Estudios Internacionales 198 (2021)–ISSN 0719-3769 • 169–197
Instituto de Estudios Internacionales–Universidad de Chile

Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior

Latin America challenges and opportunities in cyber security in the face of the global context of cyber threats to national security and foreign policy

Juan Manuel Aguilar Antonio*

RESUMEN

La presente investigación parte de la hipótesis que este estudio establece que la región latinoamericana posee fuertes carencias en el desarrollo de una política nacional de ciberseguridad y en la construcción de capacidades para enfrentar los riesgos y amenazas provenientes del ciberespacio en dimensiones que afectan la seguridad nacional y política exterior. De esta forma, la investigación se compone de seis partes, en la primera se presentan los enfoques teóricos del neorrealismo, constructivismo y teoría de la guerra, que establecen los vínculos entre teorías de las relaciones internacionales, seguridad nacional y ciberseguridad. En el segundo apartado se aborda el proceso de securitización de Internet en la última década del siglo xx y la primera del siglo xxi. En la tercera parte, se presenta el contexto de ciberamenazas a nivel global y su comparativo con la situación de América Latina. Después, se analiza el estado actual de cibercapacidades de la

* Candidato a Doctor por la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México (UNAM). Egresado del curso Desarrollo de Políticas Cibernéticas del Centro William J. Perry (2019). Investigador del Colectivo de Análisis de Seguridad con Democracia (CASEDE AC) en México. Correo electrónico: jm.aguilar@casede.org. ORCID: https://orcid.org/0000-0002-4686-685X. Recibido: 20 de abril de 2020. Modificaciones: 15 de enero de 2021. Aceptado: 25 de enero de 2021.

región, con base a mediciones como el Global Cybersecurity Index (GCI) y el National Cyber Security Index (NSCI), con el fin de hacer un ejercicio comparativo entre América Latina y otras regiones del mundo. En la quinta parte se analizan, a nivel individual, los esfuerzos de los países de América Latina en el desarrollo de una política nacional de ciberseguridad y construcción de cibercapacidades con base en los informes sobre la materia de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), así como los indicadores de la metodología del NCSI. Por último, se presentan unas breves conclusiones en el que se exaltan las áreas de oportunidad y mejora para la región latinoamericana en la construcción de una política de ciberseguridad y construcción de cibercapacidades.

Palabras clave: Seguridad Cibernética – Seguridad Nacional – Política Exterior – Ciberpoder.

ABSTRACT

This research is based on the hypothesis that the Latin American region has serious deficiencies in the development of a national cybersecurity policy and in the construction of skills to face the risks and threats from cyberspace in dimensions that affect national security and foreign policy. In this way, the research has six parts, the first one presents the theoretical approaches of neorealism, constructivism and theory of war, and shows the links between the theories of international relations, national security and cybersecurity. The second section explains the process of securitization of the Internet in the last decade of the 20th century and the first decade of the 21st century. In the third part, the global cyber threat context is presented and its comparison with the situation in Latin America. Then, it analyzes the current state of cyber capabilities in the region, based on measurements as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NSCI), in order to make a comparative analyzes between Latin America and other regions of the world. The fifth part analyzes at the individual level the efforts of the Latin American countries in developing a national cybersecurity policy and building cyber capabilities based on the reports of the Organization of American States (OAS) and the Inter-American Development Bank (IDB), and it also analyzes with the indicators of the NCSI methodology. Finally, some brief conclusions are presented in which the areas of opportunity and improvement for the Latin

American region in the construction of a cybersecurity policy and construction of cyber capabilities are highlighted.

Keywords: Cybersecurity – National Security – Foreign Policy – Cyber Power.

Introducción

La ciberseguridad es un tema central de la política internacional del siglo xx, con fuertes repercusiones en esferas como la seguridad nacional y política exterior de los Estados-Nación. Desde la popularización, democratización y normalización en la vida cotidiana de Internet, a finales de la década de los noventa del siglo xx, pasando por hechos como el ciberataque de Tallin, Estonia (2007), hasta el reciente ciberataque a 18,000 agencias gubernamentales y empresas detectado por el gobierno de los Estados Unidos, en diciembre de 2020, este campo se ha transformado en una nueva arena de influencia, confrontación y lucha de las relaciones internacionales.

En el ámbito de la discusión teórica existen importantes aportes de la escuela neorrealista, constructivista, y desde la comprensión de la teoría de la guerra, para analizar como el ciberespacio está reinventando la lógica de los conflictos en el siglo xxi, así como de ser utilizado como un instrumento vital para la consolidación del poder nacional en el concierto de las potencias globales y el peso de las regiones en la geopolítica internacional. Asimismo, para el caso concreto de los Estados-Nación, la necesidad de crear una política nacional de ciberseguridad y una Estrategia Nacional de Ciberseguridad (ensc) se ha transformado en un aspecto clave para garantizar la seguridad nacional (Klimburg, 2012). Y con base a la biblioteca digital del Centro de Excelencia de la Ciberdefensa Cooperativa (ccdcoe Tallin, por sus siglas en inglés), de la Organización del Tratado del Atlántico Norte (otan) un total de 77 naciones del mundo ha creado documentos vinculados al tema de la ciberseguridad con un enfoque centrado en la seguridad del Estado-Nación, entre las que se incluyen miembros de la otan, aliados estratégicos de esta alianza, así como múltiples países de África, América Latina, el Caribe, Asía y Oceanía (ccdcoe Tallin, 2020).

Frente a este contexto, las naciones miembros de la otan han priorizado la

securitización del ciberespacio. Mientras que otras regiones como América Latina y, en menor medida, Asía han abordado el tema de ciberseguridad con un énfasis más especializado en el ámbito privado, individual y penal. Del mismo modo, es importante destacar que la región latinoamericana, dadas diversas condiciones como el grado de penetración de Internet, falta de categorización de Infraestructura Crítica Nacional vinculada al ciberespacio, y reciente creación o ausencia de marco legal para atender ciberincidentes o ataques, es definida como una "zona gris" en materia de seguridad cibernética (Martin, 2015).

En ese sentido, la hipótesis de este estudio establece que la región latinoamericana posee fuertes carencias en el desarrollo de una política nacional de ciberseguridad y en la construcción de capacidades para enfrentar los riesgos y amenazas provenientes del ciberespacio en dimensiones que afectan la seguridad nacional y política exterior. De esta forma, la investigación se compone de seis partes, en la primera se presentan los enfoques teóricos del neorrealismo, constructivismo y teoría de la guerra, que establecen los vínculos entre teorías de las relaciones internacionales, seguridad nacional y ciberseguridad. En el segundo apartado se aborda el proceso de securitización de Internet en la última década del siglo XX y la primera del siglo XXI. En la tercera parte, se presenta el contexto de ciberamenazas a nivel global y su comparativo con la situación de América Latina. Después, se analiza el estado actual de cibercapacidades de la región, con base a mediciones como el Global Cybersecurity Index (GCI) y el National Cyber Security Index (NSCI), con el fin de hacer un ejercicio comparativo entre América Latina y otras regiones del mundo. En la quinta parte se analiza a nivel individual los esfuerzos de los países de América Latina en el desarrollo de una política nacional de ciberseguridad y construcción de cibercapacidades con base en los informes sobre la materia de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), así como los indicadores de la metodología del NCSI. Por último, se presentan unas breves conclusiones en el que se exaltan las áreas de oportunidad y mejora para la región latinoamericana en la construcción de una política de ciberseguridad y construcción de ciber capacidades.

I. Vínculos entre teorías de relaciones internacionales, seguridad nacional y ciberseguridad

A. El ciberespacio como instrumento de poder: la visión neorrealista

La emergencia del ciberespacio como nueva arena política internacional implica la posibilidad de su utilización para perseguir intereses particulares de los Estados-Nación, actores privados públicos o individuos a través de Internet. En ese sentido, Joseph Nye creó el término de ciberpoder al que define como: "la habilidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en el ciberdominio (Nye, 2010)". Esta definición establece al ciberespacio como una arena de interacción, control y manipulación, en la que los actores inmersos utilizan los recursos a su disposición, capacidades y ventajas cualitativas o cuantitativas para utilizar este dominio e influir en la realidad internacional con el fin de impactar o modificar sus condiciones a su favor.

Para Sheldon (2012) el uso y aplicación del ciberpoder está orientado a aspectos tácticos, técnicos y operacionales en el internet. Lo anterior está influenciado por la creación de un objetivo estratégico, perseguir los Estado-Nación, tanto en épocas de armonía como de conflicto, y tiene la función de manipular el contexto de un dominio estratégico, en este caso el ciberespacio, con el fin de obtener algún tipo de superioridad frente a adversarios y degradar o limitar el desarrollo de capacidades semejantes por los mismos. En ese sentido, el ciberpoder es "la suma de todos los efectos estratégicos generados por ciberoperaciones en el mundo virtual" (Sheldon, 2012). Por su parte, Kuehl (2009) se refiere al concepto como: "[el] centro de un conjunto nuevo de conceptos y doctrinas que son una palanca clave en el desarrollo y ejecución de política, ya sea contra el terrorismo, crecimiento económico o asuntos diplomáticos, etc". Mientras que para Starr (2012) es: "[un instrumento] que a medida que evoluciona, tiene el potencial de mejorar cada una de las palancas del poder nacional [de un Estado-Nación], en especial el militar y el informático".

En vista de las múltiples perspectivas que se tienen del concepto, capacidades y medios de impacto o influencia en torno al ciberpoder, el paradigma neorrealista atendió el problema del ciberespacio y el concepto del ciberpoder en 2010 con la publicación del artículo Cyber Power de Joseph Nye, que generó un esquema teórico para desentrañar a este nuevo campo de influencia y acción política desde la perspectiva del poder del Estado-Nación. Para Nye (2010), la emergencia del ciberespacio como campo para ejercer poder se asocia

más a un proceso de difusión de poder que a una transición del mismo. Esta difusión está vinculada a la posesión o manipulación de información por parte de los gobiernos, función para la que está diseñada el Internet, que les permita modificar la polaridad en la estructura internacional, o al menos en el ciberespacio. En ese sentido, los rápidos y vertiginosos avances de las Tecnologías de la Información (TIC's) y la tajante disminución del costo, procesamiento y transmisión de información, hacen necesario que el Estado regule y controle la arena del Internet, así como que construya doctrinas que consideren a este como un elemento crucial para salvaguardar la integridad de la soberanía, interés y seguridad nacional y política exterior.

Un aspecto vital del análisis neorrealista es que destaca que el ciberpoder no reemplaza al espacio geográfico, además de que no anula la soberanía del Estado-Nación. No obstante, acepta que este es un régimen de componentes físicos y materiales que coexisten con el ejercicio del poder estatal. Asimismo, este enfoque expresa que el ciberespacio es una arena que debe ajustarse al dominio y control del régimen jurídico de los gobiernos de cada país, el cual debe estar en sintonía con una agenda global para la gobernanza del Internet (Choucri et al., 2013; Singer y Friedman, 2013) o un Tratado del Ciberespacio en el que los actores hegemónicos claves regulen este campo y creen normas para delimitar el comportamiento de las partes interesadas (Hughes, 2010). En este sentido, un elemento clave del neorrealismo es su consideración del papel vital de las empresas privadas, promotoras o creadores de softwares, como entidades de suma importancia para la consolidación de un régimen internacional de normas del Internet, así como para salvaguardar la seguridad nacional y delimitar la política exterior de las naciones. No obstante, deja en claro que los Estados-Nación son los mandamases de la regulación y control del ciberespacio (Nye, 2010).

B.- La teoría de la guerra y la comprensión constructivista

El desarrollo de la Teoría de la Guerra Moderna, de Carl Clausewitz, ha marcado un fuerte énfasis en las características de los campos o espacios de batalla, como un hecho crucial que determina la superioridad de un Estado, sobre otro en una confrontación bélica. En su obra clásica "De la Guerra", Clausewitz delínea los conceptos clave de las estrategias castrenses del mundo contemporáneo, a la par que en su doctrina de la Guerra Total introduce un marco analítico que cimentó las características del poder terrestre de los Estados-Nación, con conceptos como el espacio, tiempo, fuerza moral y material, teatro de guerra y operaciones (Benítez, 1986). En específico, la categoría de teatro de guerra sirvió para la creación de esquemas bélicos semejantes en los años consecuentes a la publicación de los textos

de Clausewitz. Por ejemplo, en 1890 Alfred Tayer Mahan expandió la teoría de la guerra al espacio marítimo y determinaría los factores estratégicos para la superioridad del poder naval (Nye, 2014). Y para 1921, Giulio Douhet publicaría su obra "El Dominio del Aire", donde establecería los principios y ventajas del poder aéreo (Kuel, 2012). Posteriormente, el desarrollo del poder espacial, vinculado al desarrollo aeronáutico de cohetes y satélites, sería un tema de análisis recurrente y de amplia atención durante la segunda mitad del siglo xx para los teóricos de la guerra (Gray & Sloan, 1999).

Las ideas anteriores, de capacidades y factores individuales o contextuales, ligados a las características geográficas y físicas de cada teatro de guerra, presentan el hecho de que los cuatro campos de confrontación de la teoría clásica de la guerra ostentan características intersubjetivas ligadas al espacio físico, así como capacidad de influencia y poder para cada Estado-Nación. Asimismo, el desarrollo de las armas se determinó por el medio geográfico en que estas eran utilizadas —tierra, mar, aire, etc.— y debían estructurarse para causar daño e impacto al enemigo en cada una de estas arenas (Kello, 2012). Dado que la confrontación bélica terrestre, con sus estrategias, técnicas y armamento (fusiles, tanques, morteros) eran completamente diferentes al espacio marítimo (submarinos, buques) o aéreo (jets o bombarderos). También, las cualidades intersubjetivas del Estado-Nación (como su territorio, capacidades y poderío bélico) determinan su capacidad para influir en las diferentes arenas de batalla, como fue el caso de Estados insulares, que necesitaron de transportarse a otras zonas para realizar guerra terrestre (Japón o Inglaterra), o países que no detentan litoral y, por lo tanto, se vieron limitados a desarrollar un amplio margen de poder marítimo, aunque no quedaron excluidos de él (Bolivia, Bielorrusia, Suiza, Kenia, etc.). La misma condición aplica para el campo aéreo o espacial, en los que el poderío de un Estado-Nación es determinado por la cantidad de arsenal (aeronaves) o desarrollo tecnológico (programa espacial) para detentar superioridad en estas esferas.

Esta visión de la intersubjetividad de los teatros de guerra y capacidades del Estado-Nación nos acerca al concepto de identidad, desarrollado dentro del constructivismo. La identidad del Estado-Nación o actor internacional es un concepto que sirve como un puente entre la estructura de las normas o el régimen internacional y los intereses de los actores (Wendt, 1994). En sí, la identidad supone una categoría dentro del análisis constructivista que sirve para señalar que en el sistema internacional existe una estructura normativa que determina el papel y grado de importancia de sus diferentes miembros (Estados protagonistas o no protagonistas) y crea una noción en torno a lo que es correcto (cooperación, alianzas) y lo que es incorrecto (conflicto, disuasión), derivado de las

interacciones que se dan entre los actores (Stanković, 2019). Por otra parte, las interacciones entre los actores del sistema internacional y las capacidades intersubjetivas de cada Estado, u otros actores, ayudan a delimitar el papel que ocupan dentro de la estructura, así como su interés nacional (Edmunds, 2014).

Las ideas anteriores presentan al ciberespacio como un nuevo campo o espacio de batalla, en el que se miden los Estados-Nación a través de la confrontación, para alcanzar sus objetivos e intereses particulares. Este supuesto nos obliga a discutir elementos de la Teoría de la Guerra tradicionales como: a) aceptar el ciberespacio como un espacio de batalla; b) la naturaleza estado céntrico del análisis bélico y la posibilidad de aceptar otros actores en este marco de análisis; c) las características de las ciberarmas desde las categorías de espacio, tiempo y fuerza, y d) el señalar si el ciberespacio es un teatro de guerra o un teatro de operaciones.

Respecto de la primera noción, se expresa que esta idea es difícil de aceptar a cabalidad dado que el concepto de ciberguerra es una categoría no abiertamente aceptada por varios teóricos (Kello, 2017; Firdous, 2020). En ese sentido, en vez de señalar al ciberespacio como una arena de batalla, podemos expresar que es un campo de interacción, en el que pueden existir dinámicas de conflicto y cooperación entre diferentes actores. Por otra parte, la Teoría de la Guerra señala a los Estado-Nación como los actores fundamentales del análisis del conflicto bélico. Ante esto, se argumenta que —de la misma manera que en el análisis clásico de este enfoque— los conflictos más trascendentales en Internet están representados por el choque entre dos o más países. No obstante, el constructivismo permite ampliar el margen de consideración a otras entidades que tienen un papel de importancia dentro del ciberespacio y construyen una identidad e intereses particulares para utilizar o crear ciberpoder, como las empresas privadas, los hackers, o grupos criminales. Esta visión es cercana al análisis de Van Creveld (1991), que en su libro "The Transformation of War" indicó que en el futuro la guerra no se limitará a choques entre los Estado-Nación, sino entre: "[…] grupos a los que hoy llamamos terroristas, guerrilleros, bandidos y ladrones, pero que sin duda recurrirán a títulos más formales para describirse a sí mismos" (Van Creveld, 1991). La descripción anterior permite englobar a hacktivistas o cibercriminales y, de hecho, el mismo Van Creveld (2002) señaló a los hackers como parte de los nuevos actores emergentes en los conflictos del siglo xxi.

La tercera cuestión es atender las características de las ciberarmas en comparación a las categorías clásicas de Clausewitz: espacio, tiempo y fuerza. Respecto del espacio, se expresa que este elemento se desvirtúa completamente dentro del ciberespacio

(software, malwares[1], protocolos IP[2]) dado que esta esfera carece de componentes materiales para que exista un grado de daño o amenaza. En todo caso, el máximo grado de daño que podría alcanzarse sería la interrupción o negación de un servicio derivado del saboteo por un actor rival en el mundo virtual. Respecto a la parte física del ciberespacio, se señala que el espacio físico se vuelve vital cuando se vincula con Infraestructuras Críticas del Estado-Nación (redes de energía, presas, sistema de energía en hospitales, etc.). En ese sentido, el daño a una Infraestructura Crítica es uno de los márgenes más graves de afectación que puede provocar una ciberarma. En relación al tiempo, a diferencia del concepto anterior, esta categoría maximiza su grado de afectación e impacto en el campo virtual, en contraste con el espacio físico. Dado que el lapso de planificación de una agresión en contra de un adversario puede operacionalizarse en un período más breve. Asimismo, si un Estado es víctima de un ciberataque, se vuelve de vital importancia resolver la agresión por la extracción de información o daño que es capaz de sufrir de forma ágil. Por último, la categoría de fuerza se expresa porque al interior del ciberespacio la diferencia de fuerzas se vuelve asimétrica, y permite a un individuo o grupo de personas, equiparar su nivel de acción al de un Estado, con la capacidad de vulnerarlo severamente, al menos dentro de Internet. Sin embargo, esta condición se verá superada si las interacciones o conflictos saltan al espacio material, ya que en el mundo físico los Estado-Nación detentan más poder coercitivo que cualquier otro actor. Finamente, se debe resolver si el ciberespacio es un teatro de guerra o de operaciones, que se anexa a los otros campos de confrontación de la Teoría Clásica de la Guerra. Además, se establece que el ciberespacio no modifica completamente la naturaleza de la guerra, aunque se acepta que sí crea nuevas dinámicas en el desarrollo de los conflictos que se desenvuelven en este dominio.

1 Un malware es un programa, código, o software malicioso o dañino, cuyo fin es causar un grado de afectación a un sistema informático de forma intencionada y sin el conocimiento del usuario.

2 El Protocolo IP o Internet Protocol (IP) es uno de los pilares básicos de Internet, ya que permite el desarrollo y transporte de paquetes de datos, aunque su recepción no está asegurada. Además, forma parte del conocido protocolo TCP/IP.

II. Seguridad nacional, securitización del internet y ciberseguridad

En los hechos, la ciberseguridad es un tema incipiente que hace presente su importancia en la seguridad nacional y política internacional en la última década de siglo xx. Desde su creación, durante la década de los sesenta, y hasta el año 2000, se pensó que Internet era un espacio libre de la injerencia del Estado e inmune a la soberanía que transformaría el flujo de información, democratizaría el conocimiento y cambiaría las dinámicas de participación ciudadana. Este período –que abarca los años 1960 a 2000–, es definido por Palfrey (2010) como la fase de acceso abierto del ciberespacio y comprende su popularización en la sociedad y uso cada vez más constante en la economía, medios de comunicación, temas de gobierno y demás esferas de la sociedad. No obstante, las dinámicas derivadas de este proceso lo hicieron un campo en que la injerencia del Estado-Nación fue inevitable y necesaria.

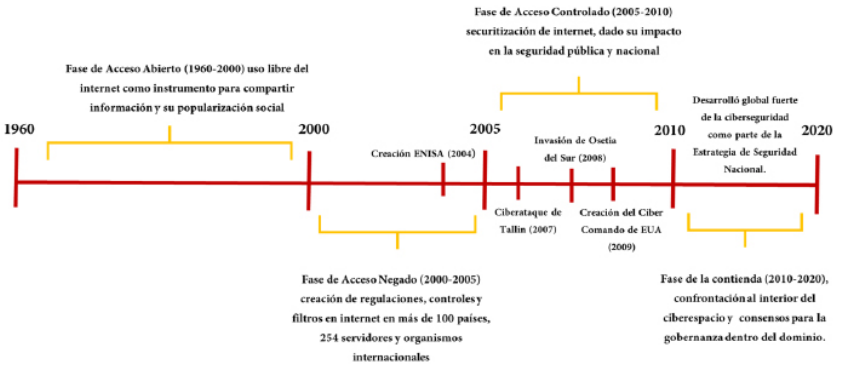
En ese sentido, la primera penetración del Estado-Nación en la esfera de Internet se da durante los años 2000–2005, que es definida como la fase del acceso negado (Palfrey, 2010; Deibert & Rohozinski, 2010). Esta inmersión de los gobiernos en el ciberespacio se da a razón de que se comenzó a considerar que existen actividades y expresiones en Internet que deben ser reguladas, administradas e incluso bloqueadas. Respecto de esto, en el informe "Access Denied: The Practice and Policy of Global Internet Filtering", Zitrain y Palfrey (2007) documentaron que durante ese período alrededor de 70 países y 289 proveedores de servicio de Internet crearon legislaciones para el control de actividades en el dominio, o implementaron filtros para controlar su contenido o bloquearlo. El primer conjunto de legislaciones de este tipo se dio en el campo económico, dado el gran potencial de Internet para acelerar las dinámicas comerciales. Posteriormente, la segunda etapa de la injerencia del Estado se da en el control de los contenidos legales e ilegales, y regulación del flujo de datos e información. Esta aplicación de controles coercitivos se dio tanto en los países democráticos como autoritarios. Las diferencias oscilan en que naciones como la República Popular China, la Federación Rusa y Arabia Saudita, crearon filtros de control de contenido y prohibieron el flujo de información o acceso a sitios en línea que se consideraba afectaban la imagen del gobierno. Mientras que en las naciones democráticas se redactaron leyes y códigos de justicia aplicados a actividades económicas, políticas y de medios de comunicación.

También es importante destacar que fue durante estos años que Internet sufrió un proceso de securitización, en que los países pusieron énfasis en crear nuevas definiciones para delimitar delitos o actividades ilícitas que se

realizaran a través de esta plataforma o la utilizaran para su realización. En los hechos, más de cien países establecieron en sus códigos de justicia y sistema penales, definiciones sobre los cibercrímenes que debían ser juzgados y castigados por el Estado, y organismos internacionales como la Organización para la Cooperación Económica (OCDE), la Unión Europea (UE), o la Unión Internacional de Telecomunicaciones (ITU), crearon convenios y acuerdos para la regulación de estas actividades, hasta la creación del Convenio de Budapest en 2004, que fue el primer intento de una armonización sobre ciberdelitos para su investigación y persecución (Klimburg; 2012, Take, 2012).

Es en este punto que el ciberespacio mostró su capacidad de injerencia en la seguridad pública y se empezó a evaluar su capacidad de impacto en la seguridad nacional, por lo que se considera que la fase del acceso negado no creó, como tal, bordes y barreras reales en Internet, pero sí empezó a delimitar las líneas geopolíticas de contacto entre los diferentes países en su tendencia política, modelo económico e intereses nacionales. Posteriormente, sería en la fase de acceso controlado, que abarca entre los años 2005 y 2010, que el proceso de securitización del ciberespacio alcanza a la seguridad nacional. Esto se dio a través de la creación de un marco de instituciones que previnieran ciberincidentes y eventos concretos a nivel global, entre los primeros destaca que tanto la creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés), en 2004, como el Cibercomando de Estados Unidos, en 2009, los cuales consideraron que el uso del ciberespacio por parte de grupos terroristas islámicos era una acción que podía vulnerar la seguridad nacional del Estado (Newmeyer, 2015; Samaan, 2010). Sin embargo, en los hechos, eventos como el ciberataque de Tallin, Estonia (2007), o el hackeo a la red gubernamental de Georgia, durante la invasión de Osetia del Sur (2008), mostraron el potencial que tenía el ciberespacio para vulnerar a un Estado-Nación. Sería a razón de estos eventos que la ciberseguridad pasa a ser un apartado necesario en toda doctrina y estrategia de seguridad nacional, para garantizar su seguridad y capacidad de decisión soberana. Y es precisamente a raíz de los hechos de Tallin que todos los países de la OTAN, y posteriormente el resto del mundo, empiezan a incluir al tema en la Estrategia de Seguridad y crear sus primeras ENCS. Por último, Palfrey (2010) expresa que desde 2010 nos encontramos en la fase de la contienda, que se define por la confrontación entre las diferentes partes interesadas al interior del ciberespacio y su capacidad para crear consensos y la gobernanza dentro de este dominio. Las cuatro fases se muestran en la figura 1.

Figura 1 Fases de regulación de Internet e inclusión de ciberseguridad en seguridad nacional

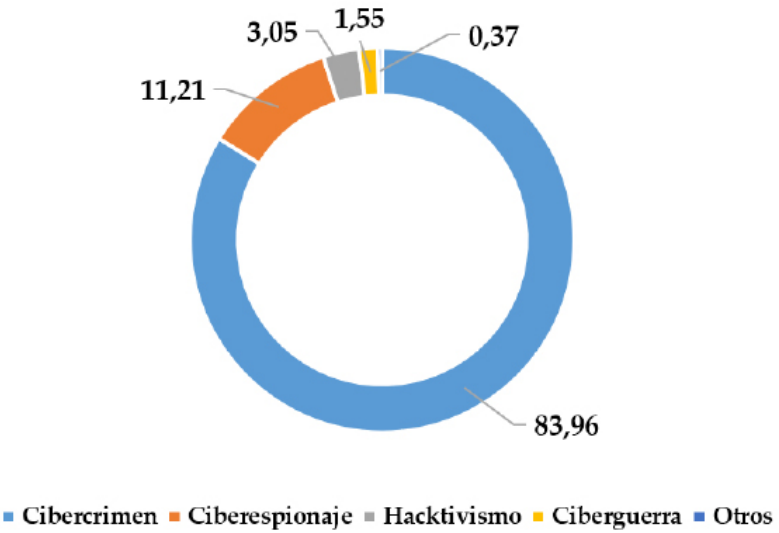


Fuente: Elaboración propia con base en Zitrain y Palfrey (2007) y Palfrey (2010).

III. Contexto global de ciberamenazas y situación de América Latina

La inclusión de la ciberseguridad como una parte trascendental de la política de seguridad nacional se da a razón de un contexto adverso y cambiante de amenazas provenientes del ciberespacio. En relación a esto, el sitio Hackmageddon (2020), centrado en la documentación de ciberincidentes o ataques de trascendencia para gobiernos y empresas, registró un total de 1,802 eventos en 2019, que involucraron a TIC's e infraestructuras nacionales críticas de múltiples países, como se muestra en la figura 2. En las motivaciones detrás de dichos ciberincidentes o ataques, con connotaciones políticas o centrados en dañar la seguridad nacional de un actor gubernamental representaron un total 298 casos, entre los que se encuentran las clasificaciones de ciberguerra, hacketivismo y ciberespionaje, categorías que competen a intentos de vulneración de sistemas informáticos, tecnologías de la operación y bases de información de gobiernos nacionales.

Figura 2. Motivaciones de ciber incidentes 2019



Fuente Hackmageddon (2020).

Dicho contexto representa un reto para gran cantidad de países, por el gasto y necesidad de creación de capacidades para enfrentar riesgos y amenazas provenientes del ciberespacio. En ese sentido, el portal Cybersecurity Ventures (2020) expresa que desde 2004 el mercado global de ciberseguridad pasó de los 3,500 a los 120,000 millones de dólares en 2017, con lo cual creció 35 veces a su tamaño original en dicho período y se prevé que el gasto mundial en productos y servicios de ciberseguridad para la defensa contra el ciberdelito supere los mil millones de dólares de forma acumulativa durante el período 2017–2021. Con ello se anticipa un crecimiento del 12 al 15% anual hasta 2025.

Sin embargo, en muchos aspectos los retos de la ciberseguridad avanzan más rápido que la capacidad de acción de los gobiernos. Tan solo 2017, se presentaron 1,579 brechas de información en el sector financiero de Estados Unidos, las cuales aumentan a una tasa promedio de 44.6% anual (PR Newswire, 2018). A la par, el T-Sec Radar de Deutsche Telekom detecta que se dan 60,312[3] ciberataques cada mi-

3 Las visualizaciones de mapas en torno a ciberincidentes de *T-Sec Radar* de *Deutsche Telekom* es una de las aplicaciones más impresionantes que permite tecnologías de vanguardia como el *Internet of Things* (IoT) y el Big Data, una visualización rápida puede verse en este link: https://sicherheits-tacho.eu/start/main

nuto, lo que representa 3,712,960 por hora, y 79,390,302 en un solo día (Sicherheitstacho, 2021). Por su parte, la plataforma Digital Attack Map (2021) lleva el registro diario de los ataques DDoS en el mundo, que son accesibles a cualquier individuo, empresa o gobierno por tan solo 150 dólares[4]. Por lo que este sitio se encarga de detectar su origen y país-destino, los cuales alcanzaron cifras de más 8,000 diarios durante el último año.

Respecto al ámbito regional, el informe Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos presentó que desde el 2012 los ciberataques a entidades o sitios de Internet públicos y privados han crecido a cifras anuales de más del 61% (OEA/Symantec 2014). A la par que países como Ecuador, Guatemala, Bolivia, Perú y Brasil, estuvieron dentro de las diez principales países que con más afectaciones por *malware*. Del mismo modo, Uruguay, Colombia y Chile presentaron cifras de infección por *malware* por encima de la media global, situación que enmarcó a la región, junto a Asia, con las tasas más altas de virus maliciosos a nivel global (Aguilar-Antonio, 2019). También se destaca que desde 2015 el uso del ciberespacio para realizar fraude bancario se ha transformado en un problema, dado que se estima que el 92% de las entidades financieras han presentado un ciberataque, con una tasa de éxito del 37% (OEA 2018).

Por su parte, Kaspersky Lab (2020) registró más de 746 mil ataques de *malware* diarios durante 2020 en América Latina, lo que implica que se realizan 9 ciberataques de *malware* por segundo. A la par que se detectó que los tres principales países con mayor incidencia para el cibercrimen son Brasil (56.25%, del total de la región), México (22.81%) y Colombia (10.20%). Por otra parte, es importante señalar que, de un total de 62 millones de ataques detectados por esta firma durante 2020, 66% se vinculaban a robos a entidades privadas y comerciales, mientras el 34% restante se vinculaban a actividades criminales, hacktivismo y ataques a sistemas gubernamentales.

4 Los ataques DDoS son de los más accesibles y baratos, y los que más éxito tienen en vulnerar seguridad informática, la plataforma de *Digital Attack Map* muestra la profundidad y utilización diaria de esta modalidad de ciber agresión: https://www.digitalattackmap.com/

IV. Contexto actual de cibercapacidades de América Latina

Entender el contexto actual de cibercapacidades de América Latina se puede realizar a través de dos métricas internacionales que evalúan la política de ciberseguridad de los Estados-Nación, las cuales son el Índice Nacional de Ciberseguridad (National Cyber Security Index o NCSI, en inglés), de la E-Governance Academy, y el Índice Global de Ciberseguridad (GCI, por sus siglas en inglés), de la Unión Internacional de Telecomunicaciones (ITU).

Respecto del NCSI (2019), se especifica que esta medida evalúa la preparación de los países para prevenir ciberamenazas y gestionar ciberincidentes, a través de doce indicadores, concentrados en una ponderación global que van del 0 al 100. Esta medición permite medir las capacidades de ciberdefensa de los países evaluados. Por otra parte, el GCI (2018) mide el grado de compromiso e importancia que los Estado-Nación han dado al tema de la ciberseguridad en el desarrollo de su política de seguridad nacional. Con base en los cinco ejes de la Agenda Global de Ciberseguridad[5] (AGCS), establecida por la ITU en 2007, vinculados a tres objetivos principales de los cuales se encarga esta medición, que son: 1) tipo, nivel y evolución a lo largo del tiempo del compromiso con la ciberseguridad; 2) progreso y seguimiento en el grado de compromiso con la ciberseguridad desde una perspectiva global y regional, y 3) la división del compromiso de seguridad cibernética o la diferencia entre países en términos de su nivel de participación en iniciativas de ciberseguridad. Del mismo modo, es importante mencionar que el GCI (2018) evalúa a los 194 países del mundo, y otorga una calificación que va del 0 al 100 por ciento, en la que cien representan el mayor compromiso con la AGCS, y 0 la ausencia total de compromiso.

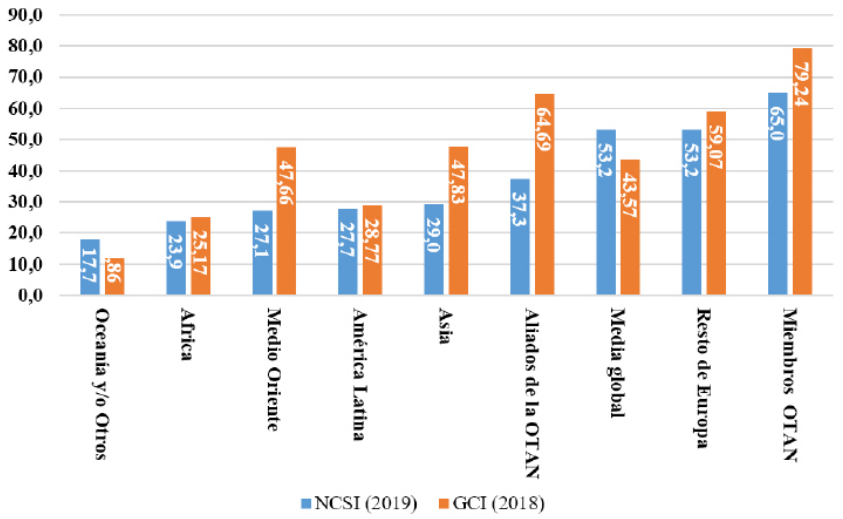
Por último, es importante mencionar que tanto las mediciones del NCSI (2019) y el GCI (2018), abordan aspecto claves para el desarrollo de cibercapacidades como marco legal de

5 Los 5 ejes de la AGCS son marco legal para la ciberseguridad y ciber crimen, 2) medidas técnicas e instituciones encargadas de ciberseguridad, 3) existencia de instituciones y estrategias de coordinación de políticas para el desarrollo de una ENCS, 4) desarrollo de métricas que analizan la investigación científica, educación y programas de capacitación y certificación de profesionales y agencias del sector público, 5) existencia de asociaciones, marcos cooperativos y redes de intercambio de información del gobierno para la cooperación internacional:

ciberseguridad, medidas técnicas, estructura internacional y cooperación internacional. También exponen las áreas de oportunidad y de mejora de las legislaciones nacionales contra cibercrimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT). No obstante, el NCSI posee un apartado más amplio en el desarrollo de cibercapacidades, dado que trata con mayor profundidad las habilidades para atender ciberincidentes y combatir amenazas.

Para ubicar el nivel de cibercapacidades en el que está ubicado América Latina respecto de otras regiones o conjunto de países del mundo, se agruparon el total de naciones incluidas en el GCI (2018) y el NCSI (2019) en ocho diferentes grupos, que son: 1) Países de la OTAN, 2) Aliados de la OTAN, 3) Resto de Europa, 4) Asia, 5) Medio Oriente, 6) América Latina, 7) África y 8) Oceanía y otros. De cada conjunto se obtuvo el promedio del total de la calificación asignada a cada país que oscila entre 0 y 100, a la que se calculó la media global en cada métrica. Los resultados de este análisis se muestran en la Figura 3 con el comparativo entre los dos índices. En dicho gráfico es visible que el grupo de países que más ha priorizado el desarrollo de cibercapacidades y mostrado el mayor compromiso con la AGCS son los miembros de la OTAN. Dado que detentan las calificaciones más altas en ambas métricas, con ponderaciones del 79.2 sobre 100 para el NCSI (2019), y 65 puntos para el GCI (2018). Del mismo modo, destacan grupos como el Resto de Europa con notas de 59.1 y 53.2, respectivamente, y Aliados de la OTAN, con ponderación de 64.9 y 37.3. En relación a América Latina, esta se encuentra en la sexta posición con una calificación de 28.8 para el GCI (2018), y solo por delante de regiones como África y Oceanía y otros. Para el caso de NCSI (2019) la región se encuentra en la quinta posición con una nota de 27.7. Por último, se destaca que en ambas mediciones Latinoamérica se encuentra por debajo de la media global con 25.5 y 14.8 puntos, respectivamente.

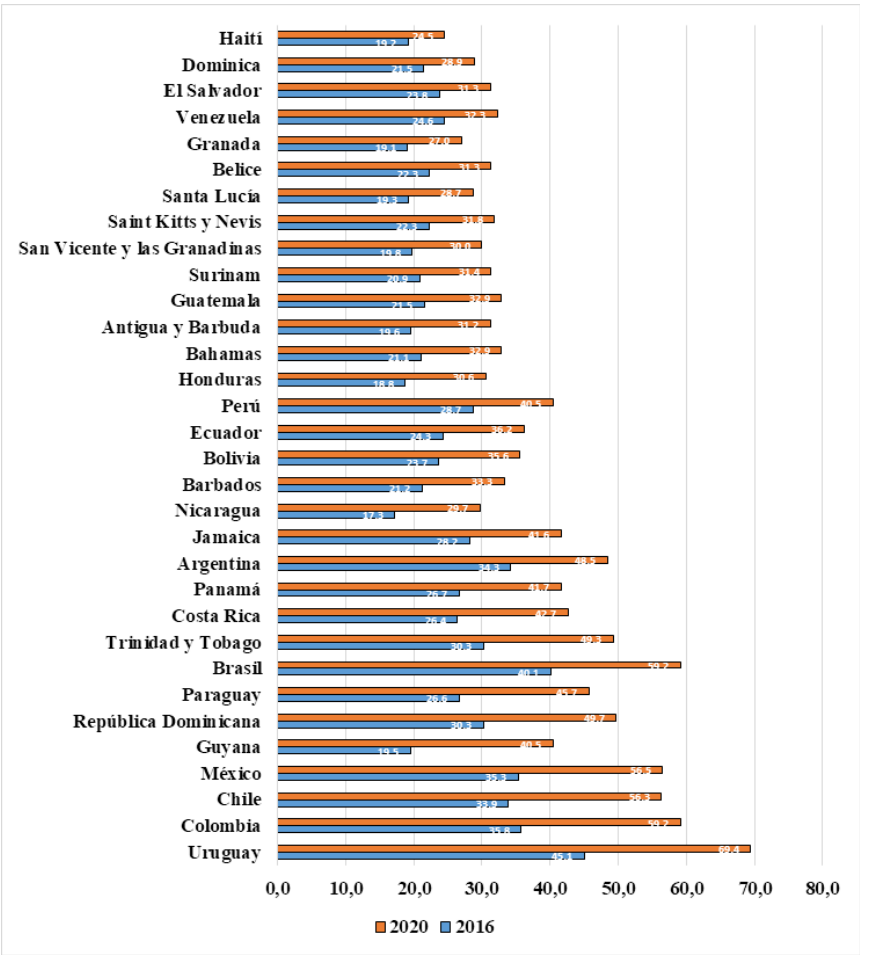
Figura 3 Comparativo regional y global entre ponderaciones del GCI (2018) y el NCSI (2019)



Fuente: Elaboración propia.

Si bien el GCI (2018) y el NCSI (2019) muestran un atraso de América Latina en el desarrollo de capacidades de ciberdefensa, las diferencias entre los países de la región muestran claras desigualdades. Para salvaguardar el tema de las diferencias nacionales entre los países latinoamericanos, se destaca el trabajo realizado por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) con la publicación de los informes "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?", en 2016, y el reporte "Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe", en 2020. Sendos informes corresponden a un esfuerzo de ambas instituciones por medir el desarrollo de una política y capacidades en materia de ciberseguridad a través de cinco dimensiones y 49 indicadores (OEA & BID, 2016: 2020). Lo importante de ambos informes es que dan continuidad al análisis de los esfuerzos individuales de cada país y muestran las naciones que más han avanzado en el desarrollo de capacidades y política de seguridad en el período 2016-2020, dichos cambios pueden observarse en la figura 4.

Figura 4 Evolución de política y capacidades de ciberseguridad con base a la OEA & BID



Fuente: Elaboración propia.

No obstante, dado que se considera que el análisis e identificación de las áreas de oportunidad para el desarrollo de una política de ciberseguridad, así como para la construcción de cibercapacidades de los países de América Latina. En la siguiente sección se realiza un análisis a profundidad de las naciones de la región.

V.- Áreas de oportunidad y retos para la ciberseguridad en América Latina

Para analizar a nivel individual los esfuerzos de cada nación de América Latina con el desarrollo de una política y creación de capacidades de ciberseguridad, son útiles dos de las tres métricas presentadas en la sección anterior: NCSI (2019) y los informes de OEA & BID (2016; 2020). Sin embargo, es importante mencionar que ambas métricas nos dan dos diferentes perspectivas en torno a la comprensión de las áreas de oportunidad y los retos de la ciberseguridad en América Latina. Lo anterior se debe a que de momento el NCSI (2019) se ha publicado en una sola edición, con lo cual podemos tener una panorámica estática del contexto de cibercapacidades de los 11 países latinoamericanos[6] incluidos en este estudio. Por otra parte, los informes realizados por la OEA & BID (2016; 2020) nos permitan acceder a un análisis dinámico, en el cual podemos observar la evolución de los esfuerzos de las 32 naciones de la región. Del mismo modo, es importante expresar que a pesar de que se describirán en detalle cada una de las metodologías de los dos diferentes estudios, se pondrá énfasis solamente en las dimensiones que describan más los elementos claves para una política de ciberseguridad, estrechamente relacionada con la seguridad nacional y política exterior.

En ese sentido, se expresa que la metodología del NCSI (2019) está compuesta de un total de doce indicadores, que son: 1) desarrollo de política de seguridad cibernética, 2) delimitación de amenazas en el ciberespacio, 3) educación y formación de especialistas capacitados en ciberseguridad y concientización de la población, 4) aportación de cada país para mejorar el contexto global de ciberseguridad, 5) nivel de desarrollo digital del país, 6) protección de servicios esenciales por el Estado de Infraestructura Nacional Crítica, 7) servicios digitales y confidencialidad en la vida diaria, 8) Protección de datos y garantía de privacidad, 9) respuesta a ciberincidentes por parte de equipos de emergencia informática (CSIRT o CERT) ante ciberincidentes, 10) capacidad para administrar una crisis cibernética del Estado-Nación, 11) grado de compromiso del Estado para luchar contra el cibercrimen, y 12) capacidad de operaciones militares de las fuerzas armadas en el ciberespacio. Del total de indicadores, se considera que ocho están estrechamente vinculados a temas de ciberpoder, como parte del desarrollo de capacidades en el ciberespacio, así como con la seguridad nacional y política exterior del Estado-Nación, mientras otros se refieren a otras esferas políticas como educación digital, seguridad pública y servicios digitales de gobierno, como se muestra en el cuadro 1.

6 Los once países son Perú, Colombia, Chile, México, Argentina, Brasil, Jamaica, Panamá, Trinidad & Tobago, Surinam y Honduras.

Cuadro 1. Indicadores y esferas de influencia del NCSI (2019)

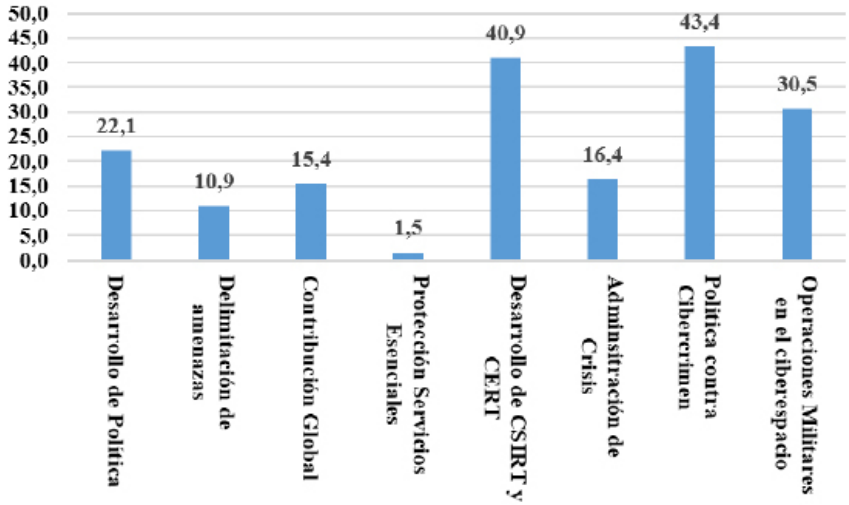
No.	América Latina	Esfera de influencia
1	Desarrollo de Política	Seguridad Nacional
2	Delimitación de amenazas	Seguridad Nacional
3	Desarrollo de Educación	Educación Digital
4	Contribución Global	Política Exterior
5	Protección Servicios Digitales	Seguridad Pública
6	Protección Servicios Esenciales	Seguridad Nacional
7	Identificación electrónica y confianza digital	Servicios Digitales de Gobierno
8	Protección Personal de Datos	Servicios Digitales de Gobierno
9	Desarrollo de CIRC	Seguridad Nacional
10	Administración de Crisis	Seguridad Nacional
11	Política contra Cibercrimen	Seguridad Nacional y Política Exterior
12	Operaciones Militares en el ciberespacio	Seguridad Nacional y Política Exterior

Fuente: Elaboración propia con base NCSI (2019).

De las ocho dimensiones vinculadas a la seguridad nacional y la política exterior, se obtuvo la media de cada indicador, así como el promedio de ponderación regional de cada uno de los once países de América Latina incluidos en el NCSI (2019), esto se puede observar en la figura 5. En dicho gráfico es visible que las dimensiones en la cuales han avanzado más los países de la región son las referentes al desarrollo de política contra cibercrimen (43.4), desarrollo de CSIRT y CERT (40.9) y operaciones militares en el ciberespacio (30.5). Respecto de la dimensión de desarrollo de política de cibercrimen, se destaca que este indicador está vinculado a la creación de códigos y legislaciones, así como a la homologación de los ciberdelitos con acuerdos internacionales, como el Convenio de Budapest, en ese sentido, los países con las ponderaciones más altas son Perú, Chile, México y Jamaica (78 puntos sobre 100 cada uno), mientras que Surinam, Hondura y Brasil son evaluados con una calificación de 0. En aspecto de desarrollo de CSIRT y CERT. Esta métrica da una ponderación de 50 puntos sobre cien, a todos los

países, con excepción de Surinam y Honduras, que son evaluados con cero. Finalmente, destaca que las Fuerzas Armadas mejor capacitadas para realizar ciberoperación son las de Perú, Colombia, Argentina y Brasil (con 67 puntos de 100), seguidos de Chile, México, Jamaica y Honduras (17 puntos) y Trinidad y Tobago, Surinam y Panamá con una ponderación de cero.

Figura 5 Ponderación de dimensiones



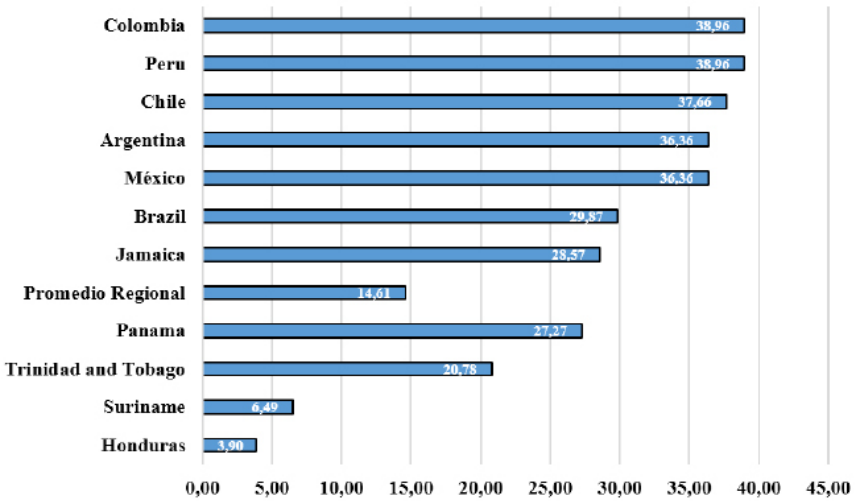
Fuente: Elaboración propia con base NCSI (2019).

Por otra parte, destaca que los indicadores en los cuales se encuentra más atrasada la región son protección se servicios esenciales (1.5), delimitación de amenazas (10.9), contribución global a la ciberseguridad (15.4) y administración de crisis cibernética del Estado-Nación (16.4). La dimensión de protección de servicios esenciales está relacionada con la capacidad de contención de un ataque que vulnere Infraestructura Nacional Crítica, vinculada a servicios esenciales como electricidad, luz, etc. En ese sentido, destaca que todos los países de la región tienen una ponderación de cero en este indicador, con excepción de Trinidad y Tobago (17 puntos), lo que demuestra que los países son altamente vulnerables en esta dimensión.

Del mismo modo, esta variable está estrechamente relacionada con el indicador de administración de crisis cibernética, en el que Argentina es el país mejor calificado (60 puntos), seguido de Colombia, México, Chile,

Panamá, Trinidad y Tobago y Honduras (20 puntos cada uno). Respecto de la dimensión de contribución global a la ciberseguridad, el mejor posicionado es Perú (66 puntos de 100), mientras el resto de las naciones tienen una calificación de 17 puntos, con excepción de Jamaica y Honduras, que son evaluados con 0, lo que devela poca acción de los gobiernos para estar comprometidos con la AGCS y realizar convenios internacionales de cooperación en materia cibernética. También destaca que los países están severamente mal evaluados en delimitación de ciberamenazas, donde todos tienen una calificación de cero con excepción de Brasil (80 puntos) y Colombia y Chile (20 puntos), lo que demuestra que a pesar de que las once naciones han avanzado en la creación de una política de ciberseguridad, no han establecido una delimitación de los riesgos provenientes del ciberespacio para el Estado-Nación. Por último, en la Figura 6 se presentan la ponderación global de los once países del NCSI (2019).

Figura 6. Ponderación global de los países de América Latina NCSI (2019).



Fuente: NCSI (2019).

Respecto de los informes realizados por OEA & BID (2016; 2020), se destaca que la metodología de estas instituciones está compuesta de cinco dimensiones: 1) política y estrategia de seguridad cibernética, 2) cultura cibernética y sociedad, 3) formación, capacitación y habilidades de seguridad cibernética, 4) estándares, organizaciones y tecnologías, y 5) marcos legales

y regulatorios. De las dimensiones expuesta, se expresa que la numero 1 y 5 están vinculadas a aspectos de ciberpoder, seguridad nacional y política exterior. Del mismo modo, en la figura 4 de la sección anterior se presentaron las ponderaciones y avances que alcanzaron los 32 países de América Latina en el período 2016–2020. Sin embargo, en este apartado nos concentraremos en analizar cuales han sido los cinco países que más han mejorado en dicho lapso y cuáles tuvieron el desempeño más precario en la elaboración de una política de ciberseguridad. En este sentido es importante destacar que la ponderación nuevamente va del 0 al 100 y los dos grupos de países se presentan en el cuadro 2.

Cuadro 2 Países con mejor y más precario desempeño en fortalecimiento de política de ciberseguridad OEA & BID (2016; 2020).

Países con el mejor desempeño				
No.	**País**	**2016**	**2020**	**Δ Cambio**
1	Uruguay	45.1	69.4	24.4
2	Colombia	35.8	59.2	23.4
3	Chile	33.9	56.3	22.4
4	México	35.3	56.5	21.2
5	Guyana	19.5	40.5	20.9
Países con el desempeño más precario				
No.	**País**	**2016**	**2020**	**Δ Cambio**
1	Granada	19.1	27.0	7.9
2	Venezuela	24.6	32.3	7.8
3	El Salvador	23.8	31.3	7.5
4	Dominica	21.5	28.9	7.4
5	Haití	19.2	24.5	5.4

Fuente: Elaboración propia.

Respecto de las dimensiones de Política y Estrategia de Seguridad Cibernética y Marcos Legales y Regulatorios, destaca el liderazgo de Uruguay, Colombia y Chile, los cuales han manejado una política consistente y continua de proyecto como el Fortalecimiento de la Ciberseguridad en Uruguay, la aprobación de la segunda ENCS de Colombia y la promulgación

de la Ley Marco de Ciberseguridad en Chile, así como la mejora y establecimiento del Sistema Nacional de Ciberseguridad, de dicho país.

En menor medida se destaca lo realizado por México con la creación de su primer ENCS, en 2017, y la presentación de tres propuestas legislativas vinculadas a ciberseguridad en el gobierno de México durante 2018 y 2019. Lo mismo para Guyana, que en 2018 promulgó una legislación sobre delitos cibernéticos y en 2019 creó un Grupo de Trabajo de Estrategia Nacional de Ciberseguridad. En relación a los países que menos han avanzado en acciones de política destaca la situación de Granada, Venezuela, El Salvador, República Dominicana y Haití, que al día de hoy no cuentan con una ENCS. En el cuadro 3 se presenta un avance de este conjunto de naciones en el período 2016–2020.

Cuadro 3 Países con el mejor desempeño y desempeño más precario en las dimensiones de Política y Estrategia de Seguridad Cibernética y Marcos Legales y Regulatorios OEA & BID (2020).

Política y Estrategia de Seguridad Cibernética					**Marcos Legales y Regulatorios**				
Países con el mejor desempeño					**Países con el mejor desempeño**				
No.	País	2016	2020	Δ Cambio	No.	País	2016	2020	Δ Cambio
1	Uruguay	52.0	70.7	18.7	1	Uruguay	32.0	72.0	40.0
2	Colombia	44.0	76.0	32.0	2	Colombia	36.0	70.0	34.0
3	Chile	46.7	62.7	16.0	3	Chile	42.0	86.0	44.0
4	México	40.0	52.0	12.0	4	México	38.0	76.0	38.0
5	Guyana	37.3	53.3	16.0	5	Guyana	38.0	78.0	40.0
Países con el desempeño más precario					**Países con el desempeño más precario**				
No.	País	2016	2020	Δ Cambio	No.	País	2016	2020	Δ Cambio
1	Granada	18.7	21.3	2.7	1	Granada	22.00	46.00	24.00
2	Venezuela	20.0	21.3	1.3	2	Venezuela	24.00	46.00	22.00
3	El Salvador	18.7	20.0	1.3	3	El Salvador	20.00	46.00	26.00
4	Dominica	18.7	20.0	1.3	4	Dominica	26.00	46.00	20.00
5	Haití	20.0	21.3	1.3	5	Haití	18.00	30.00	12.00

Fuente: Elaboración propia con base en OEA & BID (2016;2020).

En lo que respecta a nuestro análisis realizado con base al NCSI (2019) y los informes de la OEA & BID (2016;2020) se ha verificado la hipótesis central de la investigación, destinada a probar que América Latina detenta carencias en el desarrollo de cibercapacidades y una política nacional de ciberseguridad que edifique una ENCS apta para encarar los retos y amenazas provenientes del ciberespacio, con el fin de salvaguardar su seguridad nacional y política exterior. Por último, según expresan Moreno, Albornoz & Maqueo (2020), América Latina es una región que se encuentra en una fase primeriza de construcción de sus ENCS y el desarrollo de sus cibercapacidades para combatir amenazas provenientes del ciberespacio; tarea frente a la cual existen múltiples áreas de oportunidades que los países de la región deben atender en el futuro cercano.

Conclusiones

En la actualidad el ciberespacio se ha transformado en una nueva arena de interacción, cooperación y conflicto de la política global. Lo anterior se ha demostrado en los hechos, con eventos como la securitización de Internet y eventos globales que han demostrado el potencial del ciberespacio para influir en la realidad internacional, como el ciberataque de Tallin, en 2007, o el hackeo a las agencias gubernamentales de Estados Unidos detectado en 2020. Del mismo modo, el campo de la ciberseguridad ha despertado el interés de la academia y teóricos de las relaciones internacionales, siendo el paradigma neorrealista, constructivista, así como la Teoría de la Guerra, las que han promovido la noción del ciberpoder y los vínculos de la problemática del ciberespacio con la seguridad nacional y la política exterior.

En ese sentido, destaca cómo en la última década las amenazas y riesgos provenientes del ciberespacio se han incrementado a un ritmo acelerado, transformando a la ciberseguridad en un tema central de la política de seguridad nacional, así como factor de trascendencia de la política exterior de los Estados-Nación. En el ámbito global, destaca el papel de organismos como la ITU al crear la AGCS que marca una línea de acción de los países del mundo para desarrollar una política de ciberseguridad y crear cibercapacidades para enfrentar los riesgos provenientes del ciberespacio. A razón de la AGCS se han estructurado importantes métricas como el GCI (2018) y el NCSI (2020), que permiten ver el avance de los países en el nivel individual y grupal, y permiten ver la brecha regional que detenta Latinoamérica en la construcción de cibercapacidades respecto de otro conjunto de naciones y regiones del mundo, como los países integrantes de la OTAN, Europa o Asia. También

es importante destacar el liderazgo de la OEA & BID (2016; 2020) con la publicación en el ámbito latinoamericano, que para el período 2016–2020 permiten analizar el grado de avance de los países y mejoría en el desarrollo de su política de ciberseguridad en dimensiones como Política y Estrategia de Seguridad Cibernética y Marcos Legales y Regulatorios. No obstante, también destaca el uso del NCSI (2016), que a través de su métrica permite identificar ámbitos de oportunidad y mejora que deben atender los países de América Latina para construir una política de ciberseguridad capaz de enfrentar el contexto actual global de ciberseguridad.

Derivado de nuestro análisis de los dos instrumentos, podemos expresar que los estudios de la OEA & BID (2016; 2020) nos permiten observa una América Latina con países cada vez más integrados en las dinámicas mundiales de ciberseguridad, así como con la AGCS de la ITU. No obstante, el análisis dinámico de los 32 países de la región, para el período 2016–2020, presentan igualmente una tremenda heterogeneidad en las acciones individuales para la construcción de una política nacional de ciberseguridad, con naciones que avanzan a grandes pasos (Chile, Uruguay y Colombia), mientras otros se mantienen en una casi total inercia (El Salvador, República Dominicana, Haití). Asimismo, a pesar de que el tema de la creación de ENCS y legislaciones para la regulación del ciberespacio es uno de los ámbitos en el cual América Latina presenta un avance constante y paulatino, el ENCS (2019) devela cómo los países se mantienen severamente rezagados en aspectos como la delimitación de ciberamenazas para la seguridad nacional, el desarrollo de protocolos para atender una crisis cibernética que afecte a la Infraestructura Nacional Crítica y al Estado-Nación, o en crear aportes de ciberseguridad para la comunidad internacional. Sin embargo, es una tarea y labor de las naciones de la región transformar estas debilidades en áreas de oportunidad y mejora en aras de encarar los retos y amenazas provenientes del ciberespacio.

Bibliografía

Aguilar-Antonio, J.M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO. *Revista Latinoamericana de Estudios de Seguridad*, (25), pp. 24-40.

Benítez, R. (1986). El pensamiento militar de Clausewitz. *Revista Mexicana de Ciencias Políticas y Sociales*, 126, pp. 97-123.

CCDCOE Tallin (2020). Strategy and Governance. Cooperative Cyber Defence Centre of Excellence, Recuperado de: https://bit.ly/37I0jrm

Choucri, N.; Madrick, S., y Ferwerda, J. (2013). Institutional Foundations for Cyber Security: Current Responses and New Challenges. MIT. Massachusetts, EUA, 27 pág.

Cybersecurity Ventures (2016). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Recuperado el 12 de enero de 2020 de: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Deibert, R. & Rohozinski, R. (2010). Beyond Denial: Introducing Next Generation Information Access Controls, en Deibert, R.; Palfrey, J.; Rohozinski, R. & Zittrain, J. (eds.) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press: Cambridge, pp. 3-13.

Digital Attack Map (2021). Recuperado el 12 de enero de 2021de: https://www.digitalattackmap.com/

Edmunds, T. (2014). Complexity, strategy and the national interest. *International Affairs* 90(3), pp. 525-539

Firdous, M. (2020). Cyber Warfare and Global Power Politics. *CISS Insight Journal*, 8(1), pp. 71-93.

GCI (2018). Global Cybersecurity Index. International Telecommunication Union. Recuperado el 12 de enero de 2021 de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Gray, C. & Sloan, G. (1999). *Geopolitics, Geography and Strategy*. Routledge Taylor & Francis Group, Oxfordshire: United Kingdom, 298 pág.

Hackmageddon (2020). Cyber Attacks Statistics. Recuperado el 12 de enero de 2020: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Hughes, R. (2010). A treaty for cyberspace. *International Affairs*, 86(2), pp. 523-541.

Kapersky (2020). Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado el 12 de enero de 2020: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Kello, L. (2017). *The virtual weapon and international order*. Reino Unido: Yale University Press, 320 pág.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), pp. 7-40.

Klimburg, A. (2012.). National Cyber Security Framework Manual. Tallinn; Estonia: NATO CCD COE Publication.

Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem", en Kramer, F.; Starr, S.; Wentz, L. *Cyberpower and National Security*. Washington D.C.: National Defense University Press, pp. 25-42.

Martín, P. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. Instituto Español de Estudios Estratégicos, 8.

Moreno; J.; Albornoz, M., y Maqueo, M. (2020). Ciberseguridad en América Latina. Revista de Administración Pública INAP. Ciberseguridad Nacional; 148 (1): pp.23-46.

NCSI (2019). National Cyber Security Index. E-Governance Academy, Recuperado el 12 de enero de 2021 de: https://ega.

ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Newmeyer, P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*; 1(3): pp. 9-19.

Nye, J. (2014). The regime complex for managing global cyber activities. Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 32 pág.

Nye, J. (2010). Cyber power. Harvard University, Cambridge MA Belfer Center for Science and International Affairs.

OEA & BID (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 204 pag. Recuperado el 12 enero de 2021 de: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

OEA (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. 186 pág. Recuperado el 12 de enero de 2021 de: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OEA & BID (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? 193 pág. Recuperado el 12 enero de 2021 de: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

OEA/Symantec (2014). Tendencias de Seguridad Cibernética en América Latina y el Caribe. 100 págs. Recuperado el 12 de enero de 2021 de: https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

Palfrey, J. (2010). Four Phases of Internet Regulation. Social Research, 77(3): pp. 981-996.

Samaan, J. (2010). Cyber command: The rift in US military cyber-strategy. *The RUSI Journal*, 155(6): pp. 16-21.

Sheldon, J. (2012). "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, vol. 5, no. 2, 2011, pp. 95–112.

Sicherheitstacho (SF). Overview of Current Cyber Attacks. Deutsche Telekom. Recuperado el 12 de enero de 2021 de: https://www.sicherheitstacho.eu/start/main

Singer, P. y Friedman, A. (2014). *Cyber Security and Cyber War*. Oxford, Reino Unido: Oxford University Press, 321 págs.

Stanković, N. (2019). The conceptual analysis of identities and interests in the thought of Alexander Wendt. *Politeia*, 9(18), pp. 37-154.

Starr, S.H. (2009). Toward a preliminary theory of cyberpower, en Kramer, F.; Starr, S. & Wentz, L. *Cyberpower and National Security*. Washington D.C.: National Defense University Press, pp. 43-88.

Take, I. (2012). Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS. *Regulation & Governance*, 6(4): pp. 499-523.

Van Creveld, M. (2002). The transformation of war revisited. *Small Wars and Insurgencies*, 13(2), pp. 3-15.

Van Creveld, M. (1991). *The transformation of war: the most radical reinterpretation of armed conflict since Clausewitz*. Washington D.C.: Free Press, 254 pág.

Wendt, A. (1994). Collective identity formation and the international state. *American Political Science Review*, pp. 384-396.

Zittrain, J. & Palfrey, J. (2007). *Access denied: the practice and policy of global Internet filtering*. United Kingdom: Oxford Internet Institute, 80 pág.