Brújula. Semilleros de Investigación
Volumen 10, Número 20, julio-diciembre, 2022. pp. 7-16
Bogotá D. C., Colombia
ISSN 2346-0628 (en línea)
https://doi.org/10.21830/23460628.118

DOSIER

Políticas públicas de ciberdefensa en Chile y Colombia: un análisis desde el rastreo de procesos

Hackzel Mauricio Montenegro Moreno
Maverick Johannes Pantoja Rosero
Angie Yurani Rojas Larrotta
Ricardo García Briceño
Escuela Militar de Cadetes "General José María Córdova"

RESUMEN

Este artículo tiene como finalidad organizar los eventos que confluyeron en el diseño de la política pública de ciberdefensa de Colombia y Chile con el propósito de comprender el proceso de institucionalización y los elementos presentes en la formulación de estas políticas. Para alcanzar este objetivo se parte del institucionalismo internacional para el diseño de política. Por medio del método de rastreo de procesos se procede a observar los eventos que acompañaron la formulación de las políticas de ciberdefensa en ambos Estados. Se concluye que la institucionalización de estas políticas se suscribió a una construcción impulsada desde actores internacionales regionales y adoptada por los Estados, así como por ser países altamente atacados por ciberataques.

PALABRAS CLAVE

Chile, ciberdefensa, Colombia, defensa, políticas públicas, regímenes internacionales, seguridad internacional.

CITACIÓN

Montenegro, H., Pantoja, M., Rojas, A., & García, R. (2022). Políticas públicas de ciberdefensa en Chile y Colombia: un análisis desde el rastreo de procesos. *Revista Brújula de Investigación, 10*(20), 7-16.
https://doi.org/10.21830/23460628.118

Recibido: 15 de marzo de 2022
Aceptado: 6 de junio de 2022
Contacto: Ricardo García Briceño ricardo.garcia@esmic.edu.co

Introducción

Este artículo de investigación tiene como finalidad organizar los eventos que confluyeron en el diseño de la política pública de ciberdefensa de Colombia y Chile con el propósito de comprender el proceso de institucionalización y los elementos presentes en la formulación de estas. A continuación, se presenta de forma general el contexto de la ciberseguridad y la ciberdefensa en América Latina y el Caribe (ALC).

En el siglo XX, a nivel global, la revolución tecnológica generó un nuevo espacio denominado *ciberespacio*. Este surge por el uso de la "electrónica y el espectro electromagnético para crear, modificar, guardar, intercambiar y explotar información mediante de sistemas de interconexión e internet, y sus infraestructuras asociadas, incluyendo medios de transmisión como la radio, la televisión y dispositivos como tabletas y celulares" (Piñeros *et al*., 2019, p. 510). Este espacio se ha constituido en un importante escenario de interacciones informáticas, comunicativas, comerciales, sociales y militares, las cuales, con el paso del tiempo, se han incrementado en su número y nivel de importancia, lo que también ha implicado el aumento de sus riesgos y vulnerabilidades, implicando, con ello, nuevos desafíos y amenazas para la seguridad y la defensa de los Estados y sus sociedades, tales como el ciberterrorismo, los ciberataques a la infraestructura digital y financiera, y en general, el cibercrimen (Horowitz, 2020).

Este incremento de amenazas en el ciberespacio durante los últimos años cuestiona directamente las capacidades en seguridad y defensa de los Estados. Según Fortinet[1], solamente entre el 2020 y 2021 ha habido un incremento del 600% en las amenazas y ataques en ALC. Durante el 2021, ALC sufrió más de "289 mil millones de intentos de ciberataques […] México fue el país que más intentos de ataques recibió (156 mil millones), seguido de Brasil (88,5 mil millones), Perú (11,5 mil millones) y Colombia (11,2 mil millones)" (Fortinet, 2021). Este tipo de amenazas demand**ó** plantear una respuesta por parte de los Estados mediante la institucionalización de aparatos normativos y de políticas públicas que brindaran las herramientas necesarias para atender esta problemática.

La llegada del siglo XXI dio paso a la formulación de diversas políticas enfocadas en la ciberseguridad y la ciberdefensa de los Estados, que apuntaban a responder desde estas a las amenazas señaladas. En este contexto, se identificó que en el escenario regional Colombia fue el primer Estado en institucionalizar desde una política pública su estrategia nacional de ciberdefensa (Hernández, 2018). Esta fue aprobada bajo el Documento Conpes[2] 3701 denominado "Lineamientos de política para ciberseguridad y ciberdefensa" publicado el 14 de julio del 2011 bajo el Gobierno del presidente Santos (DNP, 2011). En el caso de Chile, la formulación de la política de ciberdefensa se suscribe al Gobierno de la presidente Michel Bachelet, el 9 de noviembre del 2017, en el marco del cumplimiento de uno de los objetivos estratégicos de la política de ciberseguridad formulada en abril del mismo año (Horzella, 2021). En consecuencia, a continuación, se brindará un marco de referencia desde el institucionalismo internacional para analizar este proceso de formulación de políticas para la ciberdefensa de Chile y Colombia.

1 Fortinet (NASDAQ: FTNT) es el proveedor mundial de dispositivos de seguridad de red y líder en gestión unificada de amenazas (UTM).

2 Consejo Nacional de Política Económica y Social.

Marco teórico

El estudio de las políticas públicas como disciplina es un ejercicio reciente que se remonta a la década de los cincuenta desde lo propuesto por Harold Laswell como el estudio secuencial de las políticas públicas (DeLeón, 1997). Desde allí, esta disciplina ha realizado una gran contribución en la comprensión del Estado, de su acción gubernamental y de las relaciones entre los actores sociales-estatales partícipes del proceso (De la Hoz, 2016). En ese orden de ideas, en primer lugar, es importante comprender las "políticas públicas" como la acción del Estado (Oszlak y O'Donnell, 1981); en segundo lugar, entender que esta definición abarca bajo un mismo término tanto "la producción normativa de las instituciones públicas (planes, leyes, decretos, resoluciones, ordenanzas, acuerdos, fallos jurídicos, etc.) como las actividades políticas y administrativas realizadas tanto por actores políticos y sociales como por autoridades públicas" (Roth, 2010, p. 42). Finalmente, la formulación de una política pública se suscribe a un proceso complejo, razón por la cual, cuando se observan los eventos que anteceden su formulación es posible ampliar la comprensión de esta.

En este sentido, la acción de los Estados puede tener impacto en el diseño de sus políticas públicas o domésticas por parte de actores internacionales, tales como Estados, organizaciones internacionales gubernamentales, no gubernamentales (ONG), organismos regionales, entre otros. De la dinámica relacional de estos actores surgen diversos modelos de interdependencia, cooperación, multilateralismo y gobernanza ejecutados en el marco del sistema internacional (Keohane y Nye, 1977; Keohane, 1984), desde los cuales surgen instituciones o regímenes, entendidos, según Krasner (1983), como

> los principios, normas, reglas y procedimientos de toma de decisiones, explícitos o implícitos, en torno a los cuales convergen las expectativas en un área temática concreta de las relaciones internacionales. Los principios son creencias de hecho, causación y rectitud. Las normas son estándares de comportamiento definidos en términos de derechos y obligaciones. Las reglas son prescripciones o proscripciones específicas para la acción. Los procedimientos de toma de decisión son las prácticas prevalecientes para la realización y la implementación de las elecciones colectivas[3]. (p. 2)

En este orden de ideas, la comprensión y el análisis de los regímenes y de las instituciones se adelanta desde el institucionalismo internacional (Hasenclever *et al.*, 1997), implicando con ello el estudio del "papel de la estructura para explicar el comportamiento de los Estados en el sistema internacional y observa los regímenes como instituciones del nivel internacional" (De la Hoz, 2016, p. 117). De lo anterior se desprende la importancia de observar para efectuar el proceso de análisis de las políticas públicas a los actores dentro del sistema internacional y cómo desde estos se promueven o impactan en la formación de estas (Hasenclever *et al*., 1997; Krasner, 1984).

El estudio de los regímenes desde el institucionalismo internacional implica entonces comprender cómo se forman y su impacto en los actores adscritos a estos. A su vez, implica entender cómo las normas, procedimientos y reglas sirven de instrumento de cohesión entre los Estados vinculados a la institución que las promueve (Krasner, 1983). En tercer lugar, el estudio de las instituciones u organismos internacionales demanda validar si los regímenes promueven normas legítimas. Para ello, estos "validan y estabilizan el mejor pensamiento disponible, especialmente aquel conocimiento

3 Traducción propia del inglés al español.

que es coherente con los modelos de políticas y economía del actor racional" (Sogge, 2009, p. 12), es decir, los actores deben percibir que estas normas son válidas e identificadas a favor de cada uno de estos planteando objetivos comunes o brindando solución a los desafíos o necesidades de cada actor. Por lo tanto, los Estados adoptan los principios, normas, reglas y procedimientos propios de los regímenes internacionales implementando estos en sus políticas públicas. En consecuencia, los regímenes se construyen sobre mecanismos multilaterales de cooperación desde los cuales se propende por alcanzar objetivos colectivos que se desarrollan sobre los intereses de cada Estado, lo que estimula los vínculos de colaboración y coadyuva entre Estados.

Después de este breve planteamiento teórico se tomará lo referente al impacto o influencia de los organismos internacionales y de sus regímenes en el diseño de la política pública de los Estados y su validación, continuidad y permanencia.

Métodos

Para alcanzar el objetivo trazado en este artículo de investigación se empleó el rastreo de procesos como método de concatenación (Waldner, 2012) aplicado en el marco del estudio de caso comparado suscrito a este trabajo[4]. Se entiende por rastreo de procesos a un modo de inferencia causal al cual se llega al enlazar varios eventos que forman una cadena causal. El "process tracing" o rastreo de procesos es el análisis de una serie de factores particulares dentro de una secuencia Bennett y Checkel (2015). En este caso, al observar la formulación de las políticas públicas como producto es importante fijarse en la serie de acontecimientos que las antecedieron o los hechos históricos que les permitieron a unos actores tomar ciertas medidas para enfrentar o adaptarse a estos.

Dicho esto, el análisis se realiza con la intención de formular hipótesis respecto de las causas que dan origen al caso (Yin, 2015). Para ello, este proceso cuenta con dos componentes fundamentales: 1) el componente inductivo por medio del cual se desarrollan las hipótesis, y 2) el componente deductivo a través del cual se evalúan las hipótesis. De esta forma, en este artículo se organizaron los acontecimientos principales que impactaron la formulación de la política de ciberdefensa en Chile y Colombia. Se consultaron fuentes oficiales de ambos Estados (fuentes primarias) y artículos académicos y de prensa (fuentes secundarias).

Resultados

En este apartado se presentan los resultados y hallazgos encontrados en el rastreo de procesos aplicado al caso de estudio. Los eventos observados se exponen en el siguiente orden: incidencia de actores internacionales y regionales y formulación de las políticas propuestas en ambos Estados.

Incidencia de actores internacionales a la formación de la política de ciberdefensa

En primera instancia, el proceso del diseño y formulación de las políticas públicas en ciberdefensa en Colombia y Chile (y a nivel regional) se ha suscrito a la adhesión de los actores estatales a regímenes internacionales de orden regional y mundial. Particularmente, se reconocen tres momentos centrales, los cuales han contribuido al desarrollo de dichas políticas: 1) El convenio de Budapest celebrado en noviembre

4 Este artículo se suscribe al resultado del primer objetivo del proyecto de investigación señalado.

del 2001, el cual entró en vigor el 1.º de julio del 2004; 2) la Estrategia Interamericana Integral de Seguridad Cibernética propuesta en junio del 2004 por la Organización de Estados Americanos (OEA), y 3) la estrategia de ciberdefensa para la Unión Europea en el 2008.

Para el caso de las Américas, la OEA ha desempeñado un papel de liderazgo central y preferente en el direccionamiento regional para el establecimiento de marcos normativos (ciberlegislaciones) que apuntan a tratar el problema de la ciberseguridad y la ciberdefensa. Este organismo regional tiene su origen en el contexto de la Guerra Fría, desde el cual se construye el Tratado Interamericano de Asistencia Recíproca (TIAR) y se conforma la Junta Interamericana de Defensa (JID), la cual tendrá un papel importante en la formulación de lineamientos para la ciberdefensa a nivel regional. En el contexto de los atentados terroristas ocurridos en Nueva York el 11 de septiembre del 2001, desde la OEA se produce la Declaración de Bridgetown (2002), instrumento que plantea la implementación a nivel regional del concepto del "Enfoque multidimensional de la seguridad hemisférica" (Resolución OEA, AG/DEC. 27; XXXII-O/02). A su vez, desde este mismo organismo se crea el Comité Interamericano contra el Terrorismo (CICTE) con el objetivo de aunar esfuerzos entre la sociedad civil, el sector gobierno y privado para identificar las necesidades en materia.

Ya en el 2004, la OEA formula la Estrategia Integral para Combatir las Amenazas a la Seguridad Cibernética: desde la cual se estipulan tres líneas de acción: 1) la creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores (CSIRT16), 2) la identificación y adopción de normas técnicas para una arquitectura segura de internet, y 3) la adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios (Resolución OEA, AG/RES 2004, XXXIV-O/04). Esta estrategia de este organismo regional fue innovadora en su momento y anterior a lo propuesto por la Unión Europea en el 2008.

A lo largo del siglo XXI, la OEA con la participación del Banco Interamericano de Desarrollo (BID) han promovido el fortalecimiento de los mecanismos de cooperación en el área de ciberdefensa en la región. En el 2006 se suma a la OEA la Junta Interamericana de Defensa, organismo con más de 60 años al servicio del sector defensa. Desde esta institución, en el 2020 se promovió la "Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar", financiada y publicada por el Gobierno de Canadá (Junta Interamericana de Defensa, 2020). Aunado a este esfuerzo, la OEA, en el 2019, lanza la primer Conferencia en Ciberdefensa con la participación de 25 Estados y de 170 participantes de alto nivel. En el 2020, esta conferencia tuvo una segunda edición desde la cual se presenta la guía citada. De este modo, como es señalado por Navarro

> La participación de la gran mayoría de los países de América Latina en la Cumbre Mundial de la Sociedad de la Información, así como en los Planes eLAC2007, eLAC2010 y eLAC2015, ha influido de manera decisiva en el desarrollo de instrumentos nacionales armonizados para la ciberlegislación conforme al contexto regional. (Navarro, 2011, p. 1)

En el caso de Colombia, como se señal**ó**, en el 2011 fue el primer Estado en América Latina y el Caribe en plasmar una estrategia de ciberdefensa para la nación desde una política pública; en el caso de Chile, para el 2017 plante**ó** su estrategia, que será analizadas a continuación.

Políticas formuladas en Chile y Colombia

En el Gobierno del presidente Juan Manuel Santos (2010-2014) dio inicio en el 2011 a un segundo momento de transformación de las Fuerzas Militares, suscrito a un proceso de modernización más amplio extendido por el mandatario a todo el sector defensa. Desde su Gobierno se adelantó la formulación de diferentes documentos e instrumentos de política que, a su vez, han dado al inicio de nuevas instituciones sobre ciberdefensa; principalmente, en su mandato se implementó el Documento Conpes 3701 desde el cual se planteó el siguiente objetivo "Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio" (Departamento Nacional de Planeación, 2011, p. 20).

A su vez, este documento autoriza la creación de una Comisión Intersectorial para fijar una visión estratégica para la ciberseguridad y la ciberdefensa, así como del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), el cual prestará apoyo a los otros comandos: "al Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC)" (DNP, 2011, p. 22). Este documento reconoció un referente normativo para la formulación de esta política a la Resolución AG/RES 2004 (XXXIV- O/04) de la OEA, el Convenio de Budapest del Consejo de Europa y la Resolución 64/25 del Sistema de Naciones Unidas.

En el caso de Chile, la política de ciberdefensa se enmarca en su política de ciberseguridad presentada en el 2017. Durante el mismo año, el 9 de noviembre fue aprobada la "Política de ciberdefensa", la cual tiene el objetivo de

> resguardar la seguridad de las personas y de sus derechos en el ciberespacio y plantea además cinco objetivos estratégicos de largo plazo, destinados a abordar los múltiples desafíos que enfrenta nuestro país, y un conjunto de medidas de política pública que deben ser implementadas en el corto tiempo. (Diario Oficial de la República de Chile, 2017)

Frente al Convenio de Budapest, el Estado de Chile se adhirió en el 2017 a este a partir de la solicitud realizada al presidente de la república el 16 de noviembre del 2010 (Biblioteca del Congreso Nacional de Chile, s. f.), lo que signific**ó** un avance importante para combatir y enfrentar el crimen organizado y la ciberdelicuencia a partir de una legislación penal y procedimientos comunes en los Estados firmantes. En el caso de Colombia, su proceso de adhesión fue en el 2020 radicando ante el Consejo de Europa el instrumento vinculante a este convenio, del cual otros Estados en ALC ya forman parte: "Argentina (2018), Chile (2017), Costa Rica (2018), Panamá (2014), Paraguay (2018) y Perú (2019)" (Cancillería de Colombia, 2020).

Discusión

En este apartado se discutirán particularmente dos aspectos: 1) la comparación de las políticas y estrategias de ciberdefensa y ciberseguridad de Colombia y Chile, según el régimen internacional de la OEA y el BID, y 2) la importancia de la institucionalización regional de una política de ciberdefensa y, en ese sentido, la función de la OEA como actor regional.

En relación con el ejercicio comparativo, desde el Observatorio de la Ciberseguridad en ALC, la OEA y el BID han desarrollado desde cinco indicadores o categorías una propuesta de medición en el avance del desarrollo de capacidades institucionales estatales para este subsector. Estos son: 1) cultura cibernética y sociedad,

2) política y estrategia de seguridad cibernética, 3) formación, capacitación y habilidades de seguridad cibernética, 4) marcos legales y regulatorios y estándares, organizaciones y tecnologías (BID y OEA, 2020). En cuanto a la categoría 2, "Política y estrategia de seguridad cibernética", según el informe del 2020 "Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe", del Observatorio de la Ciberseguridad en ALC, Colombia presenta mayores avances respecto a la formación de políticas que apuntan a la ciberseguridad y ciberdefensa. Este observatorio mide en cinco niveles los avances de cada Estado según los indicadores allí plasmados: 1) inicial, 2) formativo, 3) establecido, 4) estratégico y 5) dinámico. Desde esta parametrización, se sitúa principalmente a Colombia ya en la consolidación de un nivel estratégico por encima del nivel "establecido" en el que preferentemente se encuentra Chile (ver la figura 1).

Ahora bien, en relación con el segundo aspecto propuesto para este apartado, pese a que a nivel regional ha existido un esfuerzo importante por parte de la OEA, el BID, las Naciones Unidas y otros actores estales, "de dotar con modelos o estrategias para afrontar las amenazas de ciberdefensa y ciberseguridad a los Estados" (Borbúa et al., 2017, p. 35), así como de brindar documentos, estándares y lineamientos para la formulación de políticas públicas sobre ciberdefensa, para el 2018 solo diez Estados de ALC contaban con políticas de seguridad acerca de ciberdefensa (Álvarez, 2018).

Siguiendo a Keohane *et al.* (1998), uno de los retos sobre ciberseguridad y ciberdefensa es

Figura 1. *Comparación política y estrategia de seguridad cibernética Chile-Colombia*
Fuente: Informe Observatorio de la Ciberseguridad en ALC (2020).

la seguridad del ciberespacio. No obstante, esto no constituye una necesidad individual, ni para los Estados ni para las empresas o la sociedad civil, sino antes bien, debido a las relaciones de interdependencia construidas desde internet y de las tecnologías de la información y la comunicación, es menester construir bloques regionales para garantizar la integridad y la protección de los derechos de sus connacionales y también para brindar garantías para el acceso seguro y protegido del ciberespacio. Por lo tanto, aunque existe un alto grado en la institucionalización de las políticas de ciberdefensa, tanto en Colombia como en Chile, sumado a otras acciones emprendidas sobre ciberseguridad por cuenta de ambos Estados, esta depende de una apropiación regional y complementaria entre todos los actores.

Conclusión

En este artículo se abordaron diferentes elementos relativos al desarrollo de las políticas de ciberdefensa en Colombia y Chile. En lo relativo al planteamiento teórico se observa la pertinencia del institucionalismo regional como marco interpretativo que brindó elementos pertinentes para desarrollar el análisis. Debido al método aplicado (rastreo de procesos), se pudo establecer una relación entre la OEA como organismo regional y su incidencia en la formulación de las políticas de ciberdefensa de Colombia y Chile. A su vez, se concluye que existe una trazabilidad entre los actores internacionales regionales y los Estados estudiados en el desarrollo de sus instrumentos normativos. Es decir, la institucionalización de las políticas de ciberdefensa en Colombia y Chile se suscribe a una construcción impulsada principalmente desde la región y adoptada por los Estados.

En este sentido, tanto la OEA como el BID han sido los actores más relevantes desde los cuales se formulan lineamientos y parámetros para la construcción de una política hemisférica enfocada hacia la ciberdefensa y la ciberseguridad. Desde estos organismos se han realizado esfuerzos en el marco de la cooperación y el multilateralismo para que los Estados en la región cuenten con los insumos e instrumentos necesarios a nivel local para abordar la dimensión de la seguridad en el ciberespacio y defender a sus connacionales y su infraestructura de cualquier amenaza que atente contra estos. Esto, a su vez, con el objeto de crear un bloque que sostenga una lucha frontal contra el ciberterrorismo, la ciberdelincuencia y en general, contra los ciberdelitos y el cibercrimen.

Por otra parte, pese a que a nivel regional ha existido un esfuerzo importante en la formulación de lineamientos en esta materia, persiste un avance asimétrico en el desarrollo de sus políticas. No obstante, tanto Colombia como Chile son países líderes en la región en estos asuntos, lo que ha impulsado que los avances sean mayores en comparación con otros países de la región.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. Los puntos de vista y los resultados de este artículo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Sobre el artículo

Este artículo forma parte del proyecto de investigación “Colombia y Chile: análisis comparado de sus capacidades militares en ciberde-

fensa" de la Escuela Militar de Cadetes "General José María Córdova".

Sobre los autores

Hackzel Mauricio Montenegro Moreno es cadete. Actualmente realiza el curso de oficiales del Ejército Nacional en la Escuela Militar de Cadetes "General José María Córdova" y en relaciones internacionales. Contacto: hackzel.montenegro@esmic.edu.co

Maverick Johannes Pantoja Rosero es cadete. Actualmente realiza el curso de oficiales del Ejército Nacional en la Escuela Militar de Cadetes "General José María Córdova" y en relaciones internacionales. Contacto: maverick.pantoja@escmic.edu.co

Angie Yurani Rojas Larrotta es cadete. Actualmente realiza el curso de oficiales del Ejército Nacional en la Escuela Militar de Cadetes "General José María Córdova" y en relaciones internacionales. Contacto: angie.rojas@esmic.edu.co

Ricardo García Briceño es doctorando en Estudios Políticos de la Universidad Externado de Colombia, magíster en Relaciones Internacionales de la Universidad Javeriana y licenciado en Ciencias Religiosas de la misma universidad. Contacto: ricardo.garcia@esmic.edu.co

Referencias

Álvarez Valenzuela, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista Chilena de Derecho y Tecnología*, *7*(1), 1-2. https://dx.doi.org/10.5354/0719-2584.2018.50416

Banco Interamericano de Desarrollo (BID), & Organización de Estados Americanos (OEA). (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte 2020. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bennett, A., & Checkel, J. (Eds.). (2015). *Process tracing in the social sciences. From metaphor to analytic tool*. Cambridge University Press.

Biblioteca del Congreso Nacional de Chile. (s. f.). Convenio 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest). https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest).pdf

Borbúa, R. V., Herrera, L. R., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 31-45.

Cancillería de Colombia. (2020, 17 de marzo). Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia. https://www.cancilleria.gov.co/colombia-adhiere-convenio-budapest-ciberdelincuencia

De la Hoz Reyes, R. (2016). Institucionalismo nuevo y el estudio de las políticas públicas. *Justicia*, (30), 107-121. https://doi.org/10.17081/just.21.30.1353

DeLeón, P. (1997). Una revisión del proceso de las políticas: de Lasswell a Sabatier. *Gestión y Política Pública*, *VI*(1), 5-17.

Departamento Nacional de Planeación (DNP). (2011, 14 de julio). Lineamientos de Política para la ciberseguridad y ciberdefensa (Documento Conpes 3701). DNP.

Diario Oficial de la República de Chile. (2017, 9 de noviembre). Ministerio de Defensa aprueba política de ciberdefensa. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Fortinet (2022). Global Threat Land Scape Report. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-q1-2022-threat-landscape.pdf

Hasenclever, A., Mayer, P., & Rittberger, V. (1997). *Theories of international regimes* (No. 55). Cambridge University Press.

Hernández, J. C. (2018). Estrategias nacionales de ciberseguridad en América Latina. *Análisis GESI*, (8), 1.

Horowitz, M. C. (2020). Do emerging military technologies matter for international politics? *Annual Review of Political Science*, *23*(1), 385.

Horzella, B. (2021). Política nacional de ciberdefensa. Biblioteca del Congreso Nacional de Chile; Asesoría Técnica Parlamentaria.

Junta Interamericana de Defensa. (2020). Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Gobierno de Canadá.

Keohane, R. (1984). *International institutions and state power, Boulder (etc.)*. Westview Press.

Keohane, R. O., & Nye, H. (Eds.). (1977). *Internationalization and domestic politics*. Cambridge University Press.

Keohane, R., Nye, J. R., & Joseph, S. (1998). *Poder e interdependencia en la era de la información*. Asuntos Exteriores.

Krasner, S. D. (Ed.). (1983). *International regimes*. Cornell University Press.

Navarro Isla, J. (2011). Ciberlegislación en América Latina. En *Newsletter eLAC2015*, 15. https://www.cepal.org/sites/default/files/publication/files/36921/elacnewsletter15_es.pdf

Observatorio de la Ciberseguridad en ALC. (2020). Observatorio de la Ciberseguridad. https://observatoriociberseguridad.org/#/home

Oszlak, O., & O'Donnell, G. A. (1981). Estado y políticas estatales en América Latina: hacia una estrategia de investigación. *Documento GE CLACSO, 4. Buenos Aires, CEDES*, 98-128.

Piñeros, D. V., Prieto, P., & Garzón, D. (2029). La ciberseguridad, la ciberdefensa, la identidad y los intereses nacionales y las Fuerzas Militares de Colombia. *Identidad*, 507.

Resolución OEA, AG/DEC. 27 (XXXII-O/02) Declaración de Bridgetown: Enfoque Multidimensional de la Seguridad Hemisférica

Resolución OEA, AG/RES 2004 (XXXIV- O/04) de la Asamblea General de la Organización de los Estados Americanos.

Roth, A. (2010). *Enfoques para el análisis de políticas públicas*. Universidad Nacional de Colombia.

Sogge, D. (2009). Sistema de ayuda extranjera: ¿Régimen o vehículo hegemónico? The Foreign Aid System: Regime or Hegemonic Vehicle? *Relaciones Internacionales*, (12).

Waldner, D. (2012). Process tracing and causal mechanisms. En H. Kincaid (ed.), *The Oxford Handbook of Philosophy of Social Science* (pp. 65-84). Oxford University Press.

Yin, R. K. (2015). *Case Studies. International Encyclopedia of the Social & Behavioral Sciences*, 2.ª ed., 3 (pp. 192-201). https://doi.org/https://doi.org/10.1016/B978-0-08-097086-8.10507-0