo (PNUD), *Informe sobre Desarrollo Humano 1994: Nuevas dimensiones de la seguridad humana* (Nueva York: PNUD, 1994), https://hdr.undp.org/system/files/documents//hdr1994es.pdf.
[3] Instituto Interamericano de Derechos Humanos (IIDH), *Seguridad Humana y Derechos Humanos en las Américas: Enfoques integrados* (San José: IIDH, 2006), https://www.iidh.ed.cr/multic/UserFiles/File/Revista/Revista%2043/SeguridadHumana.pdf.
[4] Claudio Fuentes, Alfredo Rojas y Francisco Rojas Aravena, *Seguridad Humana en América Latina: Un enfoque multidimensional y cooperativo* (Santiago de Chile: FLACSO-Chile, 2005), https://biblioteca-repositorio.clacso.edu.ar/bitstream/CLACSO/2434/1/FuentesRojas_SeguridadHumana.pdf.
[5] George F. Kennan, *American Diplomacy, 1900–1950* (Chicago: University of Chicago Press, 1951).

ya que ese importante instrumento internacional, establece principios y mecanismos específicos para mantener la paz nacional de los Estados, insumo principal e imprescindible para alcanzar y mantener la paz internacional.

Por otro lado, Diniz y Muggah[1], consideran que, para alcanzar la seguridad cibernética regional, es necesario incrementar la cantidad de regulaciones a nivel nacional y generar mayor cantidad de acuerdos a nivel multilateral. Por consiguiente, para que la protección de las infraestructuras críticas regionales resulte efectiva, debe llevarse a cabo en base a la observancia y ejecución de esos acuerdos y nunca de forma aislada.

APORTE DE LAS RELACIONES INTERNACIONALES A LA SEGURIDAD MULTIDIMENSIONAL

En el año 2011, la Organización de las Naciones Unidas (ONU)[2] declaró que el acceso libre a internet constituía "un derecho humano". Sin embargo, tal afirmación resultó polémica, porque traía ocultas importantes responsabilidades y obligaciones para los Estados, sin mencionar los riesgos y amenazas que su provisión universal conllevaría en términos de ciberseguridad.

Por su parte, la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA)[3] considera que, el Derecho Internacional y el respeto a la Carta de la ONU son claves para concientizar a la comunidad internacional respecto al uso responsable del ciberespacio.

En efecto, es incuestionable que, para someterse a la declaración de la ONU sobre el acceso libre a internet y elevar su provisión al rango de derecho humano fundamental, los países del hemisferio primero deberían comprometerse a cumplir los compromisos subsidiarios que derivan de él, para que el texto de ese maravilloso instrumento internacional, no se convierta en una mera expresión de buenos deseos o en una simple enumeración de mejores prácticas.

Respecto a la naturaleza jurídica de la ciberseguridad, Barlow[4] considera al ciberespacio como un bien común global, porque no se encuentran bajo el control ni la jurisdicción de ningún Estado en particular. Sobre el punto, la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID)[5] a través de los organismos internacionales y la gobernanza cibernética hemisférica, instrumentados mediante organismos especializados como el Comité Interamericano contra el Terrorismo (CICTE) son los encargados de diseñar, negociar y consensuar reglas de uso responsable en el ciberespacio.

Examinemos ahora la interesante dualidad que las Relaciones Internacionales plantean respecto al ciberespacio y sus riesgos. Si observamos el fenómeno desde el prisma de la corriente de pensamiento Realista, cuyos principales representantes fueron Hobbes, Maquiavelo, Morgenthau y Mearsheimer, verificamos que ciertamente se trata de un ámbito anárquico, en donde existe alta conflictividad y una tenaz lucha por el poder[6].

Sin embargo, cuando lo analizamos desde la óptica opuesta de la corriente de pensamiento Idealista, representada por Woodrow Wilson[7], advertimos que, existiendo multiplicidad de diferentes actores relevantes involucrados, la cooperación adquiere un rol protagónico y necesario para zanjar las disputas.

[1] Eugênio Diniz y Robert Muggah, "A Resposta da América do Sul aos Desafios da Segurança Cibernética," *Revista Brasileira de Política Internacional* 57, no. 1 (2014): 9–29. https://www.scielo.br/j/rbpi/a/VcJgNq7nGbsKFrkWdqDkFhM/.

[2] Asamblea General de las Naciones Unidas, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, A/HRC/17/27 (Ginebra: Consejo de Derechos Humanos, ONU, 2011), https://undocs.org/es/A/HRC/17/27.

[3] Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA), *Desarme y ciberseguridad: amenazas y tendencias globales* (Nueva York: ONU, 2022), https://www.un.org/disarmament/publications/more/cybersecurity-report-2022/.

[4] John Perry Barlow, "Declaración de Independencia del Ciberespacio," *Electronic Frontier Foundation*, Davos, 1996, https://www.eff.org/es/cyberspace-independence.

[5] Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID). *Estado de la ciberseguridad en el sector energético en América Latina y el Caribe*. Washington, D.C.: OEA/BID, 2020. https://publications.iadb.org/es/estado-de-la-ciberseguridad-en-el-sector-energetico-en-america-latina-y-el-caribe.

[6] Hans Morgenthau y John Mearsheimer, citados en Robert Jackson y Georg Sørensen, *Introducción a las relaciones internacionales: teorías y enfoques* (México, D.F.: Oxford University Press, 2016).

[7] Woodrow Wilson, citado en Robert Jackson y Georg Sørensen, *Introducción a las relaciones internacionales: teorías y enfoques* (México, D.F.: Oxford University Press, 2016).

Esto, demuestra que, lejos de la obligación de competir por la razón, ambas corrientes funcionan perfectamente de forma complementaria para alcanzar soluciones hemisféricas que satisfagan a todas las partes interesadas, a través de la cooperación hemisférica y la aplicación escrupulosa de los instrumentos regionales de gobernanza cibernética aportados por la OEA.

Pero, profundicemos este análisis. Si aplicásemos las teorías enunciadas en el párrafo anterior a la casuística propuesta por este trabajo, respecto a las infraestructuras hidroeléctricas críticas sudamericanas, verificaríamos fácilmente que, a partir de la firma de los Tratados binacionales constitutivos de ambas represas hidroeléctricas, los países involucrados automáticamente pasan a desarrollar interdependencia compleja, tal como lo que señalan Keohane y Nye[1].

Esto, ocurre porque a partir de la suscripción de los Tratados, sus acuerdos empiezan a generar beneficio económico mutuo, lo que ubica automáticamente sus relaciones en la categoría denominada interdependencia compleja, tal como se ha señalado.

Sobre el mismo punto, Keohane y Nye, distinguen además otras características que casi siempre se encuentran presentes en este tipo de relaciones interdependientes, ellas son: la sensibilidad y la vulnerabilidad. Entendiendo la primera como la velocidad con que los cambios influyen en los actores y la segunda, como el grado de afectación que el fenómeno ejerce sobre los actores. En el caso planteado como ejemplo de este trabajo académico, ambas son muy elevadas.

En este punto, queda claro que, las Relaciones Internacionales, aportan estrategias y mecanismos colectivos de gran valor para afrontar de manera coordinada y colaborativa los desafíos comunes que plantea la inseguridad cibernética en exponencial aumento en nuestro hemisferio y en el mundo.

Las Relaciones Internacionales y la Ciberdiplomacia efectiva que la articula, hacen posible llegar a consensos amplios que permitirán no sólo prevenir y combatir de manera cooperativa los ciberataques; mediante la aplicación de las herramientas jurídicas, instrumentos regionales y multilaterales ofrecidos por la OEA, sino que, además, fomentan la confianza mutua para alcanzar de forma rápida la resiliencia cibernética hemisférica[2] y mantener la paz del hemisferio americano.

A propósito multilateralismo interamericano, es importante destacar la ardua labor que realizan los organismos que coordinan la cooperación regional en materia de ciberseguridad, como por ejemplo la Estrategia Interamericana Integral de Seguridad Cibernética (EIISC-OEA, 2004)[3] que trabaja en permanente contacto con otras comisiones del OEA como el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos de la Reuniones de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas (REMJA).

Otra dependencia que también aborda estos delicados temas dentro de la OEA y que se encuentra financiada por el Banco Interamericano de Desarrollo (BID), es el Observatorio de Ciberseguridad de América Latina y el Caribe (OCALC)[4] esta entidad, está encargada de medir los niveles de madurez y la capacidad de respuesta cibernética en la región, además de contribuir ostensiblemente a que el sistema interamericano cumpla con su objetivo inclaudicable de fomentar la cooperación regional, la confianza mutua, así como la resiliencia cibernética para mantener la paz y resguardar la seguridad multidimensional del hemisferio americano.

CONCLUSIONES

El preocupante y sostenido aumento de ciberataques a infraestructuras críticas en el mundo,

[1] Robert O. Keohane y Joseph S. Nye, *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).

[2] Organización de los Estados Americanos y Banco Interamericano de Desarrollo, citado en Organización de los Estados Americanos y Banco Interamericano de Desarrollo, *Estado de la ciberseguridad en el sector energético en América Latina y el Caribe* (Washington, D.C.: OEA/BID, 2020).

[3] Organización de los Estados Americanos (OEA), *Estrategia Interamericana Integral de Seguridad Cibernética (CICTE-OEA)* (Washington, D.C.: OEA, 2004), https://www.oas.org/es/sms/cicte/EstrategiaCiberseguridad.pdf.

[4] Banco Interamericano de Desarrollo (BID) y OEA, *Observatorio de Ciberseguridad de América Latina y el Caribe (OCALC)*, https://obser**vatoriociberseguridad.oas.org/**.

inquieta a la comunidad internacional, al mismo tiempo, hace necesaria una reflexión crítica, analítica y profunda sobre la manera como nuestra región gestiona la ciberseguridad.

El acelerado desarrollo de las tecnologías disruptivas, trae consigo enormes beneficios para la humanidad, pero también, grandes riesgos y desafíos para la ciberseguridad global. La vertiginosa evolución de las tecnologías emergentes y disruptivas, no da tregua a los encargados de custodiar el uso responsable del quinto dominio y mucho menos de anticipar suficientemente las actividades cibernéticas maliciosas.

Identificar a tiempo las vulnerabilidades que presentan los sistemas de ciberseguridad regional, es vital para corregirlos cooperativamente y mantener la estabilidad y la paz regional. En el afán de ejemplificar la manera de detectar debilidades institucionales de ciberseguridad, este trabajo, analizó el caso de las Represas Hidroeléctricas de Itaipu y Yacyreta, ambas situadas en Sudamérica y de gran importancia para la economía y la soberanía energética de esa subregión.

Las características tan particulares que presentan los ciberataques, son el caldo de cultivo ideal para dificultar su combate, por lo difícil que resulta atribuir concretamente la autoría de un ciberataque a sus responsables, e incluso, aun lográndolo, se tropezaría igualmente con las profundas lagunas legales que posee el Derecho Internacional en materia de ciberseguridad, pues al ser un ámbito sin gobernanza global, el acatamiento de los compromisos jurídicos internacionales es de cumplimiento voluntario.

El presente trabajo, concluye que los problemas que se suscitan en el ámbito del ciberespacio, deben gestionarse siempre a través de la cooperación, la colaboración y el consenso regional, apoyados en las Relaciones Internacionales e instrumentadas mediante la Ciberdiplomacia hemisférica efectiva, que contribuyan a alcanzar acuerdos regionales amplios que favorezcan la confianza mutua y la resiliencia cibernética para mantener la paz social y la seguridad cibernética de las Américas.

"Ciberseguridad hemisférica"

Las infraestructuras hidroeléctricas sudamericanas mencionadas, se encuentran en la primera línea de fuego entre los activos regionales críticos, encabezando una la larga lista de posibles blancos estratégicos para la actividad cibercriminal organizada internacional, precisamente, por el tipo de bien que producen.

La energía eléctrica que generan estas Represas Hidroeléctricas Binacionales, mueven la economía, la tecnología, la salud y todos los demás ámbitos de la actividad humana en la región sudamericana, por lo tanto, un ciberataque a una de ellas o a ambas en simultáneo, tendría consecuencias devastadoras para nuestro hemisferio.

Este estudio, considera que, alcanzar la resiliencia cibernética después de un ciberataque de esas características y proporciones, definitivamente insumiría muchísimo tiempo y recursos, tanto de los Estados afectados, como de los demás países del hemisferio.

En base a la casuística analizada, se recomienda respetuosamente a las Hidroeléctricas de Itaipu y Yacyreta, añadir una nueva capa a sus sistemas de ciberseguridad, creando un CSIRT en conjunto, que incremente sus niveles de protección ante eventuales ataques cibernéticos y que sirva para fortalecer la integración de sus sistemas de respuesta ante ataques cibernéticos individuales.

Finalmente, se recuerda a los países de la región que los organismos internacionales y los Comités interamericanos especializados en temas de ciberseguridad, se encuentran a disposición de todas las naciones del hemisferio; ofreciendo respaldo técnico, teórico, legal y documental, aportando importantes instrumentos normativos internacionales para orientar las negociaciones, incluso, existen financiamientos blandos para acompañar los esfuerzos de protección de los activos estratégicos de nuestra región de cuya protección dependen la paz y la seguridad multidimensional del hemisferio americano.

REFERENCIAS BIBLIOGRÁFICAS

Asamblea General de las Naciones Unidas. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, A/HRC/17/27. Ginebra: Consejo de Derechos Humanos, ONU, 2011. https://undocs.org/es/A/HRC/17/27.

Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). *Observatorio de Ciberseguridad de América Latina y el Caribe (OCALC)*. https://observatoriociberseguridad.oas.org/.

Barlow, John Perry. "Declaración de Independencia del Ciberespacio." *Electronic Frontier Foundation*, Davos, 1996. https://www.eff.org/es/cyberspace-independence.

Banco de Desarrollo de América Latina y el Caribe (CAF). *Gestión integrada del recurso hídrico en América Latina: desafíos institucionales, legales y políticos*. Caracas: CAF, 2018. https://scioteca.caf.com/handle/123456789/1293.

Banco de Desarrollo de América Latina y el Caribe (CAF). *La infraestructura en el desarrollo integral de América Latina: la visión desde el sector eléctrico*. Caracas: CAF, 2019. https://scioteca.caf.com/handle/123456789/1434.

Bartolomé, Mariano. "Ciberseguridad: una mirada estratégica desde la defensa hemisférica." *Revista Hemisferio*, Colegio Interamericano de Defensa, no. 14 (2021): 22–25. https://www.college.cid.edu/revistah/download/revista-hemisferio-14.pdf.

Colegio Interamericano de Defensa (CID). *Documento de posición sobre ciberseguridad hemisférica y amenazas híbridas*. Washington, D.C.: CID, 2022. https://www.college.cid.edu/documentos/ciberseguridad-hemisferica.pdf.

Comisión Económica para América Latina y el Caribe (CEPAL). *La Hidrovía Paraguay-Paraná: desafíos y perspectivas logísticas para la integración regional*. Santiago de Chile: CEPAL, 2020. https://www.cepal.org/es/publicaciones/45674-la-hidrovia-paraguay-parana-desafios-perspectivas-logisticas-la-integracion.

Comité Intergubernamental de la Hidrovía Paraguay-Paraná. *Acuerdo de Santa Cruz de la Sierra sobre Transporte Fluvial por la Hidrovía Paraguay-Paraná (Puerto Cáceres – Puerto Nueva Palmira)*. Santa Cruz, Bolivia: Comité Intergubernamental de la Hidrovía, 1992. https://www.hidrovias.org/.

Consejo de Europa. *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. Estrasburgo: Consejo de Europa, 2001. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Diniz, Eugênio, y Robert Muggah. "A Resposta da América do Sul aos Desafios da Segurança Cibernética." *Revista Brasileira de Política Internacional* 57, no. 1 (2014): 9–29. https://www.scielo.br/j/rbpi/a/VcJgNq7nGbsKFrkWdqDkFhM/.

Entidad Binacional Yacyreta. *Tratado entre la República del Paraguay y la República Argentina para el aprovechamiento hidroeléctrico del río Paraná en el sitio denominado Yacyreta-Apipé*. Asunción-Buenos Aires: 1973. https://www.eby.org.ar/.

Entidad Binacional Yacyreta. "Ubicación geográfica." https://www.eby.org.ar/.

Escuela de Altos Estudios Nacionales (CAEN). *Seguridad y defensa nacional en el ciberespacio: retos y estrategias en América Latina*. Lima: CAEN, 2021. https://www.caen.edu.pe/documentos/seguridad-cibernetica.pdf.

Fuentes, Claudio, Alfredo Rojas y Francisco Rojas Aravena. *Seguridad Humana en América Latina: Un enfoque multidimensional y cooperativo*. Santiago de Chile: FLACSO-Chile, 2005. https://biblioteca-repositorio.clacso.edu.ar/bitstream/CLACSO/2434/1/FuentesRojas_SeguridadHumana.pdf.

Fuerza Aérea de los Estados Unidos (USAF). *Cybersecurity and Cyberspace Operations Doctrine (AFDP 3-12)*. Washington, D.C.: Department of the Air Force, 2020. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/AFDP%203-12-Cyberspace%20Operations.pdf.

Gobierno del Paraguay. "*Equipo de Respuesta a Incidentes de Seguridad Informática* (CSIRT Paraguay)." https://www.gov.py/csirt.

ITAIPU Binacional. *Tratado entre la República del Paraguay y la República Federativa del Brasil para el aprovechamiento hidroeléctrico del río Paraná*. Asunción-Brasilia: 1973. https://www.itaipu.gov.br/.

ITAIPU Binacional. "Datos técnicos y geográficos." https://www.itaipu.gov.br/.

Instituto Interamericano de Derechos Humanos (IIDH). *Seguridad Humana y Derechos Humanos en las Américas: Enfoques integrados*. San José: IIDH, 2006. https://www.iidh.ed.cr/multic/UserFiles/File/Revista/Revista%2043/SeguridadHumana.pdf.

Jackson, Robert, y Georg Sørensen. *Introducción a las relaciones internacionales: teorías y enfoques*. México, D.F.: Oxford University Press, 2016.

Kennan, George F. *American Diplomacy, 1900–1950*. Chicago: University of Chicago Press, 1951.

Keohane, Robert O., y Joseph S. Nye. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown, 1977.

Lieberman, Joe. Citado en U.S. Senate Committee on Homeland Security and Governmental Affairs. *Hearing on "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"*. Washington, D.C.: U.S. Government Printing Office, 2002.

Ministerio de Seguridad Argentina. "Centro de Respuesta a Incidentes de Seguridad en Tecnología de la Información (CSIRT)." https://csirt.argentina.gob.ar/.

NIC.br. "Centro de Tratamento e Resposta a Incidentes Cibernéticos (CERT.br), Brasil." https://www.cert.br/.

Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA). *Desarme y ciberseguridad: amenazas y tendencias globales*. Nueva York: ONU, 2022. https://www.un.org/disarmament/publications/more/cybersecurity-report-2022/.

Organización de las Naciones Unidas contra la Droga y el Delito (UNODC). *La conexión entre el delito cibernético y la financiación del terrorismo*. Viena: ONUDD, 2021. https://www.unodc.org/unodc/es/cybercrime/terrorism.html.

Organización de las Naciones Unidas. *Carta de las Naciones Unidas y Estatuto de la Corte Internacional de Justicia*. San Francisco: ONU, 1945.

Organización de los Estados Americanos (OEA). *Declaración sobre Seguridad en las Américas*. México, D.F.: Conferencia Especial sobre Seguridad, 2003. https://www.oas.org/es/sms/docs/DeclaracionSeguridad2003.pdf.

Organización de los Estados Americanos (OEA). *Estrategia Interamericana Integral de Seguridad Cibernética (CICTE-OEA)*. Washington, D.C.: OEA, 2004. https://www.oas.org/es/sms/cicte/EstrategiaCiberseguridad.pdf.

Organización de los Estados Americanos (OEA). *Marco de referencia para una arquitectura de ciberseguridad regional*. Washington, D.C.: OEA, 2019. https://www.oas.org/es/sms/cicte/docs/Framework-Ciberseguridad.pdf.

Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID). *Estado de la ciberseguridad en el sector energético en América Latina y el Caribe*. Washington, D.C.: OEA/BID, 2020. https://publications.iadb.org/es/estado-de-la-ciberseguridad-en-el-sector-energetico-en-america-latina-y-el-caribe.

Programa de las Naciones Unidas para el Desarrollo (PNUD). *Informe sobre Desarrollo Humano 1994: Nuevas dimensiones de la seguridad humana*. Nueva York: PNUD, 1994. https://hdr.undp.org/system/files/documents//hdr1994es.pdf.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013.

Unión Internacional de Telecomunicaciones (UIT). *Guía de ciberseguridad: marco para políticas nacionales de ciberseguridad*. Ginebra: UIT, 2018. https://www.itu.int/en/publications/Documents/tsb/2021-Guidelines-National-Cybersecurity-Frameworks-es.pdf.