ARI 38/2023
9 de mayo de 2023

Ciberdiplomacia en América Latina: niveles, enfoques y velocidades

Jorge M. Vega | Doctor en Seguridad Internacional.

Tema

El multilateralismo cibernético latinoamericano replica el complejo entramado de mecanismos superpuestos y ritmos dispares propios de la integración política en esta parte del mundo, por lo que la respuesta diplomática regional a los desafíos de la ciberseguridad no es única ni uniforme, conviviendo distintos niveles, enfoques y velocidades.

Resumen

La cooperación internacional sobre asuntos cibernéticos tiene larga data en América Latina, siendo una región pionera en la conformación de instancias multilaterales de concertación de políticas en la temática. También es una zona prolífica en el desarrollo de arquitecturas subregionales de cooperación sobre el ciberespacio que funcionan enmarcadas en los regímenes de integración existentes. Tales atributos configuran un ecosistema cibernético signado por la variedad de iniciativas vigentes y la dinámica multinivel de los acuerdos.

Este análisis procura caracterizar el estado de la cooperación cibernética regional atendiendo a dichos factores. En esta línea, plantea una descripción de las principales acciones colectivas impulsadas en los ámbitos regional –sobre todo, en el plano hemisférico– y subregional (Sudamérica y Centroamérica), abordaje que se complementa posteriormente con una semblanza comparada sobre las capacidades estatales desarrolladas a nivel nacional para generar respuestas diplomáticas conjuntas en materia de ciberseguridad.

Sus resultados evidencian disparidades de velocidad y enfoque entre el entorno regional y el intrarregional. Además, indican diferencias de profundidad programática entre los regímenes subregionales. En el plano nacional, los hallazgos refieren a capacidades institucionales y normativas incipientes comparadas a nivel agregado con las de otras latitudes. En efecto, únicamente siete países se adhirieron al Convenio sobre la Ciberdelincuencia y sólo uno prestó colaboración a terceros para desarrollar tales capacidades en los últimos tres años.

Análisis

Se entiende por ciberdiplomacia la cooperación internacional en el ámbito de los asuntos cibernéticos bajo una mirada amplia que abarca diversas perspectivas analíticas y temáticas de interés prioritario. En esta dirección, la diplomacia cibernética comprende tanto el abordaje securitario de la problemática –cooperación en el ámbito de la

ciberseguridad– como las iniciativas interestatales asociadas a la incorporación colaborativa de las tecnologías de la información y la comunicación en la economía –cooperación técnica digital–.

La cooperación internacional es una dimensión prioritaria de la agenda de ciberseguridad, derivada de la naturaleza intrínsecamente transnacional de los riesgos y amenazas que emanan del ciberespacio. Tal es así que la política de ciberseguridad es entendida, por definición, como una responsabilidad global compartida que impone soluciones comunes. En conjunto con las capacidades estatales domésticas del sector y la colaboración entre el ámbito público y el privado, conforman la tríada de requisitos mínimos para su buena gobernanza.

En América Latina la cooperación cibernética internacional comprende sendas perspectivas y se caracteriza por ser multilateral y multinivel. Multilateral, porque la mayor densidad de esfuerzos colectivos en la materia se localiza en foros regionales preexistentes con diverso –y solapado– alcance geográfico. Multinivel, porque conviven iniciativas entrelazadas de nivel panregional (que incluyen a América del Norte), con pronunciamientos regionales unificados América Latina-Caribe y con programas subregionales (sobre todo en Sudamérica y Centroamérica).

En el plano regional, el foco de atención del análisis está puesto en el accionar de la Organización de Estados Americanos (OEA) por la densidad de las iniciativas programáticas desplegadas en la materia desde hace un cuarto de siglo. También incluye una mención sobre la posición de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC). Por su parte, en el ámbito subregional, se abordan las intervenciones del Mercado Común del Sur (Mercosur), de la Alianza del Pacífico y del Sistema de la Integración Centroamericana (SICA).

El tercer nivel de análisis corresponde al plano nacional, es decir, a las capacidades estatales sobre ciberseguridad. Para ello se consideran dos dimensiones de interés: (1) las aptitudes locales sobre cooperación internacional en la temática según las entiende la e-Governance Academy (eGA) en el Índice Nacional de Ciberseguridad (INCS); y (2) el aporte de cada país para mejorar el contexto global de ciberseguridad, de acuerdo con la conceptualización empleada por la Unión Internacional de Comunicaciones (UIT) en el Índice de Ciberseguridad Global (ICG).

Vanguardia hemisférica

Una simple búsqueda sobre la institucionalidad latinoamericana en ciberseguridad pone de manifiesto el papel preponderante de la OEA en el diseño de iniciativas diplomáticas contribuyentes. De hecho, el carácter pionero de la región en el abordaje colectivo de la ciberseguridad es producto de las intervenciones de la OEA, la cual a fines del siglo XX ya contaba, por ejemplo, con un Grupo de Trabajo en Delitos Informáticos en el marco de la Reunión de Ministros de Justicia y Fiscales Generales de las Américas (REMJA).

Esta presencia de la OEA contrasta en el plano regional con el posicionamiento de la CELAC, régimen que abarca a todos los países de América Latina y el Caribe. En sólo tres de sus siete cumbres presidenciales se hizo referencia a aspectos vinculados a la

ciberseguridad: las declaraciones de 2015 y 2016 condenan "toda forma de delincuencia cibernética" y la de 2022 incluye una mención más amplia, destacando la cooperación "en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos". La piedra angular del andamiaje cooperativo panamericano centrado en la OEA es la "Estrategia de Seguridad Cibernética" de 2004,[1] cuyo desarrollo y aplicación descansa de forma conjunta en el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y la REMJA. Se destaca su enfoque multidimensional y pluridisciplinar, así como su temprana ponderación de la cooperación regional, el desarrollo de las capacidades nacionales y la necesidad de la colaboración público-privada.

A pesar del papel coordinador de la Comisión de Seguridad Hemisférica y el papel concurrente del CICTE, la CITEL y la REMJA en la implementación de la estrategia, ha sido desde entonces el CICTE el principal brazo ejecutor de la OEA en materia de ciberseguridad. Si bien ello responde en parte a la emergencia del ciberterrorismo como amenaza regional, las razones de tal preponderancia quizá se relacionen también con la importancia institucional (y global) del terrorismo al momento de gestarse la estrategia y con cuestiones de organización interna de la OEA.

El accionar sectorial del CICTE se estructura en torno al "Programa de Seguridad Cibernética", concebido principalmente para ayudar a los Estados miembros a desarrollar capacidades técnicas y formular políticas públicas. En este sentido, entre otras iniciativas, realiza actividades de investigación y divulgación, contribuye con el diseño de estrategias nacionales de ciberseguridad y el establecimiento de equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés).

Sobre este último punto cabe destacar la labor de "CSIRTAmericas", la red de CSIRT gubernamentales de los Estados miembros de la OEA, lanzada en 2016 para impulsar el "Programa de Seguridad Cibernética" del CICTE a través del intercambio de información sobre alertas de ciberseguridad, la capacitación a sus especialistas y la asistencia técnica gubernamental para fortalecer los servicios de los CSIRT (por ejemplo, mediante las buenas prácticas para establecer un CSIRT Nacional).[2]

Las mencionadas intervenciones del CICTE se complementan con diversos pronunciamientos generales de orden político-institucional como, por ejemplo, la Declaración sobre el "Fortalecimiento de la Seguridad Cibernética en las Américas" de 2012,[3] la Declaración sobre "Protección de Infraestructura Crítica ante las Amenazas Emergentes" de 2015[4] y con la creación de instancias técnicas de trabajo colaborativo,

[1] AG/RES. 2004 (XXXIV-O/04), "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética" (30, https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp).

[2] Actualmente la red está conformada por 36 CSIRT de 21 países, incluyendo Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Guyana, México, Panamá, Paraguay, Perú, Surinam y Uruguay. Véase https://csirtamericas.org/es.

[3] Declaración CICTE/DEC.1/12 rev. 1.

[4] Declaración CICTE/doc.1/15.

como es el caso del grupo de trabajo sobre "Medidas de Fomento de Cooperación y Confianza en el Ciberespacio Confianza" de 2017.[5]

Párrafo aparte merece la creación conjunta entre la OEA y el Banco Interamericano de Desarrollo (BID) del Observatorio de la Ciberseguridad en América Latina y el Caribe. Esta iniciativa, sustentada metodológicamente en el "Modelo de Madurez de la Capacidad de Ciberseguridad" (MMCC), permite monitorizar el avance de todos los países de la región sobre ciberseguridad en diversas dimensiones de interés,[6] parametrizando los resultados en términos de niveles de madurez: inicial, formativa, consolidada, estratégica y dinámica.

La medición del MMCC se realizó sólo en dos cortes temporales (2016 y 2020). Sus parámetros de monitorización se refieren, por ejemplo, al desarrollo, organización y contenido de una estrategia nacional de seguridad cibernética, a la mentalidad de seguridad cibernética en el gobierno, el sector privado y los usuarios, al marco para la formación (provisión y administración), al sistema de justicia penal (fuerzas del orden, enjuiciamiento y tribunales), y al cumplimiento de estándares de seguridad de las tecnologías de información y comunicaciones (TIC) en las adquisiciones y el desarrollo de *software*.

Ciberdiplomacia subregional

Los principales regímenes subregionales de integración desarrollaron en el último tiempo plataformas específicas de trabajo sobre el ciberespacio, cuyo común denominador es el abordaje del problema en tanto dimensión de la Agenda Digital institucional. Ello deviene de un enfoque económico-privado del asunto, centrado en la aplicación de las TIC y la transformación digital para la mejora de la gestión pública y empresarial. Tal es el caso del Mercosur y de la Alianza del Pacífico en Sudamérica y de la SICA en Centroamérica.

Este enfoque de la ciberdiplomacia contrasta con la perspectiva securitaria característica de la OEA y responde a la naturaleza económico-comercial de sendas instituciones subregionales. A partir de ello, la idea de ciberseguridad en los mencionados regímenes subregionales presenta una connotación distinta a la empleada en el plano hemisférico, alejándose de su asociación con la alta política y la ciberdelincuencia para referirse como "seguridad digital" a aspectos técnicos propios de la integración económica de cara a la creación de un mercado digital multilateral.

En efecto, la ciberseguridad en el Mercosur es competencia del Grupo Agenda Digital (GAD), instancia creada en el marco del Grupo Mercado Común a fines de 2017 para promover el desarrollo de un Mercosur Digital. En las propias palabras de la institución, hasta el establecimiento del GAD el Mercosur "no contaba con una agenda que coordinase los temas relativos a la economía digital", por lo que la seguridad cibernética

[5] Resolución CICTE/RES.1/17.

[6] Política y estrategia; cultura cibernética y sociedad; formación, capacitación y habilidades; marcos legales y regulatorios; estándares, organizaciones y tecnologías.

–entre otros "tópicos sueltos"– era conducida por "foros independientes y sin una coordinación entre sí".[7]

Los planes de acción bianuales del GAD incorporan, en sintonía, a la "seguridad y confianza en el entorno digital" como eje de trabajo, contemplando iniciativas como el diagnóstico e intercambio de información sobre ciberseguridad entre los países del bloque (Plan 2021-2023). Es menester mencionar que en la LXI Cumbre de Jefes de Estado del Mercosur y Estados Asociados (diciembre de 2022) se destacaron los avances logrados sobre ciberseguridad, con miras a la firma de un próximo "Memorando de Entendimiento sobre Ciberseguridad".

La Alianza del Pacífico también cuenta con un Grupo de Agenda Digital (GAD), creado en 2017, entre cuyas atribuciones figura potenciar la cooperación sobre seguridad digital.[8] La misión del GAD es implementar la "Hoja de Ruta del Mercado Digital Regional", cuyo eje programático –ecosistema digital– contiene un apartado específico sobre seguridad digital que presenta, entre otros objetivos, promover la seguridad de la información de los consumidores, la cooperación entre los CSIRT y la adhesión al Convenio sobre Delitos Cibernéticos o Convenio de Budapest.

Centroamérica dispone de una Estrategia Regional Digital (ERDI) elaborada por la SICA en 2015, en cuyo contexto se elaboró la "Agenda Regional Digital 2022-2025" como mecanismo para promover su implementación. Entre las áreas de acción de la agenda hay una denominada "Seguridad Digital", que presenta como objetivo estratégico fortalecer el marco jurídico regional, la ciberseguridad y la protección de activos de información de la población, y la coordinación regional para prevenir y responder a incidentes cibernéticos.

Esta Agenda se especifica a su vez en planes de acción bianuales. En el correspondiente a 2022-2023, el área de Seguridad Digital enumera las siguientes acciones en ejecución: "la creación y puesta en funcionamiento del equipo de respuesta ante incidentes de seguridad informática regional" (CSIRTs-SICA); el desarrollo de una guía regional de ciberseguridad; la realización de un encuentro regional de ciberseguridad; la formulación de una estrategia regional de seguridad digital; y la creación de un centro regional de ciberseguridad.[9]

Capacidades estatales

Siguiendo a la UIT, se entiende a la cooperación internacional como una "esfera prioritaria" en la elaboración de toda estrategia nacional de ciberseguridad. Ello en virtud de reconocer la importancia de la ciberseguridad como una prioridad de la política exterior y, por ende, de las respectivas capacidades estatales como herramienta para fomentar el desarrollo y la utilización de competencias y aptitudes sobre asuntos

[7] Agenda Digital de Mercosur, https://www.mercosur.int/temas/agenda-digital/.

[8] Alianza del Pacífico, Grupo Técnico de Agenda Digital, https://alianzapacifico.net/grupotecnico-agenda-digital/.

[9] Estrategia Regional Digital del SICA – ERDI, https://www.sica.int/erdi/proyectos?search=AA05.

cibernéticos (ciberdiplomacia) *que complementen* los métodos y procesos tradicionales de la diplomacia.[10]

En consecuencia, uno de los pilares del Índice de Ciberseguridad Global (ICG) de la UIT –denominado justamente "cooperación internacional"– mide las capacidades estatales en la materia considerando como datos de interés la firma de acuerdos bilaterales o multilaterales y la participación en actividades internacionales. Este pilar también contempla la participación estatal en asociaciones público-privadas, aunque estas pueden no ser internacionales, por lo que su tratamiento específico se reserva para un futuro análisis complementario.

Los resultados del ICG en 2020 evidencian que, en los tres aspectos mencionados, las Américas ocupan el cuarto lugar global, posicionándose como región sólo delante de los Estados Árabes y de la Comunidad de Estados Independientes (CEI).[11] En el plano nacional, ningún país de América Latina tiene en este pilar su mejor *performance*, siendo por lo general el segundo o tercero en puntuación (sobre un total de cinco). Brasil y México presentan las mejores calificaciones de la región en la materia, siendo nula en Belice, Ecuador, Guatemala, Honduras y Venezuela.

El mencionado Índice Nacional de Ciberseguridad (INCS) de la eGA aporta un enfoque complementario sobre tales capacidades estatales. Su foco está puesto en la contribución de cada país para mejorar el entorno global de ciberseguridad a nivel internacional, dimensión que operacionaliza a través de un conjunto de indicadores: ratificación del Convenio sobre la Ciberdelincuencia; representación en regímenes de cooperación internacional; ser sede de una organización dedicada a la ciberseguridad; y creación de capacidades sobre ciberseguridad para terceros Estados.

El desempeño de la región en esta dimensión es magro, porque prácticamente la totalidad de los países obtiene uno o dos puntos sobre seis posibles.[12] Sólo siete países ratificaron el Convenio sobre la Ciberdelincuencia, [13] ninguno es sede de una organización regional o internacional dedicada a la ciberseguridad y únicamente Ecuador apoyó el desarrollo de capacidades de otro Estado en los últimos tres años. No obstante, salvo los dos casos de Nicaragua y El Salvador, todos participan en al menos un régimen de cooperación sobre ciberseguridad.

[10] UIT, Banco Mundial, Secretaría de la *Commonwealth*, Organización de Telecomunicaciones de la *Commonwealth* y Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (2018), "Guía para la elaboración de una estrategia nacional de ciberseguridad", pp. 48-49.

[11] UIT (2021), "Índice Mundial de Ciberseguridad", pp. 20-22.

[12] NCSI, National Cyber Security Index, https://ncsi.ega.ee/compare/.

[13] Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay y Perú.

Conclusiones

En América Latina conviven dos enfoques sobre ciberdiplomacia asociados a los niveles preexistentes de integración. En el plano hemisférico, el abordaje se focaliza en la dimensión de seguridad de la problemática y presenta una arquitectura de cooperación enraizada y de desarrollo progresivo. Por su parte, en el campo subregional, su tratamiento es concebido desde un prisma económico y relativo al empleo de las TIC, en el marco de un entorno cooperativo novel, aunque dinámico y creciente, dada la prioridad del tema en la agenda institucional.

Ambos enfoques sobre ciberdiplomacia recurren a la noción de ciberseguridad, pero con una connotación y alcance programático disímiles. Mientras que en el plano regional el concepto se refiere sobre todo a los riesgos y amenazas propios de la ciberdelincuencia, cuya competencia atañe al sector de Seguridad y Defensa, en el ámbito subregional se emparenta con aspectos técnicos, normativos y tecnológicos relacionados con la protección de datos personales e información privada en el marco de la integración económica multilateral.

La cooperación latinoamericana sobre ciberseguridad replica las estructuras y dinámicas históricas de la integración regional en esta parte del mundo, por lo que a pesar de sus significativos y pioneros avances, dista de contar con la institucionalidad de otras latitudes como la europea, donde la UE dispone de una autoridad supranacional para emitir directivas que aproximen la legislación de los Estados miembros, tales como la Directiva NIS,[14] o reglamentos de ejecución vinculante para los anteriores, tales como el Reglamento por el que se crea la Agencia de Ciberseguridad de la UE (ENISA en sus siglas inglesas).[15] Ello responde no sólo al diseño y atribuciones de sendos regímenes de integración sino también a sus objetivos de medio y largo plazo.

El nivel nacional conjuga ambos enfoques sobre ciberseguridad en el contexto de un mapa del Estado en construcción. En lo que específicamente respecta a las capacidades estatales para la cooperación internacional en la materia, las fuentes indican que los países de América Latina presentan una baja puntuación comparados con sus pares de otras regiones. Sin embargo, corresponde destacar como activo su extendida presencia en los principales regímenes internacionales multilaterales de alcance global sobre ciberseguridad.

[14] "Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo sobre las medidas para elevar el nivel común de ciberseguridad", 14/XII/2022.

[15] "Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo", 17/IV/2019, https://www.enisa.europa.eu/about-enisa/about/es.