SEGURIDAD

AMÉRICA LATINA Y LA GOBERNANZA GLOBAL Y REGIONAL SOBRE CIBERSEGURIDAD

Marcos Robledo Hoecker

Octubre 2023

→ América Latina tiene un rol marginal en el desarrollo de la cuarta revolución industrial y un rezago en el debate internacional sobre la gobernanza global de la ciberseguridad.

→ Es una de las regiones más rezagadas en la *brecha digital* y sus Estados tienen el valor promedio más bajo en los indicadores globales de gobernanza digital.

→ La crisis del regionalismo latinoamericano ha debilitado la capacidad de concertación y acción en un contexto global de crisis. La región enfrenta fragmentada la gobernanza sobre ciberseguridad y es vulnerable a la captura geopolítica de las potencias que disputan la hegemonía internacional.

FRIEDRICH EBERT STIFTUNG
RED DE SEGURIDAD INCLUYENTE

SEGURIDAD

AMÉRICA LATINA Y LA GOBERNANZA GLOBAL Y REGIONAL SOBRE CIBERSEGURIDAD

CONTENIDO

1

LA GOBERNANZA DE SEGURIDAD Y LA CRISIS DEL REGIONALISMO EN AMÉRICA LATINA

De entre todas las dimensiones de la crisis del regionalismo latinoamericano una de las menos analizadas es la de la ciberseguridad. Si bien se trata de un tipo de gobernanza cuya evolución es relativamente reciente y se encuentra en proceso global de construcción, es posible observar un contraste entre la robustez los regímenes que América Latina ha desarrollado en los ámbitos tradicionales de la seguridad *cinética* regional e internacional, que la han consolidado como una de las zonas más estables del planeta desde una perspectiva estratégica, y el avance en el ámbito de la ciberseguridad. La región tiene un rol marginal en el desarrollo de la cuarta revolución industrial (4RI) y, en ese contexto, experimenta también un rezago preocupante en el debate internacional mediante el cual se está construyendo la gobernanza global de la ciberseguridad.

Desde una perspectiva comprehensiva que considera todas las dimensiones relacionadas con un ambiente de paz, en 2023 el Global Peace Index del Institute for Economics & Peace (IEP) situó a América Latina en un rango intermedio, entre Europa, Asia-Pacífico y América del Norte, por un lado, y Rusia/Eurasia, África Subsahariana, Asia del Sur y el Medio Oriente/Norte de África, por el otro (Institute for Economics & Peace, 2023: 13).

Lo anterior se explica porque la región se caracteriza por presentar un gran contraste entre la inseguridad que experimenta la ciudadanía en el interior de los países y las sociedades y la estabilidad de las relaciones internacionales entre los Estados de la región.

En el primer caso, América Latina se ha consolidado como una de las regiones más violentas del mundo: continúa con la tasa de homicidios más alta (21,2 por 100.000 habitantes), casi el doble de la de África (12,06), y cerca de cuatro veces mayor que la tasa mundial: 5,61 (UNODC, 2022; Albarracín, 2023). Se trata de indicadores que resultan de un déficit histórico de gobernanza democrática, de autoritarismo y de policiamiento autoritario.

La gobernanza de la seguridad en los Estados se caracteriza por procesos de acomodación entre élites políticas e instituciones del sector de seguridad con altos grados de autonomía que conducen a la ausencia de reformas policiales y a la reproducción de formas de policiamiento autoritario, de militarización y de militarismo (González, 2021; Dammert, 2022). Lo anterior ocurre en el contexto de un proceso gradual de erosión democrática del cual forma parte la gobernanza de la seguridad pública (Robledo Hoecker, 2022), y en el que a pesar de ser la tercera región con más democracias en el mundo después de América del Norte y Europa, América Latina muestra importantes retrocesos democráticos (IDEA Internacional, 2021).

La crisis democrática ha generado a su vez una crisis en el regionalismo latinoamericano, que se ha fragmentado, lo cual ha debilitado tanto la capacidad de concertación y gobernanza de la región, como la capacidad de acción en un contexto global de crisis, conduciendo a una "ausencia deliberada de acción colectiva de la región que, de no revertirse, podría conducir a la pérdida de su condición de actor en el sistema global y a su mera expresión geográfica" (González y otros, 2021: 51). Pese a señales recientes, como la reunión de presidentes sudamericanos en Brasil en mayo de 2023 y la adopción del "Consenso de Brasilia" (NODAL, 2023), la crisis del regionalismo ha debilitado al conjunto de las instituciones regionales.

A pesar de la crisis democrática y de la más severa en la historia del regionalismo latinoamericano, en el ámbito de la seguridad interestatal se observa la continuidad y

efectividad de otros regímenes, y América Latina exhibe la mayor estabilidad desde una perspectiva estratégica comparada, que ha sido conceptualizada como la existencia de una *zona de paz* regional (Kacowicz, 1998; Oelsner, 2016), cuyos componentes más destacados son la tradición de la resolución pacífica de las controversias y el respeto por el derecho internacional (Kacowicz, 1998); la prohibición efectiva de las armas de destrucción masiva (AMD), y un robusto régimen multinivel –interamericano, latinoamericano, subregional, plurilaterales y bilaterales– de instituciones de diálogo político, transparencia y gobernanza de la seguridad (Robledo, 2021).

De ese modo, América Latina tiene una arquitectura de seguridad regional compleja, multinivel, robusta y resiliente, sobre la cual descansa la estabilidad de las relaciones interestatales en el ámbito de la seguridad, un patrimonio amical que le permite a la región ser comparada positivamente en una perspectiva global. Sin embargo, todos los componentes de dicho atributo fueron construidos durante el periodo anterior a la crisis democrática y del regionalismo latinoamericano, así como en la etapa más temprana de desarrollo de la sociedad de la información, la que dio paso a la cuarta revolución industrial y con esta a una nueva agenda de seguridad, lo que plantea interrogantes acerca de la capacidad de la región para desarrollar una gobernanza efectiva frente a ese nuevo tipo de desafíos.

Este trabajo examinará la evolución de la gobernanza de la ciberseguridad en la región. Con ese propósito, la segunda sección abordará la cuarta revolución industrial (4RI) y el desarrollo de su gobernanza, con énfasis en la gobernanza de la ciberseguridad. La tercera resumirá la inserción de América Latina en la 4RI y su participación en el debate global sobre gobernanza de la ciberseguridad y otras tecnologías interrelacionadas, así como los avances de la región en ese ámbito. La cuarta, por último, resumirá los hallazgos.

2

CUARTA REVOLUCIÓN INDUSTRIAL, GOBERNANZA Y SEGURIDAD

La expansión de las tecnologías de la información de la tercera revolución industrial (computadores personales e Internet) al conjunto de las actividades productivas y sociales se ha visto acelerada por el desarrollo y la integración de la nanotecnología, la computación cuántica, el Internet de las cosas, la inteligencia artificial (IA), la robótica y la biotecnología, dando origen a lo que ha sido conceptualizado como la *industria 4.0* (Lasi y otros, 2014) o *cuarta revolución industrial (4RI)* (Schwab, 2016)[1]. La crisis originada por el covid-19 ha significado, más recientemente, una aceleración de ese proceso.

Los cambios impuestos por esta revolución se encuentran en desarrollo y hay una opinión amplia y creciente de que se trata de una transformación social global y cualitativa. Desde una perspectiva económica y social, se trata de una economía digitalizada, cuya producción y consumo se basa en la incorporación de tecnologías digitales en todas las dimensiones económicas, sociales y medioambientales, transitando desde un mundo hiperconectado a otro digitalizado en el que conviven y se fusionan la economía tradicional –con sus sistemas organizativos, productivos y de gobernanza– con la economía digital, originando ecosistemas complejos que se encuentran en proceso de adecuación organizativa, institucional y normativa, con efectos en la sociedad, el aparato productivo y el Estado (Cepal, 2021).

La cuarta revolución industrial está profundizando también las desigualdades o creando otras nuevas, y afectando las relaciones internacionales. Schmidt ha conceptualizado "el poder de innovación", o la habilidad para inventar, adoptar o adaptar nuevas tecnologías, como decisivo en la disputa geopolítica en desarrollo tras la crisis de la globalización y de la hegemonía de los Estados Unidos (Schmidt, 2023). Desde una perspectiva más amplia, Vint ha señalado que la combinación de la crisis del Antropoceno, el desarrollo de la inteligencia artificial, así como de la biotecnología, han planteado que el siglo veintiuno puede ser descrito como "el momento crítico después de lo humano" (Vint, 2020: 1).

La revolución tecnológica ha introducido una nueva agenda en la gobernanza de la sociedad de la información (WEF, 2017). La agenda oscila desde la gobernanza de Internet y de la inteligencia artificial, incluyendo la regulación del impacto de las nuevas tecnologías en la política (Freedom House, 2023) y los derechos humanos (Fidler, 2021), hasta el desarrollo sostenible, y todos los aspectos del desarrollo de las sociedades (Kurbalija, 2016).

La gobernanza de la cuarta revolución industrial enfrenta grandes desafíos. Por un lado, requiere la transformación de las estructuras tradicionales de gobernanza y los modelos de formulación de políticas, debido a que los procesos tradicionales de desarrollo de políticas son más lentos que la innovación tecnológica (WEF, 2017). Por otro, demanda llegar a acuerdos políticos nacionales y globales cada vez más difíciles en un periodo de creciente multipolarización, conflicto internacional y, sobre todo, crisis de la gobernanza internacional.

La gobernanza de las tecnologías de la cuarta revolución industrial está siendo desarrollada globalmente (en especial en el marco de las Naciones Unidas), en la región latinoamericana y nacionalmente. Se trata de tecnologías que tienen enormes potencialidades para resolver

1 Solo desde una perspectiva industrial, las tecnologías involucradas en la industria 4.0/4RI son la Internet de las cosas, la *cloud computing*, la inteligencia artificial y *machine learning, el edge computing,* la ciberseguridad y el gemelo digital (IBM, 2023).

problemas importantes para la humanidad (Nicholson y Reynolds, 2020), para incrementar las desigualdades (Costas Trascasas, 2022), o para generar riesgos existenciales a partir de la bioseguridad (Evans y otros, 2020) o de la inteligencia artificial (CICR, 2015), que pueden afectar todas las dimensiones de la vida humana. De entre todos los temas asociados, junto a los biotecnológicos, dos áreas de gobernanza han emergido como especialmente complejas: la del ecosistema de tecnologías que han generado el *ciberespacio* (Kurbalija, 2016) y, más recientemente, la de la *inteligencia artificial* (Cihon y Maas, 2020; Boulanin, Bruun y Goussac, 2021).

Reflejando esa complejidad, la *gobernanza global del espacio ciber* está siendo desarrollada en el marco de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), cuyas once Líneas de acción son ejecutadas por el Foro de la Cumbre.

La Cumbre organizó también el Foro de Gobernanza de Internet (FGI; IGF: Internet Governance Forum) de las Naciones Unidas. En 2020, el secretario general publicó la "Hoja de ruta para la cooperación digital", organizando la agenda sobre la gobernanza en torno a la construcción de una economía y una sociedad digitales inclusivas; la creación de capacidad humana e institucional; la protección de los derechos humanos y la capacidad de acción humana; la promoción de la confianza, la seguridad y la estabilidad digitales; y el fomento de la cooperación digital mundial (Naciones Unidas, 2020).

2.1 GOBERNANZA GLOBAL SOBRE CIBERSEGURIDAD

En el ámbito más específico de la *ciberseguridad*, la construcción de la gobernanza es un proceso multinivel que involucra tanto a las Naciones Unidas como a organizaciones regionales, plurilaterales, regímenes bilaterales y el desarrollo de normas y capacidades nacionales, y distingue asuntos políticos y los criminales.

Los asuntos políticos corresponden a las relaciones (de conflicto o cooperación) entre actores políticos, estatales y no estatales, y se desarrollan en torno a una agenda amplia de asuntos, entre los que destacan los conflictos entre Estados; la aplicación del derecho internacional al ciberespacio; la disrupción en el espacio ciber de grupos no estatales (terroristas, extremistas violentos o ilegales); la protección de los derechos de ciudadanía –políticos, civiles o sociales– en el ámbito ciber (Freedom House, 2023); o el desarrollo de capacidades y la protección de la infraestructura crítica de los Estados. Sin embargo, el problema más complejo en el ámbito político ha sido superar la idea extendida de que el ciberespacio es un área en *estado de naturaleza* y consolidar un consenso internacional en torno a la vigencia y aplicabilidad del derecho internacional sobre ese ámbito de la vida social (Schmitt, 2020)[2]. En los asuntos criminales, la agenda de gobernanza está concentrada en el control y la represión de la actividad del crimen organizado en el espacio ciber.

La Cumbre Mundial sobre la Sociedad de la Información mandató a la Unión Internacional de Telecomunicaciones (UIT) que fuera el facilitador de la Línea de acción C5, "Fomento de la confianza y la seguridad en la utilización de las TIC", en respuesta a lo cual la UIT puso en marcha, en 2007, la Agenda sobre Ciberseguridad Global (ACG; GCA: Global Cybersecurity Agenda), como marco para la cooperación internacional en este ámbito (ITU, 2023).

En el *ámbito político de ciberseguridad*, la Asamblea General de las Naciones Unidas ha mandatado a la Primera Comisión (Desarme y Seguridad Internacional) para abordar, dentro de las cinco áreas de trabajo de su Oficina de Asuntos Desarme (OAD)[3], tanto los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional, como la función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme (Naciones Unidas, 2023), áreas cuya conceptualización ha debido ampliarse y que

2 En 2015 y en 2020, tanto el presidente de Estados Unidos, Barack Obama, como el secretario general de la ONU, António Guterres, se refirieron al ciberespacio como un "salvaje oeste" (The White House, 2015; United Nations, 2020).

3 Las cinco áreas son: Armas de destrucción masiva, Armas convencionales, Desarme regional, Transparencia y construcción de confianza y Otros temas de desarme (Naciones Unidas, 2020). Los temas relacionados con seguridad, ciber, ciencia y tecnología son abordados en la última área de trabajo de la Oficina de Asuntos de Desarme.

actualmente son tratadas como "dimensiones de seguridad de las innovaciones en ciencia y tecnología" (Unidir, 2023).

A partir de 2004, la Primera Comisión de la Asamblea General ha establecido dos tipos de instituciones. Por un lado, creó seis Grupos de Expertos Gubernamentales (GEG), integrados inicialmente por especialistas de quince Estados, ampliado a veinte en 2015 y a veinticinco en 2018[4]. El segundo tipo de institución es el Grupo de Trabajo de Composición Abierta (GTCA; OEWG: Open-Ended Working Group), establecido por la Asamblea General en 2018, en el que pueden participar todos los Estados, las empresas, la academia y la sociedad civil.

Luego de los informes de los Grupos de Expertos Gubernamentales, y debido al número limitado de Estados participantes, el foco de las deliberaciones se trasladó hacia el más amplio GTCA. Su establecimiento ha sido un paso importante hacia una gobernanza más inclusiva y participativa de las tecnologías de la información y las comunicaciones (TIC) y, desde esa perspectiva, más democrática, existiendo demandas crecientes en esa dirección.

En 2020, un grupo de cuarenta Estados propuso la adopción de un Programa de Acción para promover el comportamiento responsable de los Estados en el ciberespacio como una forma de superar los debates en dos instituciones (Grupos de Expertos Gubernamentales / Grupo de Trabajo de Composición Abierta) y establecer un foro permanente de las Naciones Unidas para examinar el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

Tanto los sucesivos Grupos de Expertos Gubernamentales como el Grupo de Trabajo de Composición Abierta presentaron recomendaciones aprobadas por la Asamblea General, constituyendo el *acquis* a partir del cual comenzó a emerger una arquitectura básica de gobernanza multilateral de la ciberseguridad.

El primer proyecto de resolución sobre ciberseguridad fue presentado por Rusia ante la Primera Comisión en 1998. Desde entonces, el desacuerdo más importante con Estados Unidos ha radicado en que Rusia ha sido partidaria de desarrollar regímenes de derecho internacional para prevenir el uso de las tecnologías de la información con fines incompatibles con las misiones de garantizar la estabilidad y la seguridad internacionales. Estados Unidos tiene la posición de que las mismas leyes que se aplican al uso de armas cinéticas deberían emplearse en el comportamiento del Estado en el ciberespacio. Estados Unidos y la Unión Europea recibieron con sospecha el impulso original de Rusia a favor de un tratado internacional que –estimaron– podría ser utilizado para limitar la libertad de información con el pretexto de aumentar la seguridad de la información y las telecomunicaciones (Henderson, 2021).

A pesar de los desacuerdos, y de un contexto de una creciente frecuencia e intensidad de ataques e incidentes internacionales, los Grupos de Expertos Gubernamentales han concordado cuatro informes de consenso (2010, 2013, 2015 y 2021) de naturaleza acumulativa. Entre otros acuerdos, establecieron que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el entorno de la tecnología de la información y las comunicaciones. También han señalado que las obligaciones existentes en virtud del derecho internacional son aplicables al uso de las tecnologías de la información y las comunicaciones de los Estados, los que deben cumplir con sus obligaciones de respetar y proteger los derechos humanos y las libertades fundamentales.

Han indicado asimismo que los Estados no deben utilizar proxies para cometer hechos internacionalmente ilícitos utilizando las tecnologías de la información y las comunicaciones, y deben tratar de garantizar que agentes no estatales no utilicen su territorio para cometer tales actos (Naciones Unidas, 2015: 2).

4 Alemania, Australia, Brasil, China, Estados Unidos de América, Estonia, Federación Rusa, Francia, India, Indonesia, Japón, Jordania, Kazajstán, Kenia, Mauricio, Marruecos, México, Noruega, Países Bajos, Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania, Singapur, Sudáfrica, Suiza y Uruguay.

La arquitectura básica de gobernanza recomendada por los Grupos de Expertos Gubernamentales también incluyó el desarrollo de medidas de fomento de la confianza para mejorar la cooperación y la transparencia y reducir el riesgo de conflictos, y sugirió que los Estados estudiaran otras para reforzar la cooperación. Los Grupos señalaron la necesidad de un diálogo regular con una amplia participación bajo los auspicios de las Naciones Unidas y mediante foros bilaterales, regionales y multilaterales.

Sus informes destacaron el derecho inmanente que tienen los Estados de adoptar medidas de conformidad con el derecho internacional, con arreglo a lo dispuesto en la Carta (Naciones Unidas, 2015: 3). El informe de 2015 recomendó once normas voluntarias y no vinculantes de comportamiento responsable del Estado. Si bien los informes de los sucesivos Grupos de Expertos Gubernamentales no son vinculantes para los Estados miembros, la Asamblea General ha modificado el lenguaje de sus resoluciones desde el inicial "tomando nota" de las recomendaciones hacia el llamado a que los Estados se guíen por las recomendaciones, lo que refleja la importancia incremental y creciente del proceso de los Grupos de Expertos Gubernamentales (Henderson, 2021).

El Grupo de Trabajo de Composición Abierta, en tanto, ha desarrollado su trabajo basado en los consensos acumulados de los Grupos de Expertos Gubernamentales, emitiendo informes en 2021 y 2022 que establecieron una hoja de ruta hasta 2025. Dando cuenta de su mayor diversidad, su informe de 2021 reconoció que los beneficios de las tecnologías de la información y las comunicaciones no están distribuidos de manera uniforme y que el cierre de la brecha digital es una tarea urgente. El grupo también valoró la participación de delegadas en sus deliberaciones, la prominencia de las perspectivas de género en las discusiones, y subrayó la importancia de reducir la brecha digital de género y de la participación eficaz y significativa y el liderazgo de las mujeres en los procesos de toma de decisiones vinculadas a la utilización de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

Adicionalmente, el Grupo de Trabajo de Composición Abierta señaló que las amenazas podían afectar de distinto modo a los Estados en función de sus niveles de digitalización, capacidad, seguridad y resiliencia de las tecnologías de la información y las comunicaciones, infraestructura y desarrollo. Igualmente, que las amenazas también pueden afectar de forma distinta a los distintos grupos y entidades, como la juventud, las personas mayores, las mujeres y los hombres, las personas vulnerables, algunas profesiones concretas, las pequeñas y medianas empresas y otros, y destacó la importancia de la colaboración con la sociedad civil, el sector privado, el mundo académico y la comunidad técnica (Naciones Unidas, 2021).

En noviembre de 2022, la Asamblea General aprobó la propuesta de una coalición de cuarenta y nueve Estados para terminar con el trabajo dual de los Grupos de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta, autorizando la creación de un Programa de Acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional como mecanismo permanente e inclusivo luego del término del mandato del Grupo de Trabajo de Composición Abierta en 2025 (Naciones Unidas, 2022).

Junto a la Primera Comisión de la Asamblea General, la Segunda (Asuntos Económicos y Financieros) y la Tercera (Asuntos Sociales, Humanitarios y Culturales) han desarrollado una amplia agenda sobre ciberseguridad. En el primer caso, con el propósito de crear una "cultura global de ciberseguridad", mientras que en el segundo la actividad se ha concentrado en la agenda sobre cibercrimen. En cuanto a la Tercera Comisión, uno de sus resultados más importantes ha sido la decisión, en 2019, de establecer un Comité Intergubernamental Especial de Expertos de Composición Abierta, representativo de todas las regiones, para elaborar una *convención internacional integral* sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos (United Nations, 2023).

Adicionalmente, el Consejo de Seguridad ha concentrado sus esfuerzos especialmente contra el terrorismo en el ámbito ciber, mientras que en el Consejo Económico y Social la Comisión de Prevención del Delito y Justicia Penal (CCPCJ) y la Comisión de Estupefacientes (CND), lo

han hecho en el uso delictivo del ciberespacio (Henderson, 2021). En el caso de la Comisión de Prevención del Delito y Justicia Penal, la Asamblea General estableció en 2011 el Grupo Intergubernamental de Expertos de Composición Abierta, el que formuló en 2021 un total de sesenta y tres conclusiones y recomendaciones (UNODC, 2021). La Comisión de Estupefacientes, en tanto, aprobó cinco resoluciones (2000, 2004, 2005, 2007 y 2016), orientadas a promover la cooperación antidrogas en el ámbito ciber (Henderson, 2021).

Con todo, la agenda global sobre la gobernanza de la cuarta revolución industrial se está expandiendo y evolucionando rápidamente y ha pasado a ser un componente central de la agenda de gobernanza global, lo que se ha visto reflejado en las doce Recomendaciones formuladas por el secretario general de la ONU en su informe de 2021, "Nuestra agenda común". De estas, seis incorporan objetivos relativos a la gobernanza digital, incluyendo la tercera y la séptima.

La número tres, "Promover la paz y prevenir los conflictos", propone una "Nueva agenda de paz" para reducir lo que identifica como "riesgos estratégicos" globales. Además de las armas nucleares, menciona la "ciberguerra" y los "sistemas de armas autónomos", por lo que constituye uno de los primeros documentos del sistema de las Naciones Unidas que reconoce la preminencia que tiene la necesidad de la gobernanza global sobre las dos nuevas realidades estratégicas. La séptima recomendación corresponde a "Mejorar la cooperación digital". Las recomendaciones fueron acogidas por la Asamblea General de 2022 y llevaron a la convocatoria de una "Cumbre del futuro" para 2024, en la que la gobernanza sobre las tecnologías digitales (y no solamente ciber) ha sido instituida como un componente central de la agenda sobre gobernanza global.

2.2 REGÍMENES REGIONALES DE GOBERNANZA DIGITAL Y DE CIBERSEGURIDAD

Las instituciones regionales también han desempeñado un papel importante en el desarrollo de una gobernanza multinivel basada en el derecho internacional, y en algunos casos sus alcances han sido globales.

Es el caso del Consejo de Europa, que en 2001 aprobó la Convención de Budapest sobre la ciberdelincuencia, el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas[5]. La Convención entró en vigor en 2004 y fue abierta a la adhesión de todos los Estados. Hasta enero de 2023 había sesenta y ocho (35%) Estados parte de un total de ciento noventa y tres, y otros diecinueve (10%) habían adherido o habían sido invitados a acceder, observándose un progreso constante en su membresía (Council of Europe, 2023).

La Organización del Tratado del Atlántico Norte (OTAN) publicó en 2013 el *Manual de Tallin*, un código de conducta no vinculante sobre las operaciones cibernéticas que violan la prohibición del uso de la fuerza, dan derecho a los Estados a ejercer su derecho a la legítima defensa u ocurren durante un conflicto armado. En 2017, el *Manual* incluyó normas del derecho internacional que rigen los incidentes cibernéticos que caen por debajo de los umbrales del uso de la fuerza o el conflicto armado (CCDCOE, 2023).

En Europa, la Unión Europea, a partir de su Estrategia de ciberseguridad de 2013, la Organización para la Seguridad y la Cooperación en Europa (OESCE) y la Organización de Tratado del Atlántico Norte comparten la opinión de que el derecho internacional desempeña un papel central en la configuración del comportamiento de los Estados y los actores no estatales en el ciberespacio (Schmitt, 2020).

En el caso de *África*, que al igual que América Latina experimenta crecientes problemas de ciberseguridad (Kshetri, 2019), la Unión Africana (UA) aprobó en 2014 la Convención africana sobre ciberseguridad y protección de datos personales (Convención de Malabo), ratificada hasta marzo de 2023 por trece de los cincuenta y cinco Estados miembros. Luego de evaluaciones críticas sobre el alcance de las normas (Orji, 2019; GLACY+, 2016),

5 La Convención establece normas internacionales sobre infracciones del derecho de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de las redes. También confiere poderes y establece procedimientos como la búsqueda de redes informáticas y la interceptación.

se estableció en 2019 el Grupo Experto de Ciberseguridad (African Union, 2019). En el continente se observa asimismo el desarrollo de regímenes subregionales de cooperación sobre ciberseguridad, como el de la Comunidad de Estados de África Occidental (ECOWAS: Economic Community of West African State) (Orji, 2019).

Al igual que Europa y África, el Asia-Pacífico, además de su participación en las instituciones multilaterales, ha desarrollado una red creciente de regímenes plurilaterales y bilaterales sobre ciberseguridad. Destacan la Estrategia de cooperación de ciberseguridad de 2017, de la Asociación de Naciones del Sudeste Asiático (ASEAN: Association of Southeast Asian Nations); la creación del Grupo de Trabajo sobre Ciberseguridad de la Reunión de Ministros de Defensa (ADMMs) de ASEAN; y las iniciativas de diálogo promovidas por el Foro Regional de ASEAN (AR: ASEAN Regional Forum) desde 2004. Este último, integrado por veintiocho Estados, incluyendo a Estados Unidos, Rusia y China, entre otros, ha terminado reproduciendo el debate desarrollado en el marco del proceso del Grupo de Expertos Gubernamentales de la ONU. El Foro de Cooperación Económico de Asia-Pacífico (APEC: Asia-Pacific Economic Cooperation), integrado por veintiuna economías, desarrolló desde los atentados del 11 de septiembre de 2001 un régimen robusto de cooperación antiterrorista para garantizar la seguridad del comercio en la cuenca, incluyendo medidas en el ámbito de la ciberseguridad y una importante participación del sector privado (Nasu, 2021).

Junto a los regímenes regionales se observa la emergencia de otros de carácter interregional, o entre regiones y potencias, así como regímenes de carácter bilateral como los desarrollados por la Unión Europea con India (Callanan y otros, 2022), ASEAN, Japón y Corea del Sur (Christou y Raska, 2021) y Estados Unidos (Anagnostakis, 2021), e incluso entre China y Estados Unidos (Louie, 2017; Levite y Ginghua, 2019; XU y LU, 2021), entre otros.

A nivel de los Estados, desde el punto de vista del desarrollo de capacidades nacionales, en enero de 2023 el 94% de los países de la ONU habían aprobado legislación específica sobre delitos cibernéticos y pruebas electrónicas o estaban legislando. Como resultado de las reformas, ciento treinta Estados (67%) han adoptado disposiciones sustantivas de derecho penal para tipificar los delitos contra y por medio de computadoras. Otro 25% había adoptado al menos algunas disposiciones específicas de derecho penal sustantivo (Council of Europe, 2022).

Existe consenso en que el balance global de la gobernanza de ciberseguridad es insatisfactorio, y que además se desarrolla en un contexto internacional crecientemente competitivo, que dificulta llegar a acuerdos internacionales. A pesar de lo anterior, también se observa que, como señaló el editor del *Manual de Tallin*,

> la tendencia es muy positiva en general (…), los esfuerzos de la ONU son particularmente notables (…). La mayor disposición de los Estados a nombrar y avergonzar a los delincuentes (…) es igualmente alentadora. Otras señales positivas incluyen la disposición de los Estados a discutir normas voluntarias y no vinculantes de comportamiento responsable cuando no pueden llegar a un acuerdo sobre el estatus legal de una supuesta regla, así como el esfuerzo por elaborar medidas de fomento de la confianza en foros regionales como la OSCE, la Organización de los Estados Americanos y la ASEAN (Schmitt, 2020)[6].

6 La traducción es nuestra.

3

AMÉRICA LATINA EN LA CUARTA REVOLUCIÓN INDUSTRIAL Y LA GOBERNANZA DE LA CIBERSEGURIDAD

La evolución de la ciberseguridad en la región se desarrolla en el contexto de su inserción en la división internacional del trabajo en medio de la cuarta revolución industrial y del incremento de la desigualdad producida durante la globalización neoliberal.

A diferencia de otras regiones en desarrollo que han adelantado procesos de industrialización, como el Asia-Pacífico, la inserción de América Latina en la división internacional del trabajo ha sido la de una región esencialmente extractivista y exportadora de materias primas. Su competitividad se basa en gran medida en la abundancia de recursos naturales, con una brecha importante de productividad con las economías de Estados Unidos, Europa y los países emergentes de Asia. Entre 1990 y 2020, la participación de América Latina y el Caribe (ALC) en el valor agregado manufacturero del mundo disminuyó levemente, manteniéndose alrededor de 5% del total mundial, mientras que en el mismo periodo China aumentó de cerca del 2% al 30%, superando a Estados Unidos y Europa (Cepal, 2022).

Medida según conectividad (número de redes de fibra óptica, puntos de intercambio de Internet), centros de datos, supercomputadores, satélites, semiconductores, participación en las grandes empresas tecnológicas (*big tech*), el control de la nube o en cantidad de patentes asociadas a tecnologías avanzadas, la región no es parte de la revolución tecnológica y solo se incorpora en las etapas más tempranas de las cadenas de valor (Cepal, 2022).

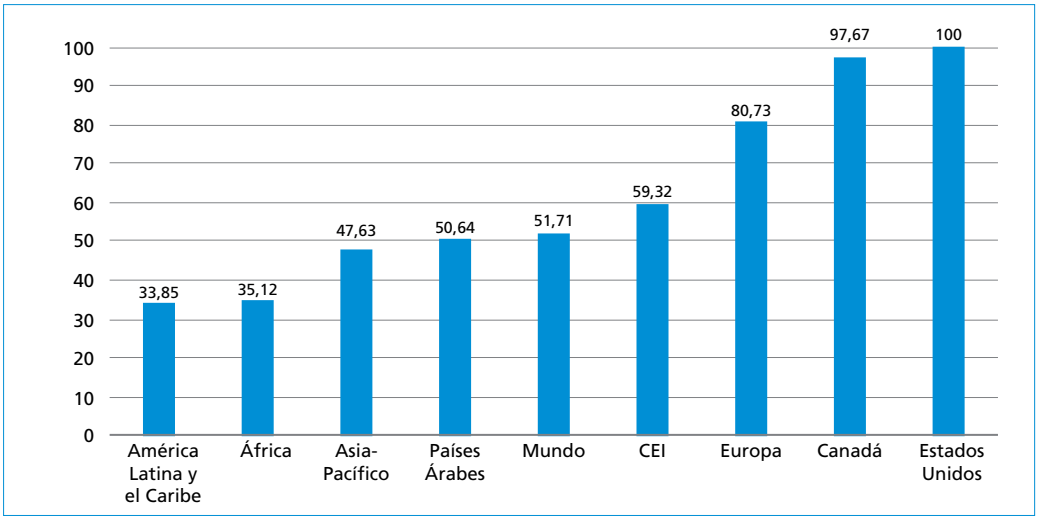
El acceso a la era digital requiere como infraestructura básica la conexión de banda ancha a Internet de alta velocidad, pero en 2019 cerca del 87% de la población de los países desarrollados utilizaba Internet, frente a tan solo el 19% en los países menos adelantados (Naciones Unidas, 2020: 4). Junto con África, los Estados árabes y la Comunidad de Estados Independientes (CEI), América Latina y el Caribe es una de las regiones rezagadas en la *brecha digital* (Hilbert, 2016; Ragnedda y Gladkova, 2020; Cepal, 2022). En 2021, la penetración promedio de la banda ancha fija en la región alcanzó casi el 62%, lo que la sitúa muy por debajo de América del Norte y Europa, con una penetración cercana al 100% y al 90%, respectivamente. En el caso de la banda ancha móvil, tenía una penetración del 78% de la población, mientras que en Europa y América del Norte el porcentaje era de 105% y cerca de 150% (Cepal, 2022).

A medida que incrementa su digitalización, la región ha comenzado a tener problemas de ciberseguridad. Si bien no hay información pública sobre conflictos políticos o incidentes cibernéticos entre Estados, el desarrollo lento e insuficiente de capacidades en el ámbito ciber (BID/OEA, 2020) ha tenido como consecuencia que en 2022 América Latina y el Caribe fuera la segunda zona del mundo con el mayor aumento de ciber ataques criminales semanales (29%), después de América del Norte: 52% (Checkpoint, 2023).

Los problemas de ciberseguridad en la región también están teniendo impactos políticos. Entre estos, existe evidencia de intervención en procesos electorales de numerosos Estados y de la diseminación masiva de noticias falsas y desinformación (OEA, 2019), por lo que la Comisión Interamericana de Derechos Humanos (CIDH) ha manifestado su preocupación por las dificultades que se observan para la plena vigencia de los derechos humanos en internet (CIDH, 2021).

El gráfico 1 resume la situación de América Latina y el Caribe desde una perspectiva global de ciberseguridad, basado en los indicadores del Índice Global de Cibersegu-

Gráfico 1
Índice de ciberseguridad global (GCI), 2020. Valores promedio



Fuente: autor con base en ITU, 2020.

ridad (CSI: Global Cybersecurity Index) publicado desde 2015 por la Unión Internacional de Telecomunicaciones con una evaluación de la calidad de la gobernanza de cinco grupos de indicadores[7] de ciento noventa y cuatro Estados y el Estado de Palestina, y de seis regiones[8]. De acuerdo con el Índice de 2020, la región muestra el valor promedio más bajo de todas las del mundo, con 33,85 puntos, menor al de África (35,12) y al promedio mundial: 50,64 (ITU, 2020).

Desde una perspectiva de gobernanza global ciber, desde el año 2000 el espacio más importante ha sido la Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, el foro de concertación política regional para la Cumbre Mundial sobre la Sociedad de la Información, y de política digital regional. Desde su creación, la Conferencia ha tenido ocho encuentros y ha establecido una cantidad similar de planes de acción regionales para desarrollar capacidades y reducir la brecha digital (Cepal, 2023). La Agenda Digital para América Latina y el Caribe (eLAC2024), aprobada por la Declaración de Montevideo de 2022, reúne treinta y un objetivos distribuidos en cuatro ejes, siendo el tercero el de "Gobernanza, seguridad y entorno habilitante". Los objetivos 11 y 12 corresponden a la promoción de políticas de ciberseguridad y ciberdelitos, respectivamente (Cepal, 2023).

El Foro de la Gobernanza de Internet ha realizado veintidós Iniciativas de diálogo regionales y subregionales en el mundo, de las cuales tres han sido con el Caribe, Centro América y América Latina y el Caribe. El objetivo de las iniciativas ha sido contribuir a identificar asuntos relevantes y prioritarios para la región, que deben ser considerados y discutidos regional y globalmente; asimismo, promover la participación regional en los debates mundiales pertinentes (Naciones Unidas, 2023). Organizada en torno a la Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, se logró concertar una agenda para el cierre de la brecha digital y el desarrollo de capacidades (Cepal, 2021; Cepal, 2022).

3.1 CIBERSEGURIDAD EN AMÉRICA LATINA

En la región se ve poca voluntad de concertación en torno a los debates globales sobre ciberseguridad en todas sus dimensiones, un débil desarrollo de regímenes regionales y un esfuerzo concentrado en el desarrollo de capacidades nacionales al respecto.

7 Medidas legales, técnicas, de organización, de desarrollo de capacidades y de cooperación.

8 África, América (incluyendo a Estados Unidos y Canadá), Estados árabes, Asia-Pacífico, Comunidad de Estados Independientes y Europa.

En el caso de las negociaciones multilaterales sobre ciberseguridad, el rasgo más importante de la región es la fragmentación en torno a coaliciones internacionales *like minded* en el debate global y, consecuentemente, una importante ausencia de agencia política en los debates globales, incluyendo los relativos a ciberseguridad e inteligencia artificial.

Cinco países, Argentina, Brasil, Colombia, México y Uruguay, han concurrido expresando posturas nacionales en los cuatro Grupos de Expertos Gubernamentales que adoptaron informes de consenso: 2010, 2013, 2015 y 2021.

El Grupo de Trabajo de Composición Abierta ha permitido una mayor participación de actores de la región, pero no se observa concertación regional. Desde su creación en 2019, la Secretaría General de las Naciones Unidas registra declaraciones o documentos de dieciséis Estados latinoamericanos: Argentina, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, México, Nicaragua, Paraguay, Perú, República Dominicana, Surinam, Uruguay y Venezuela, de la Organización de los Estados Americanos y de cuatro organizaciones de la sociedad civil: Instituto Igarapé de Brasil, Derechos Digitales de Chile, Fundación Karisma de Colombia y Red en Defensa de los Derechos Digitales de México (UN, 2020; United Nations, 2023).

En el caso de la decisión más reciente de la Asamblea General de poner fin a los debates de doble vía (Grupos de Expertos Gubernamentales / Grupo de Trabajo de Composición Abierta) y establecer un foro permanente de las Naciones Unidas para examinar el uso de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional, la región votó dividida. Seis Estados: Argentina, Chile, Colombia, Ecuador, Paraguay y República Dominicana, adhirieron a la coalición de cuarenta y nueve (incluyendo a Estados Unidos) que propusieron el Programa de Acción para promover el comportamiento responsable de los Estados en el ciberespacio. El Programa fue aprobado por ciento cincuenta y siete votos a favor y seis en contra, incluyendo Nicaragua, además de China, la Federación Rusa, Irán, República Popular Democrática de Corea y Siria, y catorce abstenciones, entre las que se contaba la de Cuba (digwatch, 2020).

En el ámbito criminal de la ciberseguridad tampoco se observa concertación. La región no tiene una postura frente al debate en torno a la propuesta encabezada por Rusia de establecer un Comité Especial (AHC) para la elaboración de una convención internacional, por un lado, y los Estados partidarios de ampliar la Convención de Budapest, por otro. A la fecha, nueve países de América Latina han adherido a la Convención de Budapest (Argentina, Brasil, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana), mientras que otros cinco, Ecuador, Guatemala, México, Trinidad y Tobago y Uruguay, han sido invitados a adherir. Estados Unidos y Canadá son miembros plenos (Council of Europe, 2023).

3.2 REGÍMENES REGIONALES DE CIBERSEGURIDAD

El desarrollo de regímenes e instituciones de gobernanza regional sobre ciberseguridad es incipiente. Los avances más importantes se han registrado en el *ámbito interamericano*. En 2003 y 2004 la OEA aprobó dos resoluciones que originaron la "Estrategia de seguridad cibernética", poniendo en marcha procesos de cooperación en los ámbitos político, de desarrollo de capacidades y criminal. La Estrategia estableció mandatos específicos para el Comité Interamericano contra el Terrorismo (Cicte), la Comisión Interamericana de Telecomunicaciones (Citel), la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (Remja) y su Grupo de Expertos Gubernamentales en Materia de Delito Cibernético.

En 2012 el Comité Interamericano contra el Terrorismo aprobó la declaración "Fortalecimiento de la seguridad cibernética de las Américas", en la que establece los objetivos y las áreas de la cooperación interamericana y su Plan de trabajo. El Comité puso en marcha un programa sobre ciberseguridad, concentrado en torno a la capacitación y el apoyo técnico para el desarrollo de políticas y el fortalecimiento de las capacidades de ciberseguridad de los Estados, y el incremento de la cooperación e intercambio de información contra la actividad criminal en el ámbito ciber.

En 2016 la Comisión de Seguridad Hemisférica de la OEA adoptó la primera medida de confianza mutua no tradicional en el ámbito ciber. Basados en las recomendaciones del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional de 2010, 2013 y 2015, en 2017 los Estados Miembros acordaron establecer el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio (Cicte, 2019: 3-4), que ha desarrollado cuatro reuniones: 2018, 2019, 2021 y 2022.

Desde entonces, los Estados de la región han avanzado mediante la designación de puntos focales y el intercambio de información sobre políticas nacionales sobre ciberseguridad e incidentes cibernéticos. A partir de los diagnósticos realizados, en 2022 el Cicte avanzó hacia medidas de fomento de la confianza de distinto orden.

Por un lado, acordó promover la inclusión, la participación y el liderazgo de las mujeres en los procesos de toma de decisiones vinculadas a las tecnologías de la información y las comunicaciones, y medidas para reducir la brecha digital de género, de conformidad con la Agenda de Mujer, Paz y Seguridad; así como el trabajo y el diálogo con la sociedad civil, las instituciones educativas, el sector privado y la comunidad técnica, entre otros. Por otro, acordó avanzar gradualmente hacia un régimen regional más robusto, incorporando dos recomendaciones sustantivas para la conducta internacional de los Estados del Sistema Interamericano.

La primera fue:

> promover el estudio, debate, desarrollo y creación de capacidades en los ámbitos nacional e internacional respecto a la aplicación del derecho internacional al uso de las tecnologías de la información y la comunicación en el contexto de la seguridad internacional, promoviendo el intercambio voluntario de posiciones y declaraciones de visión nacionales, opiniones, legislaciones, políticas y prácticas sobre la materia, a fin de promover entendimientos comunes.

El segundo acuerdo fue:

> promover la implementación de las 11 normas voluntarias no vinculantes sobre comportamiento responsable de los Estados en el ciberespacio adoptadas en la resolución 70/237 de la Asamblea General de Naciones Unidas y promover la presentación de informes sobre estas actividades, teniendo en cuenta la encuesta de implementación nacional.

Adicionalmente, el Comité Interamericano contra el Terrorismo acordó elaborar esquemas nacionales de severidad de incidentes cibernéticos y compartir información sobre estos (Cicte, 2022: 1).

Junto con el régimen incipiente de medidas de confianza mutua, en el ámbito de las capacidades, la OEA y el Banco Interamericano de Desarrollo (BID) han publicado dos reportes, basados en el Modelo de madurez de la capacidad de ciberseguridad para las naciones (CMM: Cybersecurity. Capacity Maturity Model for Nations).

De acuerdo con el segundo (2020), desde 2016 los países de América Latina y el Caribe han venido mejorando sus capacidades de ciberseguridad. Según el CMM, el nivel de madurez promedio de la región todavía está entre 1 y 2, en el que 1 significa etapa Inicial y 5 Dinámica o avanzada. De acuerdo con el informe,

> la mayoría de los países de América Latina y el Caribe han comenzado a formular iniciativas de seguridad cibernética, incluidas las medidas de creación de capacidad. Mejor aún: algunas de ellas ya están siendo implementadas, pero de manera *ad hoc* y sin coordinación entre los actores clave. Sin embargo, el nivel de madurez promedio de los 32 países en materia de ciberseguridad no debe opacar la importancia de los avances logrados por la región en los últimos cuatro años (2016-2020) (BID/OEA, 2020: 17).

Hasta principios de 2020, solamente diecisiete de treinta y dos países analizados por la OEA/BID habían aprobado una estrategia nacional de ciberseguridad (en 2016 eran cinco), y solo diez habían establecido un organismo gubernamental central responsable de la ciberseguridad.

Adicionalmente, en el ámbito criminal la OEA puso en marcha el Grupo de Trabajo en Materia de Delito Informático de la Reunión de Ministros de Justicia de las Américas.

En Latinoamérica no se observa el desarrollo de regímenes de ciberseguridad. En 2023 la Comunidad de Es-

tados Latinoamericanos y Caribeños (Celac) adoptó la Declaración de Buenos Aires, que en el capítulo sobre transformación digital incluye tres párrafos sobre ciberseguridad, pero no ha avanzado hacia la adopción de normas o estándares en ese ámbito.

La región tiene asimismo algunos acuerdos subregionales o plurilaterales sobre ciberseguridad. En el caso de América Central, el Sistema de Integración Centroamericana (Sica) adoptó la Estrategia regional digital para el desarrollo de la sociedad de la información y el conocimiento en el Sica, ERDI, ejecutada por el Grupo *ad hoc* que adoptó la "Agenda regional digital del Sica" para el periodo 2022-2025. El Área de Acción 5 del Plan de acción 2022-2023 aborda la "Seguridad digital", y definió como objetivo "fortalecer el marco jurídico regional para la protección de derechos de la población; la ciberseguridad y la protección de los activos de la información de la población; así como la coordinación regional e internacional para la prevención y respuesta ante incidentes cibernéticos" (Sica, 2015).

La Comunidad de Estados del Caribe (Caricom) inició su trabajo en 2013. En 2016 puso en marcha el Plan de acción sobre ciberseguridad y cibercrimen, que identificó cinco áreas prioritarias de intervención: conciencia pública; creación de capacidad sostenible; normas técnicas e infraestructura; entorno jurídico; y colaboración de cooperación regional e internacional - respuesta a incidentes y ciberdelincuencia. También estableció una estructura de gobernanza organizada en torno a un comité ejecutivo (en el que participa el Cicte de la OEA); un Comité Regional Ciber, de carácter intergubernamental; y puntos focales nacionales (Caricom, 2016). En 2017 aprobó la "Visión y hoja de ruta para el espacio único de tecnologías de comunicación e información", como marco general de gobernanza ciber (Caribbean Telecommunications Union, 2017).

En el caso de América del Sur, en 2017 el Consejo de Defensa Sudamericano constituyó un Grupo de Trabajo sobre Ciberseguridad, pero la crisis que condujo al término de la Unión de Naciones Suramericanas (Unasur) detuvo los avances. La Declaración de Brasilia de 2023 incluyó, en su N° 8, la promoción de iniciativas de cooperación sudamericana, incluyendo "transformación digital (…), combate al crimen transnacional organizado y ciberseguridad" (NODAL, 2023).

También en el plano subregional, el Mercado Común del Sur (Mercosur) puso en marcha en 2017 el Grupo Agenda Digital (GAD), que en 2018 aprobó su primer Plan de acción, el cual incluye compromisos sobre infraestructura digital y conectividad; seguridad y confianza en el ambiente digital; economía digital; habilidades digitales; gobierno digital, gobierno abierto e innovación pública; aspectos técnicos y regulatorios; y coordinación en foros internacionales (Mercosur, 2023).

Por último, la Alianza del Pacífico estableció entre sus áreas de trabajo un Grupo Técnico en el ámbito digital, creó un Subcomité de Economía Digital y un área de trabajo sobre mercado digital regional. La Declaración de Cali (2017) incluyó "potenciar la cooperación de los países de la Alianza del Pacífico en materia de seguridad digital y fomento de la confianza en el uso de las TIC". La Hoja de ruta del Subgrupo Agenda Digital considera medidas sobre ecosistema digital, incluyendo la "seguridad digital".

4

CONCLUSIONES

El examen del desarrollo de la gobernanza de la ciberseguridad en América Latina revela que desde una perspectiva comparada la región presenta un rezago importante. A diferencia de otras regiones del Sur global que durante el último medio siglo llevaron adelante procesos de industrialización y son actores de la cuarta revolución industrial (4RI), América Latina se ha mantenido como esencialmente extractivista y exportadora de materias primas. Junto con África, los Estados árabes, la Comunidad de Estados Independientes, y el Caribe, es una de las regiones más rezagadas en la *brecha digital* y sus Estados tienen el valor promedio más bajo en los indicadores globales de gobernanza de ciberseguridad de organismos de las Naciones Unidas como la Unión Internacional de Telecomunicaciones.

A pesar de que la región ha desarrollado una gobernanza robusta de seguridad regional y ha sido denominada "zona de paz", basada en el desarrollo de regímenes regionales de carácter vinculante que regulan tanto las capacidades cinéticas (desarme de armas de destrucción masiva y convencionales) como las intenciones estratégicas (observancia del derecho internacional, prevención y solución pacífica de controversias, transparencia de defensa), no tiene una identidad regional cooperativa y amical similar sobre ciberseguridad, tanto global como regional, aunque en el último caso se observan algunos pasos en esa dirección.

En el ámbito global, la principal característica de la participación de América Latina y el Caribe en los foros de construcción de regímenes globales sobre ciberseguridad, como el Grupo de Expertos Gubernamentales o el Grupo de Trabajo de Composición Abierta, ha sido la ausencia de concertación regional y la fragmentación.

En algunos asuntos y coyunturas en el debate sobre ciberseguridad, algunos Estados latinoamericanos se han alineado en torno a los bloques dirigidos por Estados Unidos, Rusia o China, mientras que en otros han optado por adherir o promover la organización de grupos de países afines (*like minded*) integrados por Estados de distintas regiones. La fragmentación se expresó también en la convocatoria que permitió la aprobación del Programa de acción luego del término del mandato del Grupo de Trabajo de Composición Abierta en 2025.

A pesar de la fragmentación en los procesos de negociación, los Estados latinoamericanos y caribeños han concurrido con su apoyo a los procesos de generación de consensos normativos propuestos por el Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta aprobados posteriormente por la Asamblea General.

La fragmentación latinoamericana se observa también en la posición de los Estados en el debate sobre la gobernanza de la ciberseguridad en el ámbito criminal. Mientras una cantidad creciente (catorce) adhirió al Convenio de Budapest del Consejo de Europa o iniciaron el proceso de hacerlo, otros decidieron apoyar el Comité Intergubernamental Especial de Expertos de Composición Abierta establecido por la Tercera Comisión de la Asamblea General en 2019, para elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

El análisis del regionalismo latinoamericano sobre ciberseguridad pone de presente también algunas características. La primera se refiere a las debilidades de la inserción de la región en la cuarta revolución industrial resumida en las secciones anteriores, incluyendo un de-

sarrollo heterogéneo y desigual de capacidades digitales y de ciberseguridad. Pocos países han explicitado sus políticas de ciberseguridad y muchos menos en ciberdefensa, y no se conocen o no existen posiciones oficiales en la gran mayoría de los Estados sobre los procesos de toma de decisión en los que se construye la gobernanza global de internet y de la ciberseguridad.

La segunda característica se refiere el tipo de regionalismo sobre ciberseguridad desarrollado hasta 2023. El régimen emergente más importante se ha ido organizando en el ámbito interamericano y ha privilegiado una cooperación limitada, aunque creciente, en materia judicial y criminal, de fortalecimiento de capacidades y de transparencia en torno a las medidas acordadas en el marco del Comité Interamericano contra el Terrorismo de la OEA, basadas en las recomendaciones del Grupo de Expertos Gubernamentales de las Naciones Unidas. Se trata de un régimen de transparencia gradualmente más complejo y robusto que puede legitimar el avance hacia regímenes más ambiciosos y vinculantes.

Además de los regímenes interamericanos de ciberseguridad, y reproduciendo la tradición multinivel regional, existe un creciente desarrollo de regímenes subregionales, como es el caso del Sica, del Caricom, del Mercosur o de la Alianza del Pacífico. En todos los casos se trata, sin embargo, de normas no vinculantes, concentradas en el desarrollo de capacidades, la coordinación de políticas y la transparencia conforme a las recomendaciones y estándares aprobadas por el Grupo de Expertos Gubernamentales de la Primera Comisión de la Asamblea General.

A diferencia de la tradición latinoamericana en otros ámbitos de seguridad, como desarme, prevención y resolución pacífica de conflictos, y de que otras regiones como Europa y África han desarrollado regímenes regionales más robustos sobre ciberseguridad, o incluso en áreas más complejas, como ciberdefensa en el caso de ASEAN, América Latina y el Caribe parecen carecer de la voluntad de avanzar hacia regímenes que establezcan normas regionales de carácter vinculante para la conducta de los Estados, optando por adoptar los estándares no vinculantes aceptados en el marco de la Asamblea General de la ONU.

De esa manera, la evolución de los regímenes sobre ciberseguridad en América Latina no se diferencia de la crisis del regionalismo latinoamericano. Como en otros ámbitos de la política internacional, la región está enfrentando la configuración de la nueva gobernanza internacional sobre ciberseguridad de manera fragmentada, vulnerable a la captura geopolítica de las potencias que disputan la hegemonía internacional y ausente como actor global.

REFERENCIAS

African Union. 2019. "African Union Cybersecurity Expert Group holds its first inaugural meeting". 12 de diciembre. https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting (último acceso: 3 de febrero de 2023).

Aguilar Antonio, Juan Manuel. 2020. "La brecha de ciberseguridad en América Latina rente al contexto global de ciberamenazas". *RESI: Revista de estudios en seguridad internacional*. 6 (2): 17-43.

Albarracín, Juan. 2023. "Crimen organizado en América Latina". *Paz y Seguridad*. Febrero. Friedrich-Ebert-Stiftung. Bogotá.

Anagnostakis, Dimitrios. 2021. "The European Union-United States cybersecurity relationship: A transatlantic functional cooperation". *Journal of Cyber Policy*. 6 (2): 243-261.

BID/OEA. 2020. "Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020". https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe (último acceso: 2 de febrero de 2023).

Boulanin, Vincent, Laura Bruun y Netta Goussac. 2021. "Autonomous Weapons Systems and International Humanitarian Law. Identifying Limits and the Required Type and Degree of Human–Machine Interaction". Junio. https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf (último acceso: 12 de febrero de 2023).

Callanan, Cormac, Basu Chandola, Hannes Ebert, Caitriona Heinl y Anirban Sarma. 2022. "Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives". Octubre. https://www.orfonline.org/research/enhancing-global-cybersecurity-cooperation/ (último acceso: 2 de junio de 2023).

Caribbean Telecommunications Union. 2017. "Vision and Roadmap for a CARICOM Single ICT Space". Febrero. https://caricom.org/documents/15510-vision_and_roadmap_for_a_single_ict_space_-_final_version_updated.pdf (último acceso: 2 de abril de 2023).

Caricom. 2016. "CARICOM Cyber Security and Cybercrime Action Plan". https://caricomimpacs.org/wp-content/uploads/2020/11/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan.pdf (último acceso: 16 de marzo de 2023).

CCDCOE. 2023. *The Tallinn Manual.* https://ccdcoe.org/research/tallinn-manual/ (último acceso: 2 de junio de 2023).

Cepal. 2023. *Conferencia ministerial sobre la sociedad de la información de América Latina y el Caribe.* https://www.cepal.org/es/organos-subsidiarios/conferencia-ministerial-la-sociedad-la-informacion-america-latina-caribe (último acceso: 4 de febrero de 2023).

----------. 2022. "Un camino digital para el desarrollo sostenible de América Latina y el Caribe". https://www.cepal.org/es/publicaciones/48460-un-camino-digital-desarrollo-sostenible-america-latina-caribe (último acceso: 25 de febrero de 2023).

----------. 2021. "Tecnologías digitales para un nuevo futuro". https://www.cepal.org/es/publicaciones/46816-tecnologias-digitales-un-nuevo-futuro (último acceso: 20 de febrero de 2023).

Checkpoint. 2023. *Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks*. https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (último acceso: 24 de marzo de 2023).

Christou, George y Michael Raska. 2021. "Cybersecurity". En Thomas Christiansen, Emil Kirchner y See Seng Tan. *The European Union´s Security Relations with Asian Partners*, 209-230. Palgrave Macmillan. Cham, Switzerland.

CICR. 2015. "El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos". Octubre. file:///C:/Users/Goethe/Downloads/32ic-report-on-ihl-and-the-challenges-of-armed-conflicts_es.pdf (último acceso: 20 de enero de 2023).

CICTE. 2022. *Medidas de fomento de la confianza adicionales para promover la cooperación y la confianza en el ciberespacio.* 27 de octubre. https://www.oas.org/es/sms/cicte/ciberseguridad/sesiones/ordinarias/2022/ (último acceso: 25 de mayo de 2023).

----------. 2021. "Informe sobre medidas de fomento de cooperación y confianza en el ciberespacio". https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp (último acceso: 25 de mayo de 2023).

----------. 2019. "Informe sobre medidas de fomento de cooperación y confianza en el ciberespacio". 21 de julio. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp (último acceso: 25 de mayo de 2023).

CIDH. 2021. "La CIDH advierte un punto de inflexión de la libertad de expresión en internet y convoca a diálogo en la región". 5 de febrero. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/026.asp (último acceso: 20 de febrero de 2023).

Cihon, Peter y Matthijs M. Maas. 2020. "Fragmentation and the Future: Investigating Architectures for International AI Governance". *Global Policy*. 11 (5): 545-556.

Costas Trascasas, Milena. 2022. "Tecnología y desigualdad: la gobernanza tecnológica como nuevo paradigma de la seguridad internacional". *Revista de Estudios en Seguridad Internacional*. 8 (2): 89-107.

Council of Europe. 2023. "Chart of signatures and ratifications of Treaty 185". 8 de marzo. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (último acceso: 8 de marzo de 2023).

----------. 2023. *The Budapest Convention (ETS No. 185) and its Protocols*. https://www.coe.int/en/web/cybercrime/the-budapest-convention?_82_struts_action=%2Flanguage%2Fview&_82_languageId=fr_FR# (último acceso: 2 de febrero de 2023).

----------. 2022. *The Global State of cybercrime legislation 2013.2023. A cursory overview.* 31 de diciembre. file:///C:/Users/Goethe/Downloads/Council%20of%20Europe,%202022.%20The%20Global%20State%20of%20cybercrime%20legislation%202013.2023.%20A%20cursory%20overview..pdf (último acceso: 2 de marzo de 2023).

Coveware. 2021. *Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority.* 23 de julio. https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority (último acceso: 10 de febrero de 2023).

Dammert, Lucía. 2022. "Avances y limitaciones de la reforma policial en América Latina". En Rafa Martínez. *El papel de las Fuerzas Armadas en la América Latina del siglo XXI*, 109-136. Centro de Estudios Políticos y Constitucionales. Madrid.

digwatch. 2023. "Elections in the Digital Age". https://dig.watch/trends/elections-digital-age (último acceso: 20 de febrero de 2023).

----------. 2020. *France and partners propose a programme of action for advancing responsible state behaviour in cyberspace.* 8 de octubre. https://dig.watch/updates/france-and-partners-propose-programme-action-advancing-responsible-state-behaviour (último acceso: 3 de febrero de 2023).

Eichensehr, Kristen E. 2022. "Ukraine, Cyberattacks, and the Lessons for International Law". *AJIL Unbound*. 116: 145-149.

Evans, Sam Weiss y otros. 2020. "Embrace experimentation in biosecurity governance". *Science*. 360 (6487): 138-140.

Fidler, David P. 2021. "Cyberspace and Human Rights". En Nicholas Tsagourias y Russell Buchan. *Research Handbook on International Law and Cyberspace*, 130-151. Edward Elgar Publishing Limited. Cheltenham, UK.

Freedom House. 2023. "Freedom on the Net 2022. Countering an Authoritarian Overhaul of the Internet".

https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf (último acceso: 6 de marzo de 2023).

GLACY+. 2016. "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime". https://rm.coe.int/16806bf0f8 (último acceso: 3 de febrero de 2023).

González, Guadalupe, Mónica Hirst, Carlos Luján, Carlos Romero y Juan Gabriel Tokatlian. 2021. "Coyuntura crítica, transición de poder y vaciamiento latinoamericano". *Nueva Sociedad*. 291. Enero-Febrero: 49-65.

González, Yanilda María. 2021. *Authoritarian Police in Democracy. Contested Security in Latin America.* Cambridge University Press. Camdrigde.

Henderson, Christian. 2021. "The United Nations and the regulation of cyber-security". En Nicholas Tsagourias y Russell Buchan. *Research Handbook on International Law and Cyberspace*, 582-614. Edward Elgar Publishing. Cheltenham, UK.

Hernández-Orallo, José. 2019. "Unbridled mental power". *Nature Phys*. 15 (106).

Hilbert, Martin. 2016. "The bad news is that the digital access divide is here to stay: Domestically installed bandwidths among 172 countries for 1986-2014". *Telecommunications Policy*. 40 (6): 567-581.

IBM. 2023. *Cómo las tecnologías de la Industria 4.0 están cambiando la fabricación.* https://www.ibm.com/es-es/topics/industry-4-0?mhsrc=ibmsearch_a&mhq=Industria%204%26period%3B0 (último acceso: 2 de marzo de 2023).

IDEA Internacional. 2021. "El estado de las democracias en las Américas. Democracia en tiempos de crisis". https://www.idea.int/gsod/sites/default/files/2021-11/estado-de-la-democracia-en-las-americas-2021.pdf.

Institute for Economics & Peace. 2023. "Global Peace Index 2023: Measuring Peace in a Complex World". Sydney.

ITU. 2020. "Global Cybersecurity Index". https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (último acceso: 10 de enero de 2023).

----------. 2022. "Measuring digital development: Facts and Figures 2022". https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (último acceso: 20 de febrero de 2023).

----------. 2023. *ITU Cybersecurity Activities*. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx (último acceso: 12 de febrero de 2023).

Kacowicz, Arie. 1998. *Zones of Peace in the Third World. South America and West Africa in Comparative Perspective.* State University of New York Press. New York.

Kshetri, Nir. 2019. "Cybercrime and Cybersecurity in Africa". *Journal of Global Information Technology Management*. 22 (2): 77-81.

Kurbalija, Jovan. 2016. *Introducción a la gobernanza de Internet.* 7a. DiploFoundation. Ginebra.

Lasi, Heiner, Peter Fettke, Thomas Feld y Michael Hoffman. 2014. "Industry 4.0". *Business & Information Systems Engineering*. 6: 239-242.

Levite, Ariel (Eli) y Lyu Ginghua. 2019. "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?". 24 de enero. https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213 (último acceso: 10 de julio de 2023).

Louie, Celia. 2017. "U.S.-China Cybersecurity Cooperation". 8 de septiembre. https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/ (último acceso: 10 de julio de 2023).

Mercosur. 2023. *Agenda digital*. https://www.mercosur.int/temas/agenda-digital/ (último acceso: 2 de abril de 2023).

Naciones Unidas. 2010. "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe del Secretario General". https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/458/45/PDF/N1045845.pdf?OpenElement (último acceso: 2 de febrero de 2023).

----------. 2015. *Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.*

Nota del Secretario General. 22 de julio. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/38/PDF/N1522838.pdf?OpenElement (último acceso: 15 de febrero de 2023).

----------. 2020. "Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital. Informe del Secretario General". 29 de mayo. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/54/PDF/N2010254.pdf?OpenElement (último acceso: 19 de diciembre de 2022).

----------. 2021. "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Nota del Secretario General". 18 de marzo. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/75/PDF/N2106875.pdf?OpenElement (último acceso: 10 de febrero de 2023).

----------. 2021. "Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report". 10 de marzo. https://front.unarm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (último acceso: 12 de febrero de 2023).

----------. 2022. "Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General". 8 de junio. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/375/61/PDF/N2237561.pdf?OpenElement (último acceso: 6 de febrero de 2023).

----------. 2022. "Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional". 13 de octubre. https://digitallibrary.un.org/record/3991743?ln=en (último acceso: 10 de febrero de 2023).

----------. 2023. *Oficina de Asuntos de Desarme*. https://www.un.org/disarmament/es/ (último acceso: 23 de febrero de 2023).

----------. 2023. *Regional IGF Initiatives*. https://www.intgovforum.org/en/content/regional-igf-initiatives (último acceso: 3 de febrero de 2023).

Nakayama, Bryan. 2023. "No shortcuts: Why states struggle to develop a military cyber-force". *International Affairs*. 99 (1). January: 374-375.

Nasu, Hitosi. 2021. "Cyber security in the Asia-Pacific". En Nicholas Tsagourias y Russell Buchan. *Research Handbook on International Law and Cyberspace*, 564-581. Edward Elgar Publishing. Cheltenham, UK.

Nicholson, Simon y Jesse L. Reynolds. 2020. "Taking Technology Seriously: Introduction to the Special Issue on New Technologies and Global Environmental Politics". *Global Environmental Politics*. 20 (3): 1-8.

NODAL. 2023. "Cumbre suramericana: la declaración final del "Consenso de Brasilia" y los discursos de los presidentes". 2 de junio. https://www.nodal.am/2023/06/cumbre-suramericana-la-declaracion-final-del-consenso-de-brasilia-y-los-discursos-de-los-presidentes/ (último acceso: 10 de julio de 2023).

Nolte, Detlef y Brigitte Weiffen. 2018. "Competing Claims for Security Governance in South America". En Stephen Aris, Aglaya Snetkov y Andreas Wenger. *Inter-organizational Relations in International Security. Cooperation and Competition*, 138-158. Routledge. London.

OEA. 2019. "Consideraciones de ciberseguridad del proceso democrático para América Latina y el Caribe". https://www.oas.org/es/sms/cicte/docs/ESP-Cybersecurity-Democratic-Process-LAC.pdf (último acceso: 2 de febrero de 2023).

Oelsner, Andrea. 2016. "Pluralistic security communities in Latin America". En David R. Mares y Arie M. Kacowicz. *Routledge handbook of Latin American security*, 173-184. Routledge. New York.

Orji, Uchenna Jerome. 2019. "An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states". *Computer Law & Security Review*. 35 (6).

----------. 2018. "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?". *Masaryk University Journal of Law and Technology*. 12 (2): 91-129.

Ragnedda, Massimo y Anna Gladkova. 2020. "Understanding Digital Inequalities in the Global South". En Massimo Ragnedda y Anna Gladkova. *Digital Inequalities in the Global South*, 17-30. Springer. Cham, Switzerland.

Reyes Matta, Fernando. 2022. "La confrontación de ciberseguridad entre Estados Unidos y China y sus derivaciones para América Latina". 31 de agosto. https://politica-china.org/areas/seguridad-y-defensa/la-confrontacion-de-ciberseguridad-entre-Estados-unidos-y-china-y-sus-derivaciones-para-america-latina (último acceso: 24 de febrero de 2023).

Rhiannon, Neilsen. 2023. "Coding protection: 'Cyber humanitarian interventions' for preventing mass atrocities". *International Affairs*. 99. January: 299-319.

Robledo Hoecker, Marcos. 2022. "Militarización, emergencia del militarismo civil y erosión democrática en América Latina". *Documento de Trabajo*. Fundación Carolina.

Robledo, Marcos. 2021. "La transformación estratégica argentino-chilena y ecuatoriano-peruana, y los desafíos de la relación chileno-peruana. Un análisis comparado". *Paz y Seguridad*. Agosto. Friedrich-Ebert-Stigtung. Bogotá. https://library.fes.de/pdf-files/bueros/la-seguridad/18241.pdf.

Robledo, Marcos y Francisco Rojas. 2002. "Construyendo un régimen cooperativo de seguridad en el Cono Sur de América Latina. Elementos conceptuales, políticos y estratégicos". *Fuerzas Armadas y Sociedad*. 17 (1-2), enero-junio: 5-31.

Roncagliolo, Rafael, Marcos Robledo, Óscar Vidarte y Juan Gabriel Valdés. 2021. *Perú y Chile. Del antagonismo a la cooperación: el camino hacia la transformación del vínculo bilateral.* Planeta. Lima.

Sarmiento Lamus, Andrés. 2016. "Impacto e implementación en Colombia de la decisión de fondo de la Corte Internacional de Justicia en el diferendo territorial y marítimo (Nicaragua c. Colombia)". *Anuario Mexicano de Derecho Internacional*. XVI. Agosto: 401-423.

Schmidt, Eric. 2023. "Innovation Power. Why Technology Will Define the Future of Geopolitics". *Foreign Affairs*. March/April.

Schmitt, Michael N. 2017. "Grey Zones in the International Law of Cyberspace". *The Yale Journal of International Law Online*. May.

----------. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge University Press. Cambridge.

----------. 2020. *Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive.* 28 de febrero. https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counterproductive/ (último acceso: 3 de febrero de 2023).

Schwab, Klaus. 2016. *The Fourth Industriual Revolution.* World Economic Forum. Geneve.

Sica. 2015. "Estrategia regional digital para el desarrollo de la sociedad de la información y el conocimiento en el Sica, ERDI". Marzo. https://www.sica.int/documentos/estrategia-regional-digital-del-sica_1_104748.html (último acceso: 7 de marzo de 2023).

Solar, Carlos. 2023. *Cybersecurity Governance in Latin America. States, Threats, and Alliances.* State University of New York Press. Albany.

The White House. 2015. *Remarks by the President at the Cybersecurity and Consumer Protection Summit.* 13 de febrero. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit (último acceso: 3 de febrero de 2023).

UN. 2020. "Joint civil society feedback on the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security revised non-paper norms proposals". Octubre. https://front.un-arm.org/wp-content/uploads/2020/10/joint-civil-society-groups-feedback-on-oewg-norms-proposals.pdf (último acceso: 4 de febrero de 2023).

Unidir. 2023. *Security Dimensions of Innovations in Science and Technology*. https://www.unidir.org/projects/security-dimensions-innovations-science-and-technology (último acceso: 23 de febrero de 2023).

United Nations. 2023. *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Counte-*

ring the Use of Information and Communications Technologies for Criminal Purposes. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (último acceso: 2 de febrero de 2023).

----------. 2023 "Open-Ended Working Group on Information and Communication Technologies". https://meetings.unoda.org/meeting/57871 (último acceso: 21 de marzo de 2023).

----------. 2020. *Remarks to the General Assembly on the Secretary-General's priorities for 2020.* 22 de enero. https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020 (último acceso: 3 de febrero de 2023).

UNODC. 2021. *Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 6 al 8 de abril de 2021*. 19 de abril. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V21/025/98/PDF/V2102598.pdf?OpenElement (último acceso: 3 de febrero de 2023).

----------. 2022. "Intentional homicide". Editado por data UNODC. https://dataunodc.un.org/dp-intentional-homicide-victims-est (último acceso: 2 de septiembre de 2022).

Vint, Sherryl. 2020. "Introduction". En Sherryl Vint. *After the Human. Culture, Theory, and Criticism in the 21st Century*, 1-10. Cambridge University Press. Cambridge. Edición de Kindle.

Voo, Julia, Irfan Hemani y Daniel Cassidy. 2022. *National Cyber Power Index 2022.* Belfer Center for Science and International Affairs, Harvard Kennedy School. Cambridge, Mass.

WEF. 2017. "Agile Governance. Reimagining Policy-making in the Fourth Industrial Revolution". *White Paper*. https://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf (último acceso: 22 de febrero de 2023).

XU, Manshu y Chuanying LU. 2021. "China–U.S. cyber-crisis management". *China International Strategy Review*. 3: 97-114.

SIGLAS

4RI	cuarta revolución industrial
ACG	Agenda Mundial de Ciberseguridad
ADMMs	Grupo de Trabajo sobre Ciberseguridad de la Reunión de Ministros de Defensa (África)
ALC	América Latina y el Caribe
APEC	Foro de Cooperación Económico de Asia-Pacífico (Asia-Pacific Economic Cooperation)
ASEAN	Asociación de Naciones del Sudeste Asiático (Association of Southeast Asian Nations)
BID	Banco Interamericano de Desarrollo
Caricom	Comunidad de Estados del Caribe
CCPCJ	Comisión de Prevención del Delito y Justicia Penal (Naciones Unidas)
CEI	Comunidad de Estados Independientes
Celac	Comunidad de Estados Latinoamericanos y Caribeños
Cicte	Comité Interamericano contra el Terrorismo
CIDH	Comisión Interamericana de Derechos Humanos
Citel	Comisión Interamericana de Telecomunicaciones
CMSI	Cumbre Mundial sobre la Sociedad de la Información
CND	Comisión de Estupefacientes (Naciones Unidas)
ECOWAS	Economic Community of West African State (Comunidad de Estados de África Occidental)
FGI	Foro de la Gobernanza de Internet (IGF: Internet Governance Forum)
GEG	Grupos de Expertos Gubernamentales
GTCA	Grupo de Trabajo de Composición Abierta (OEWG: Open-Ended Working Group)
IA	inteligencia artificial
IEP	Institute for Economics & Peace
Mercosur	Mercado Común del Sur
OAD	Oficina de Asuntos de Desarme (Naciones Unidas)
OEA	Organización de los Estados Americanos
OESCE	Organización para la Seguridad y la Cooperación en Europa
OTAN	Organización del Tratado del Atlántico Norte
Remja	Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas
Sica	Sistema de Integración Centroamericana
TIC	tecnologías de la información y las comunicaciones
UA	Unión Africana
UIT	Unión Internacional de Telecomunicaciones
Unasur	Unión de Naciones Suramericanas

ACERCA DEL AUTOR

Marcos Robledo Hoecker. Profesor de la Facultad de Gobierno de la Universidad de Chile y asesor de la Red latinoamericana de Seguridad Incluyente y Sostenible de la FES. Periodista, Master of Arts in National Security Affairs, Naval Postgraduate School California. Exasesor de Política Exterior y Defensa de la presidenta Michelle Bachelet (2006-2010) y exsubsecretario de Defensa (2014-2018).

PIE DE IMPRENTA

Friedrich-Ebert-Stiftung (FES)
Calle 71 nº 11-90 | Bogotá-Colombia

Responsable
Oliver Dalichau
Representante de la FES Colombia

Catalina Niño
Coordinadora de proyectos
catalina.nino@fes.de

Bogotá, octubre de 2023

SOBRE ESTE PROYECTO

Este documento es un producto del proyecto de la Friedrich-Ebert-Stiftung (FES), Red Latinoamericana de Seguridad Incluyente y Sostenible, formada por expertos y expertas internacionales provenientes de los ámbitos de la política, la academia, la diplomacia, el sector de seguridad y las organizaciones de sociedad civil. La Red se creó como un espacio permanente de discusión sobre los desafíos a la paz y la seguridad que enfrenta América Latina y sus impactos sobre la democracia en la región.

Para más información, consulte

https://colombia.fes.de

Desde una perspectiva comparada, América Latina tiene un gran rezago en materia de gobernanza de la ciberseguridad. A diferencia de otras regiones del Sur global que tuvieron procesos de industrialización y son actores de la cuarta revolución industrial, América Latina sigue siendo esencialmente extractivista y exportadora de materias primas.

A pesar de tener una gobernanza robusta de seguridad regional y ser denominada "zona de paz", no tiene una identidad regional cooperativa similar sobre ciberseguridad, ni global ni regional, aunque en el último caso se observan pasos en esa dirección.

En ciertos aspectos del debate, algunos Estados se han alineado en torno a los bloques dirigidos por Estados Unidos, Rusia o China, mientras que en otros han optado por organizarse en grupos de países afines provenientes de distintas regiones. La fragmentación se observa también en la posición en el debate sobre la gobernanza de la ciberseguridad en el ámbito criminal.

El análisis del regionalismo latinoamericano sobre ciberseguridad muestra las debilidades de la inserción de la región en la cuarta revolución industrial y su desarrollo desigual de capacidades digitales y de ciberseguridad. Pocos países han explicitado sus políticas de ciberseguridad y muchos menos de ciberdefensa.

El principal régimen emergente sobre ciberseguridad en el ámbito interamericano desarrollado hasta 2023 privilegia una cooperación limitada, aunque creciente, en materia judicial y criminal, de fortalecimiento de capacidades y de transparencia.

Además, existe un creciente desarrollo de regímenes subregionales (Sica, Caricom, Mercosur o la Alianza del Pacífico). En todos los casos se trata, sin embargo, de normas no vinculantes.

Como en otros ámbitos de la política internacional, América Latina está enfrentando la configuración de la nueva gobernanza internacional sobre ciberseguridad de manera fragmentada, vulnerable a la captura geopolítica de las potencias que disputan la hegemonía internacional y ausente como actor global.