La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas

The Cyber Security Gap in Latin America Against the Global Context of Cyber Threats

JUAN MANUEL AGUILAR ANTONIO

Universidad Nacional Autónoma de México, México

RESUMEN: La presente investigación parte de la hipótesis de que los gobiernos de América Latina y el Caribe están rezagados en la construcción de ciber capacidades de defensa para enfrentar el contexto actual e internacional de ciber amenazas, respecto a los países miembros de la Organización del Tratado del Atlántico Norte (OTAN), tanto en el plano de organización, como en el individual. Para probar este enunciado el texto se divide en seis secciones. En la primera se presenta el entorno global amenazas provenientes de ciberespacio, las pérdidas económicas que sufren gobiernos y empresas según informes de firmas de seguridad informática como Kaspersky, Microsoft, Verizon e International Business Machines Corporation (IBM). En la segunda parte, se aborda el proceso de securitización del internet, la inmersión de la ciberseguridad en los estudios de seguridad nacional, así como la definición de ciber capacidades y delimitación de amenazas al Estado-Nación desde el ciberespacio. En la tercera se aborda la trayectoria de la OTAN como organización en el desarrollo ciber capacidades en los últimos veinte años. En la cuarta parte, se analiza desde el nivel individual un conjunto de Estrategias Nacionales de Ciberseguridad (ENCS) de los países y aliados de la OTAN, de las cuales se extraen sus principales elementos y se esquematiza su anatomía general. En la sexta parte, se presenta una aproximación a diferentes entornos regionales o globales de ciberseguridad con base a mediciones del *Global Cybersecurity Index* (GCI), de la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), y el *National Cyber Security Index* (NSCI) de la *E-Governance Academy* de Estonia. En la quinta sección se presenta el contexto de la ciberseguridad en América Latina y el Caribe, según estudios realizados por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), así como firmas privadas de ciberseguridad. En la sexta, se presenta de manera breve dos estudios de caso de México, del bienio 2019-2020, que representan la falta de madurez de su ENCS y desarrollo de ciber capacidades, aspecto que comparte con la mayoría de los países de América Latina y el Caribe. Por último, se presentan unas breves conclusiones sobre los aspectos a fortalecer por la región.

PALABRAS CLAVE: Seguridad Cibernética, Seguridad del Estado, Estrategia Nacional de Ciberseguridad.

ABSTRACT: This research is based on the hypothesis that the governments of Latin America and the Caribbean are lagging behind in the construction of cyber defense capabilities to face the international context of cyber threats, with respect to the member countries of North Atlantic Treaty Organization (NATO), both in the organizational plan, as in the individual. To prove this statement, the text is divided into six sections. The first part presents the global environment of cyber threats, the economic losses suffered by governments and companies according to reports from information security firms such as Kaspersky, Microsoft, Verizon and International Business Machines Corporation (IBM). The second part presents the internet securitization process, the immersion of cybersecurity in national security studies, and the definition of cyber capabilities and the delimitation of threats to the Nation-State from cyberspace are addressed. The third part shows the trajectory of NATO as an organization in the development of cyber capabilities in the last twenty years. In the fourth part, a set of National Cybersecurity Strategies (ENCS) of NATO countries and allies is analyzed from the individual level, from which their main elements are extracted and their general anatomy is outlined. In the sixth part, an approach to different regional or global cybersecurity environments is presented based on measurements of the Global Cybersecurity Index (GCI), of the International Telecommunications Union (ITU), and the National Cyber Security Index (NSCI) of the Estonian E-Governance Academy. The fifth section presents the context of cybersecurity in Latin America and the Caribbean, according to studies made by the Inter-American Development Bank (IDB) and the Organization of American States (OAS), as well as private cybersecurity firms. In the sixth, two case studies of Mexico, from the 2019-2020, are briefly presented, which represent the lack of maturity of its ENCS and development of cyber capabilities, an aspect that it shares with most of the countries of Latin America and Caribbean. Finally, brief conclusions are presented on the aspects to be strengthened by the region.

KEYWORDS: Cybernetics Security, State security, Foreign Policy.

Recibido: 13 de mayo de 2020. Aceptado: 21 de septiembre de 2020.

ISSN: 2444-6157. DOI: http://dx.doi.org/10.18847/1.12.2

Introducción

La ciberseguridad es un tema que hizo presente su importancia en la seguridad nacional de los Estados-Nación a finales del siglo XX e inicios del XXI. En 1999, la OTAN reconoció al ciberespacio como un nuevo dominio para perseguir sus misiones de defensa colectiva, después de haber sufrido sus primeros ciberataques durante una Operación de Fuerza Aliadas en Kosovo (Healey & Van Bochoven, 2012). Sin embargo, fue con el ciberataque de Tallin, Estonia (2007), que la necesidad de crear una Estrategia Nacional de Ciberseguridad (ENSC), que forme parte de la estrategia global de Seguridad Nacional, se transformó en una exigencia para los gobiernos del mundo (Klimburg, 2012: 27-29). Para 2011, un total de veinte países de Europa y América del Norte, ya contaban con su primera versión de este documento, en el que presentaban una definición de ciberseguridad y una delimitación de las ciberamenazas con capacidad de vulnerar la integridad del Estado-Nación (Lindstrom & Luiijf, 2012: 53-58).

En la actualidad, de acuerdo al apartado de *Estrategia y gobernanza*, de la biblioteca digital del Centro de Excelencia de la Ciberdefensa Cooperativa (*CCDCOE Tallin* por sus siglas en inglés), centro integrado por 28 países, acreditado por la OTAN y a su servicio, que presenta estrategias de seguridad y defensa nacional, ENCS, legislaciones nacionales, y declaraciones de derecho internacional vinculadas a la seguridad cibernética, un total de 77 naciones del mundo han creado documentos de 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, países de África, América Latina, el Caribe, Asía y Oceanía (CCDCOE Tallin, 2020).

Sin embargo, las amenazas a la seguridad nacional y los retos a enfrentar en el ciberespacio, avanzan más rápido que la capacidad de acción de los gobiernos. Tan solo en 2017, se presentaron 1 579 brechas de información en el sector financiero de los Estados Unidos, las cuales aumentan a una tasa promedio del 44.6% anual (GBA & ITRC, 2018: 2-3). Al momento que se escribe este texto, de acuerdo a *T-Sec Radar* de *Deutsche Telekom* detecta que se dan 60 312 ciberataques cada minuto (Sicherheitstacho, 2019). Por su parte, la plataforma Digital Attack Map (2019), que lleva el registro diario de los ataques DDoS[1] en el mundo y detecta su origen y país destino, estima que se realizaron más de 8 000 diarios durante el último año.

Frente a este contexto, las naciones de Europa y Norteamérica (con especial énfasis a las naciones miembros o aliadas de la OTAN) han priorizado la securitización del ciberespacio, desde el enfoque de seguridad del Estado-Nación. Mientras que otras naciones, como las América Latina, África, Medio Oriente, y en menor medida Asía, se encuentran en el proceso de desarrollo de legislaciones y documentos nacionales vinculados a la ciberseguridad. En ese sentido, la presente investigación parte de la hipótesis de que América Latina y el Caribe están rezagados en la construcción de capacidades para enfrentar el contexto actual e internacional de ciberamenazas respecto a los países miembros de la OTAN, tanto en el plano como organización, como en el individual, enunciado central que se busca probar a través del desarrollo de este documento.

[1] *DDoS* son las siglas en inglés de *Denial of Distributed Service* o "Denegación de Distribución de Servicio", una de las técnicas de ataques a través del ciberespacio más utilizada por *hackers* o *crackers*. Su finalidad es hacer inaccesible o inoperable una red de internet o sistema computacional a sus propietarios o usuarios legales.

CONTEXTO GLOBAL DE CIBERAMENAZAS

Durante 2018, el gasto mundial en productos y servicios de seguridad de la información y ciberseguridad superó los 114 mil millones de dólares, lo que representó un incremento del 12.4 por ciento, con relación al 2017. Si bien este incremento derivado de los costos para gobiernos, empresas o individuos ostentó una tasa de crecimiento alta, es importante mencionar que en 2004, la firma *Gartner, Inc.*, centrada en consultoría e investigación de tecnologías de la información (TIC´s), expresó que el mercado global de ciberseguridad representaba un total 3.5 mil millones de dólares, lo que implica que en tan solo 15 años, la necesidad de servicios de ciberseguridad creció 35 veces (Morgan, 2019).

Asimismo, con base en el informe de la firma de ciberseguridad Verizon (2020) se presentaron al menos un total de 157 525 incidentes vinculados a brechas de información en al menos 16 diferentes industrias en todas las regiones del mundo. Mientras que el informe X-Force IRIS, de IBM Security (2020), estima que el costo destructivo de los ataques de malware a empresas multinacionales incurrió durante 2019 en un costo de 239 millones de dólares por incidente, en promedio. Conjuntando todo este tipo de ciberamenazas el portal *Cybersecurity Ventures* predice que el gasto global en productos y servicios de ciberseguridad superará el billón de dólares en gasto acumulado durante el período de 2017 a 2021 (Morgan, 2019).

Por su parte, 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. Dicha cifra fue superior en 34 por ciento a los eventos registrados en 2018 (1 337). Y 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 cibercrimen (83.96% sobre 100%), ciberguerra (1.55%), hacktivismo (3.05%) y ciberespionaje (11.21%), categorías que competen a intentos de vulneración de sistemas informáticos, tecnologías de la operación y bases de información de gobiernos nacionales.

En este contexto, AON (2019) expresa que los gobiernos alrededor del mundo ejercieron aproximadamente un trillón de dólares en gastos de ciberdefensa en 2019, dónde los más afectados fueron los sectores industriales y las actividades económicas vinculadas al internet o servicios digitales, que enfrentaron fuertes pérdidas y riesgos, dado que los gobiernos nacionales no priorizaron la ciberseguridad. Sobre este dato la *Encuesta de Percepción de Riesgo Cibernético Global*, de la empresa *Microsoft*, expresó que solo 28% de las empresas mundiales líderes en TIC´s consideran adecuadas las regulaciones o leyes gubernamentales para mejorar la ciberseguridad de cada país. A la par, las entidades privadas y gubernamentales consideraron en 2019 que el principal riesgo percibido en el ciberespacio son las ciberamenazas (46%), con el potencial de infringir daños a una nación en esferas como la incertidumbre económica, daño industrial, actividad criminal, fraude, etc. (Kaspersky, 2020: 6), como se muestra en la figura 1.

Figura 1. Seguridad en TIC´s y riesgos percibidos en el ciberespacio

Fuente: Kaspersky (2020)

Datos como los anteriores, muestran la cada vez mayor responsabilidad y dirección del Estado-Nación en la construcción de una ENCS que garantice la seguridad nacional, en un entorno cada vez más complejo, diverso y creciente de ciberamenazas. En ese sentido, se hace necesario presentar en qué momento la securitización del internet y la ciberseguridad se transforman en una esfera de influencia de los gobiernos, así como la trayectoria que ha construido la OTAN, como organización en el desarrollo de cibercapacidades.

SECURITIZACIÓN DEL INTERNET, INCLUSIÓN DE LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL Y DEFINICIÓN DE CIBERAMENAZAS

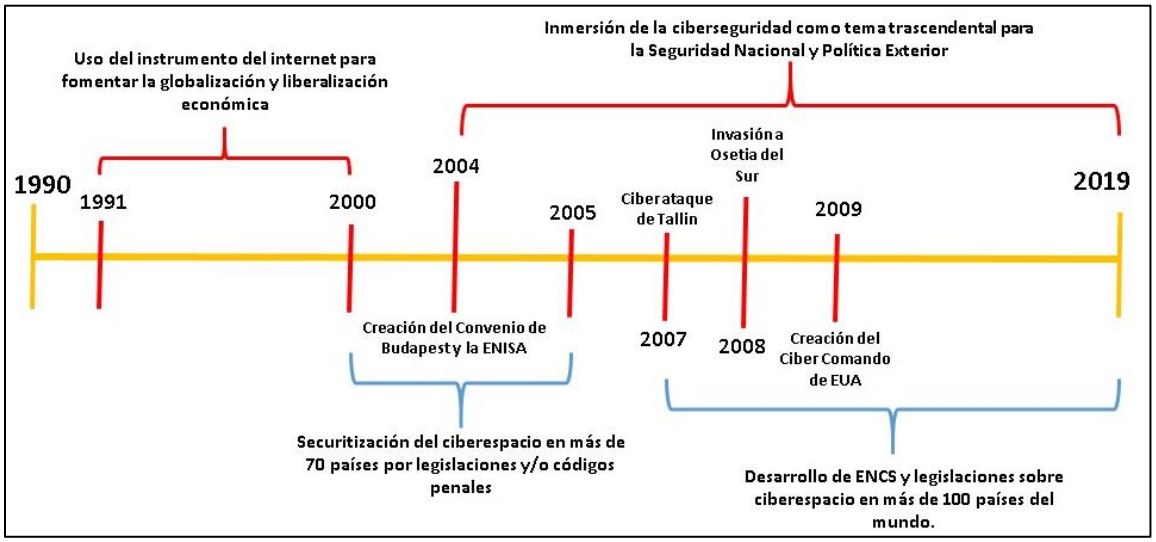
Para Palfrey (2010: 981-993) la securitización del internet fue una consecuencia del proceso de globalización y liberalización económica, que aconteció en la última década del siglo XX. En ese sentido, la primera penetración del Estado-Nación en su securitización se da durante los años 2000 - 2005 (Palfrey, 2010: 989-991). En esta primera experiencia, la inmersión de los gobiernos en el ciberespacio se da con la regulación, administración, e incluso, bloqueo de actividades y expresiones en el internet. Respecto a esto, Deibert et al. (2008: 16-19) documentaron que en ese período al menos 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. Con esto, se consolidó un proceso de securitización, que puso énfasis en crear nuevas definiciones para delimitar delitos o actividades ilícitas que se realizaran a través del ciberespacio.

En los hechos, más de 100 países establecieron en sus códigos de justicia y sistema penales definiciones sobre los cibercrímenes y delitos, a la par que 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 su regulación, hasta la creación del Convenio de Budapest, en 2004, y es el más grande intentó

de una armonización de ciberdelitos (Klimburg; 2012; Palfrey, 2010; Take, 2012). Más tarde surgió el primer conjunto de instituciones para prevenir ciberincidentes de manera multilateral, entre los que destaca la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés), y el Cibercomando de Estados Unidos (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 la seguridad nacional de un Estado-Nación. Estos eventos transformaron a la ciberseguridad en un aspecto clave de la estrategia de seguridad nacional. Y es precisamente a raíz de los hechos de Tallin que todos los países de la OTAN, y posteriormente del resto del mundo, comenzaron a crear sus primeras versiones de una ENCS, con lo que se estima que más de cien países, entre 2009 y 2020, crearon legislaciones o una ENCS cómo se muestra en la figura 2.

Figura 2. Fases de regulación del internet e inclusión de ciberseguridad en seguridad nacional



Fuente: Elaboración propia con base en Palfrey (2010)

En la actualidad, la materialización de ciberincidentes es una constante de la rutina diaria y cotidianeidad de gobiernos, empresas o individuos. A la par que diversos tipos y modalidades de ciberataques como el *pishing*, *watering-hole*, ramsonware o ataques DDoS forman parte de las preocupaciones de entidades o personas que utilizan sistemas informáticos o dispositivos de *Internet de las Cosas.* No obstante, es importante mencionar que cada clase de ciberataque corresponde a diferentes niveles de amenazas y grado de afectación, a la par de que para esta investigación son de particular interés aquellos que tengan un grado severo o de emergencia sobre la seguridad nacional. Sobre lo anterior, Noonan (2016) expresa que los estándares de riesgo cibernético de la *Directiva de política presidencial sobre la coordinación de incidentes cibernéticos de los Estados Unidos* proporcionan un estándar claro sobre los niveles de riesgo cibernético vinculados a

ciberamenazas, en relación a los efectos que tengan estos en el ciberespacio y el espacio físico, los cuales se presentan en la figura 3.

Figura 3. Niveles de riesgos de la Directiva de política presidencial sobre la coordinación de incidentes cibernéticos de los Estados Unidos

	Definición General
Nivel 5 Emergencia (Negro)	Representa una amenaza inminente y de gran escala a los servicios de provisión de infraestructura crítica, estabilidad del gobierno, o la vida de las personas
Nivel 6 Severo (Rojo)	Probable resultado en un impacto significativo en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, o libertades civiles.
Nivel 3 Alto (Naranja)	Probable resultado en un impacto demostrable en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 2 Medio (Amarillo)	Puede impactar en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 1 Bajo (Verde)	Poco probable que impacte en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 0 Línea base (Blanco)	Sin fundamento o evento sin consecuencias.

Acciones Observadas	Definición General
Efectos	**Causa consecuencias físicas.** **Daña computadoras y redes de *hardware***
Presencia	**Corrompe o destruye datos e información.**
Compromiso	**Daña disponibilidad de acceso a sistemas o servicios.** **Roba información sensible.** **Comete un crimen financiero.**
Preparación	**Cauda molestia negando acceso a servicio o interrumpiéndolo.**

Fuente: Elaborado con base en Noonan (2016) y White House PPD (2016)

De esta forma, se expresa que los diferentes tipos de *malwares* o ciberarmas pueden ser utilizados a diferentes escalas, ya que un ataque DDoS puede afectar a un sistema informático de un individuo, hasta bloquear completamente una red gubernamental y un sistema bancario, como lo fue el caso del ciberataque de Estonia, en 2007 (Chauvin, 2016). O una brecha de información puede afectar desde la reputación de una persona, hasta causar tensiones diplomáticas entre dos gobiernos, como fue el caso de los cables de Wikileaks sobre México del Cablegate de 2011 (Benítez, 2011). Por lo cual el grado de afectación de los diferentes tipos y modalidades de ciberataques no están condicionados por el medio (*pishing*, *watering-hole*, ramsonware, etc.), sino por los efectos que tienen en esferas y elementos como la infraestructura crítica, seguridad pública o libertades civiles.

En ese sentido, los principales niveles de securitización y riesgo en temas de ciberseguridad que son del interés y preocupación de esta investigación se centran en aquellos que afectan esferas como la seguridad nacional, la estabilidad política y las relaciones diplomáticas, es decir del *Nivel 2 Medio* al *Nivel 5 Emergencia*, presentados en la figura 3, que afectan la estabilidad, seguridad e interés nacional del Estado-Nación. En este punto se

hace necesario definir qué se entiende por una cibercapacidad, ante esto se expresa este concepto representa un patrón de aprendizaje por parte de los gobiernos y Estados-Nación que les permite desarrollar capacidades de resiliencia y disuasión ante un ciberincidente o ciberataque. Por resiliencia, en su noción clásica, se define a la capacidad de previsión, reconocimiento y anticipación de defensa, de un sistema y organización, para defenderse frente a una forma de riesgo cambiante, antes de que este tenga consecuencias o costos adversos (Haimes, 2006). En ese sentido, la resiliencia supone un conjunto de capacidades, acciones y protocolos que desarrolla una entidad, que se enfrenta a riesgos y amenazas constantes, que sabe que estos evolucionan y se transforman como acontece en el internet y el ciberespacio.

Por su parte, la disuasión surge como noción de la política de defensa y seguridad nacional de los Estados Unidos de América, en el marco de la Guerra Fría (Haffa Jr., 2018). Por lo que Mearsheimer (1985) define a la disuasión convencional como todas las acciones que ejecuta un Estado-Nación para persuadir a un adversario de no iniciar una acción en su contra, dado que los costos a recibir superan los beneficios que pueden obtenerse. Por lo cual el desarrollo de cibercapacidades implica poseer estas dos habilidades para prevenir un ciberincidente, mantener operaciones ante un ciberataque y enfrentar el contexto global de riesgos en el ciberespacio.

LA TRAYECTORIA DE LA OTAN COMO ORGANIZACIÓN EN EL DESARROLLO DE CIBERSEGURIDAD

La trayectoria de la OTAN en el desarrollo de cibercapacidades empieza en 1999, derivado de su intervención militar en Kosovo. A raíz de este evento la organización reconoció al ciberespacio como un nuevo dominio de defensa colectiva. En dicha operación sufrió sus primeros ciberataques a varios de sus portales de internet, que fueron atacados por hackers serbios, chinos y rusos. Como resultado, la OTAN y varios sitios de gobiernos de Estados miembros fueron afectados y no estuvieron disponibles durante períodos de tiempo significativos (Healey & Van Bochoven, 2012: 2).

A pesar de la afectación, los agresores no lograron adquirir información confidencial o impactar en las operaciones. No obstante, el organismo tomó acciones frente a los incidentes y en 2002, en su Cumbre anual en Praga, creó tres instancias para atender el tema: 1) su primer Programa de Ciberdefensa, 2) el Centro de Capacidad de Respuesta a Incidentes informáticos (NCIRC, por sus siglas en inglés) y 3) la Agencia de Servicios de Comunicación e Información. Dichas instituciones tenían como tarea principal proteger las redes y sistemas de internet de la organización, mientras que la protección de los sistemas informáticos nacionales de los países integrantes se consideraba responsabilidad de los países miembros (Szentgáli, 2013).

No fue hasta 2007, que la política de ciberdefensa conjunta se transformó a consecuencia de los ciberataques de Estonia (2007), adjudicados a Rusia, que son considerados como el detonante real del desarrollo de una política de ciberdefensa de la organización (Chauvin, 2016). Dado que a consecuencia de este evento Estonia solicitó apoyo de emergencia a la alianza, mas ésta no contaba con procedimientos para atender ciberataques. En consecuencia, la OTAN desarrolló una doctrina de defensa cibernética y una estrategia cibernética integral que le permitiera reaccionar de forma eficaz a los ciberataques de los países miembros.

Intenciones que se intensificaron tras el conflicto entre Rusia y Georgia, en 2008, dado que una vez más se presentaron ciberataques adjudicados al Kremlin que potencializaron los esfuerzos para el desarrollo de cibercapacidades de defensa como organismo y entre sus integrantes (Hughes, 2009).

Para la Cumbre de Bucarest, en 2008, la alianza estableció dos importantes instituciones de defensa: 1) el CCDCOE Tallin, con el fin de estar al servicio de la OTAN y mejorar su conocimiento en cuestiones de ciberseguridad, así como desarrollar una doctrina y estrategia cibernéticas a largo plazo. Y 2) la Autoridad de Gestión de Defensa Cibernética (CDMA, por sus siglas en inglés), con el objetivo de ayudar a los Estados miembros a mejorar, coordinar y revisar sus propias capacidades nacionales de ciberdefensa. Más tarde, en 2010, la alianza adoptó un nuevo concepto estratégico que reconoció a los ciberincidentes y ciberataques como uno de sus principales desafíos (Cavelty, 2012: 5-8).

Para 2011 la OTAN crearía su segunda política, concepto y plan de ciberdefensa, el cual estableció una visión de esfuerzos coordinados en defensa cibernética en toda la alianza y un plan para su implementación en aras de mejorar sus capacidades de defensa colectiva y gestión de crisis, entre sus metas se encontraban: 1) centrarse en la prevención, resiliencia y defensa de activos cibernéticos críticos para la OTAN y sus integrantes, 2) desarrollar sólidas capacidades de ciberdefensa y centralizar la protección de las propias redes de la OTAN. Así como 3) establecer requisitos mínimos para la ciberdefensa de las redes nacionales críticas para el organismo. También, indicó que la organización tenía la facultad de brindar asistencia a las naciones integrantes para lograr un nivel mínimo de ciberdefensa y reducir vulnerabilidades de las infraestructuras nacionales críticas (Rühle, 2011).

A partir de ese punto, y durante 2012 y 2016, la alianza se centró en asistir técnica y estratégicamente a los Estados miembros de la organización para ajustar su ENCS a los estándares mínimos de la organización, a la par de apoyar en el desarrollo de sus cibercapacidades, militares y no militares, necesarias para cumplir con los objetivos de seguridad y defensa acordados por la alianza. También, incorporó al NCIRC al Proceso de Planificación de la Defensa de la OTAN y en vista de estas acciones los Estados miembros encargaron a la OTAN el desarrollo de una política de ciberdefensa en materia de defensa colectiva, asistencia a integrantes y aliados, consideraciones legales y cooperación de la industria, que se presentó en 2016 durante la Cumbre de Gales y está vigente en la actualidad. Por último, el último gran paso de la alianza se dio en la Cumbre de Varsovia (2016) en la que el organismo y los países integrantes reconocieron al ciberespacio como un dominio estratégico de la defensa junto al aire, tierra y mar, vital para la operación de sus misiones y operaciones (Chauvin, 2016).

El desarrollo individual de cibercapacidades de países integrantes de la OTAN y la anatomía de sus ENCS

En el apartado anterior, se presentó como la OTAN hizo a la ciberseguridad y el desarrollo de cibercapacidades una de sus prioridades como organización. En este apartado, se presenta el desarrollo individual de la definición de ciberseguridad, delimitación de ciberamenazas y

el desarrollo de las ENSC de una selección de sus países miembros y aliados estratégicos.[2] En ese sentido, se específica que se revisaron un total de diez ENCS[3] de países miembros y aliados estratégicos de la OTAN. Respecto a la selección de estos documentos se expresa que corresponde al hecho de que estos eran los únicos que contaban con traducción oficial al inglés en la biblioteca digital del CCDCOE Tallin (2020), al momento de la realización de esta investigación. De esta forma en la tabla 1, se presenta un resumen y selección de cuatro ENCS con la definición de ciberseguridad y delimitación de ciberamenazas.

Tabla 1. Definición de ciberseguridad y ciberamenazas en una muestra de países de la OTAN

País	Definición de Ciberseguridad	Ciberamenazas
Alemania	*"…* [la] *ciberseguridad global se conforma de la ciberseguridad civil y militar, esta es el objetivo deseado de la situación de seguridad informática, en la que los riesgos del ciberespacio global se han reducido a un mínimo aceptable. … la seguridad cibernética en Alemania es el objetivo deseado de la situación de seguridad de TIC´s, en la que los riesgos en el ciberespacio se han reducido al mínimo* (Federal Government Germany -FG Germany-, 2016: 38)*."*	Ciberamenazas de dos tipos según FG Germany (2016: 34-46): 1. Civil: uso fraudulento de datos, espionaje industrial, daño a de sistemas informáticos de rutas de comercio y transporte, cibercrimen. 2. Militar: daños a INC, amenazas hibridas, afectación de sistemas de comunicación, cadenas de suministro o suministro de materias y energía.
España	*"*[ciberseguridad es] *el uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques que afecten al estado español, a este fin debe servir la Política de Ciberseguridad Nacional* (Departamento de Seguridad Nacional, 2013)*."*	Según Departamento de Seguridad Nacional -DSN- (2019) Entre las amenazas se encuentran: • Estados extranjeros, causas técnicas, fenómenos naturales, hacking, conflictos, crimen organizado, amenazas internas, terrorismo, sabotaje, hacktivistas, individuos aislados, delincuencia, espionaje, organizaciones terroristas.
Canadá	"*La ciberseguridad es la protección digital de la información y la infraestructura que reside en direcciones de seguridad cibernética, atender los desafíos y amenazas del ciberespacio para asegurar los beneficios y oportunidades de la vida digital* (Canadian Department for Public Safety -CDPS-, 2010)."	Cibercrimen en dos categorías según CDPS (2010): 1. *Tradicional:* fraude, abuso, acoso y explotación sexual a través del internet. 2. *Crimen de objetivos tecnológicos:* hackeo, esquemas de fraude de ramsonware, ataques DDoS, etc. Ciberamenazas avanzadas: • Espionaje y ciberexplotación, robo de información confidencial, seguridad nacional o propiedad intelectual del Estado, ataque a Infraestructura Crítica Nacional.

[2] Por aliados estratégicos se entiende a los 17 países considerados *Major non-NATO ally* o Aliado Importante no-OTAN, delimitación establecida por el Departamento de Estado de EUA y representa un conjunto de naciones que mantienen un trabajo conjunto con las fuerzas armadas de los Estados Unidos pero no son miembros de la organización (US Deparment State, 2020).

[3] Los diez países que se revisaron fueron: Canadá, Turquía, Alemania, Países Bajos, Estonia, Reino Unido, Estados Unidos, España, Australia e Israel. La selección se hizo a través del apartado de Estrategia y Defensa del CCDCOE Tallin (2020). Los documentos se escogieron dado que eran los principales que tenían traducción oficial al inglés.

País	Definición de Ciberseguridad	Ciberamenazas
Estonia	*"La ciberseguridad nacional es un término amplio que abarca aspectos de la información, los datos y los medios electrónicos, servicios que afectan los intereses y el bienestar de un país…, una estrategia de defensa cibernética debe evaluar la vulnerabilidad de la infraestructura crítica, diseñar un sistema de medidas preventivas contra ataques cibernéticos y decidir sobre la asignación de tareas relacionadas con la gestión de la seguridad cibernética a nivel nacional… también es importante mejorar el marco legal contra los ataques cibernéticos, la cooperación institucional, sensibilizar al público y desarrollar programas de capacitación e investigación sobre ciberseguridad* (Ministry of Security and Justice -MSJ-, 2017: 16-17)*."*	Tres tipos de amenazas según Ministry of Economic Affairs and Communications - MEAC- (2019: 26-28): 1. *Amenazas a la sociedad digital y el Estado:* protección de datos e información personales y del Estado, protección de INC, protección de ransomware, ataques DDoS, seguridad frente a cibercrimen. 2. *Amenazas a la industria, investigación y desarrollo:* protección de propiedad privada de start-ups en el sector seguridad, protección de investigaciones en torno a ciberdefensa y propiedad intelectual. 3. *Contribución internacional a la ciberseguridad:* aporte de Estonia a la gobernanza del ciberespacio.
Estados Unidos	*"la política de ciberseguridad incluye estrategia, política y estándares con respecto a la seguridad y las operaciones en el ciberespacio, abarca el rango completo de reducción de amenazas, vulnerabilidad, disuasión, compromiso internacional, respuesta a incidentes, resistencia y políticas de recuperación, incluidas red de computadoras para operaciones, aseguramiento de la información, derecho de aplicación de la ley, diplomacia, aspecto militar y misiones de inteligencia y como se relacionan éstas con la seguridad y estabilidad de la infraestructura global de información y comunicaciones* (Executive Office of the President Washington -EOTPW-, 2017: 1-7)."	4 tipos de amenazas según (EOTPW, 2017: 10-13): 1. Amenazas a las redes e información federales: 2. Amenazas a las infraestructuras críticas: 3. Combate al cibercrimen y mejora de notificación de incidentes: 4. Amenazas a la economía digital y propiedad intelectual:

Fuente: Elaboración propia con base en CCDCOE Tallin (2020)

Con base en este ejercicio, se identificaron un total de siete pilares que definen a las ENCS de los países de la OTAN y sus aliados:

i. *El ciberespacio es un componente del poder nacional:* la importancia del ciberespacio para la seguridad nacional es visible en cada una de las ENCS. No obstante, es importante diferenciar la forma en que cada Estado la entiende. Para casos como Estados Unidos, la EOTPW (2017) muestra la definición de un país que se asume como una potencia internacional. Países como Israel (NCD, 2017) o Australia (AAGD, 2009) consideran la construcción de cibercapacidades como un factor de relevancia en su política de seguridad nacional, con intenciones de contribuir a la consolidación de la gobernanza y securitización del ciberespacio.

ii. *La presencia del multilateralismo y cooperación:* los Estados de la OTAN asumen que la regulación del ciberespacio es una responsabilidad conjunta entre múltiples actores. No obstante, existen países con tendencia más abierta a la cooperación internacional -Alemania (FG, Germany, 2016) y Países Bajos (DMSJ, 2011; MFA, 2018)- mientras que otros buscan garantizar su capacidad de decisión soberana como Reino Unido (UK Cabinet Office, 2011) o Israel (NCD, 2017).

iii. *El ciberespacio es un instrumento de proyección internacional:* todos los países, ya sea con modesta o menor participación en esferas globales o regionales, utilizan al ciberespacio como un instrumento de poder nacional. El caso más representativo de esto se da en Estonia, país que tiene una importancia relativamente baja en temas culturales, financieros o políticos en la región europea, pero que en el dominio es una de las naciones de vanguardia en temas de ciberseguridad (MSJ, 2017; MEAC, 2019).

iv. *La ciberseguridad tiene una dimensión civil, militar y estatal:* el conjunto de países establece los diferentes niveles que engloba la ciberseguridad y el tipo de ciberamenazas que existen. Para el caso de Estonia, esta nación marca una diferencia entre amenazas a la *sociedad digital* -claramente de carácter civil o de seguridad pública-, a las *amenazas al Estado* -de connotación militar y de la soberanía nacional (MEAC, 2019).

v. *Vinculación actores estatales-actores no estatales o privados:* la importancia de la construcción de nexos entre las partes interesadas está presente en este grupo países, principalmente en actores públicos, gubernamentales y privados. Esta asociación estratégica se presenta en tres dimensiones: 1) se reconoce la necesidad e interdependencia del Estado-Nación con la iniciativa privada, principalmente instituciones de creación de tecnología de internet o sistemas informáticos, para la construcción de cibercapacidades. 2) Se incentiva y considera vital la creación de conocimiento para consolidar capacidades de resiliencia y disuasión en el ciberespacio, en específico en la creación de posgrados o programas académicos o científicos vinculados al tema de la ciberseguridad (MEAC, 2019). 3) Se expresa la necesidad de contar con capital humano o profesionales expertos en ciberseguridad frente a los retos del ciberespacio (NCD, 2017).

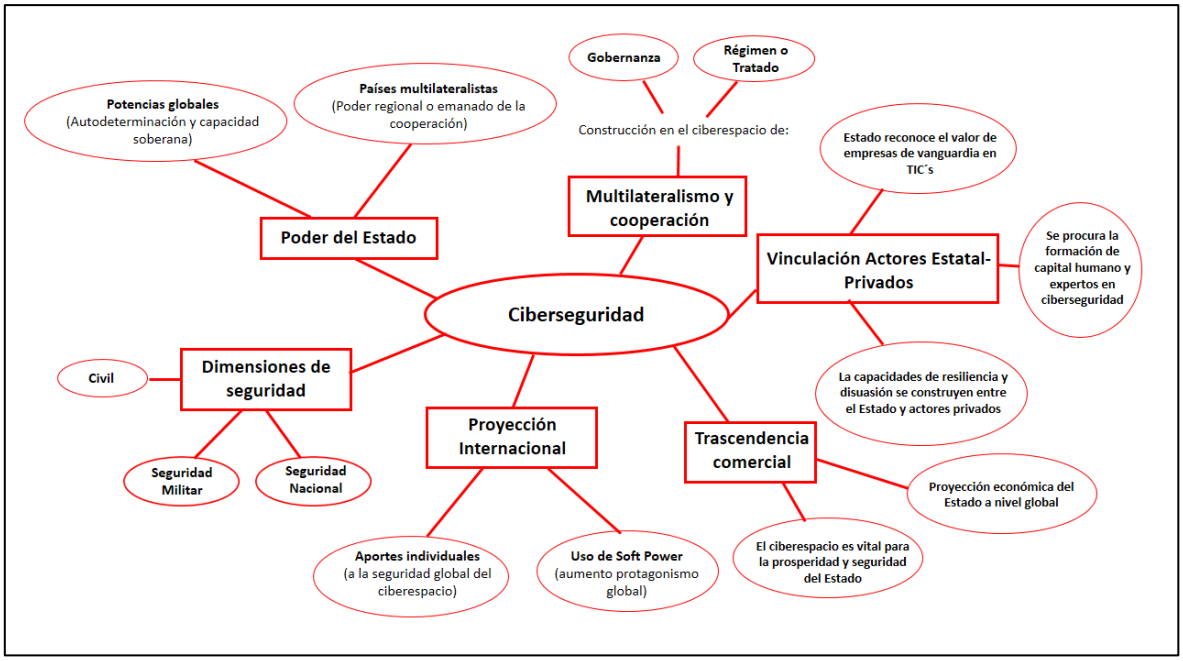
vi. *Se comprende y diferencia la parte física y virtual del ciberespacio:* las estrategias abordan las diferencias entre las tecnologías de la información (TIC´s), vinculadas a sistemas informáticos, bases de datos, etc., y relacionadas a la parte virtual del ciberespacio. Y las tecnologías de la operación (OT´s), relacionadas a infraestructura nacional crítica, cadenas de suministro, rutas de transporte y comercio, etc., Asimismo, establecen las amenazas que pueden presentarse a la seguridad nacional desde la esfera civil, militar y nacional.

vii. *Se reconoce la trascendencia comercial y económica del ciberespacio:* los documentos generados por el Estado, tales como Estrategias de Seguridad Nacional, ENCS, legislaciones nacionales o declaraciones de derecho internacional, contienen apartados en los que se aborda la importancia de la dimensión económica y comercial del dominio. Así como el papel que juega éste en la prosperidad del Estado, la seguridad nacional y la proyección del país hacia el exterior.

Es importante destacar que los siete pilares identificados en este análisis tienen una fuerte convergencia con los estándares de las ENCS de naciones e instituciones intergubernamentales líderes en la creación, formulación, desarrollo e implementación de políticas de ciberseguridad. Así como con el Modelo de Estrategia de Ciberseguridad (NCSSM, por sus siglas en inglés) presentado por Sabillon, Cavaller y Cano (2016: 67-69) que identifica ocho pilares clave que determinan el cumplimiento de todos los requisitos de

una ENCS. Para concluir esta sección, se destaca que la figura 4 presenta una anatomía de la concepción de ciberseguridad de los países de la OTAN y sus aliados.

Figura 4. Anatomía de la ciberseguridad de los países y aliados de la OTAN



Fuente: Elaboración propia

Entornos regionales y globales de ciberseguridad y la brecha de América Latina respecto a la OTAN

Como se mencionó anteriormente, la comparación entre América Latina y los países de la OTAN en esta investigación se debe a que se considera que esta organización, y sus Estados miembros y aliado estratégicos, han priorizado la ciberseguridad y desarrollo de capacidades desde la óptica de la seguridad nacional, estabilidad política y relaciones diplomáticas, aspectos clave y de interés para el Estado-Nación. En ese sentido, un aspecto central de este documento es el mostrar cómo América Latina se encuentra rezagada en el desarrollo de sus cibercapacidades respecto a este conjunto de países y otras regiones del mundo. Para esto se recurrió a dos métricas internacionales que evalúan la política de ciberseguridad de más de 100 países a nivel global y sirven de marco para medir el grado de compromiso de diferentes naciones en este campo. La primera es el *Índice Global de Ciberseguridad* (GCI, por sus siglas en inglés), de la Unión Internacional de Telecomunicaciones (ITU), y la segunda el *Índice Nacional de Ciberseguridad* o (*National Cyber Security Index* o NCSI en inglés), de la *E- Governance Academy*. Ambas métricas presentan áreas de oportunidad y de mejora de las legislaciones nacionales contra cibercrimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT), con el fin de mejorar las cibercapacidades de los países evaluados. Ante esto, se expresa que, si bien la evaluación realizada por los dos índices es más amplia a los intereses de la noción de ciberseguridad planteada en esta

investigación, sus datos e información generada sirven para mostrar las asimetrías y la brecha en el desarrollo de cibercapacidades presente en América Latina.

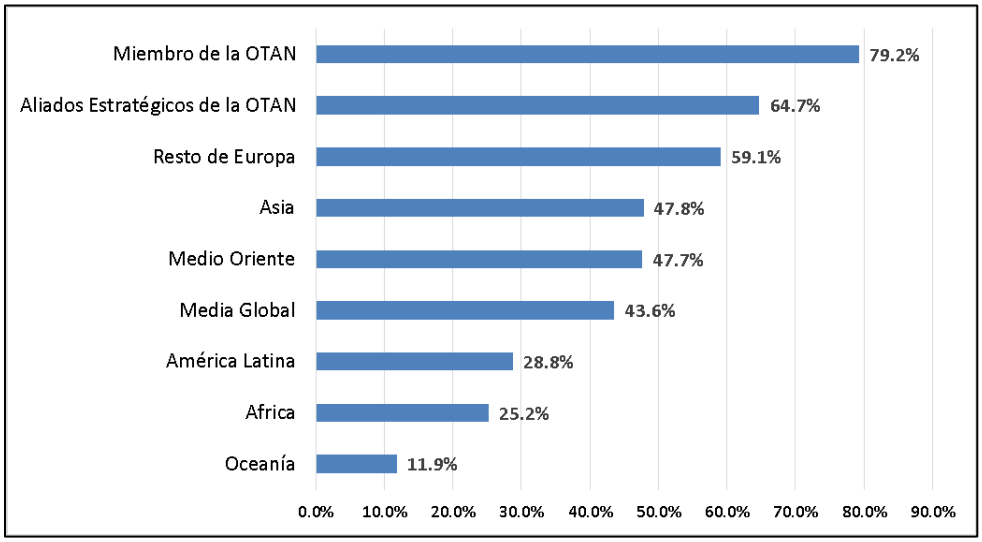
De esta forma, el GCI representa la métrica de un índice compuesto, integrado por 25 indicadores que tienen la finalidad de monitorear y comparar el grado de compromiso de los diferentes países del mundo con los cinco pilares de la Agenda Global de Ciberseguridad (AGCS), creada por la ITU, en 2007 (GCI, 2018: 8-10). Los objetivos del GCI son medir:

- El tipo, nivel y evolución a lo largo del tiempo del compromiso de ciberseguridad en los países miembros de la ITU.
- El progreso y seguimiento en el grado compromiso de ciberseguridad desde una perspectiva global y regional.
- La división del compromiso de seguridad cibernética o la diferencia entre países en términos de su nivel de participación en iniciativas de ciberseguridad.

Los puntos anteriores, integran la AGCS de la ITU y se traducen en cinco pilares: 1) marco legal: existencia de instituciones legales y marcos jurídicos de seguridad cibernética y cibercrimen. 2) Medidas técnicas: cantidad de instituciones técnicas encargadas de ciberseguridad e involucramiento de partes interesadas. 3) Estructura organizacional: existencia de instituciones y estrategias de coordinación de políticas para el desarrollo de ciberseguridad a nivel nacional. 4) Desarrollo de capacidades: existencia de investigación científica y programas de educación, capacitación, certificación de profesionales y agencias del sector público que fomentan el desarrollo de cibercapacidades. 5) Cooperación internacional: existencia de asociaciones, marcos cooperativos y redes de intercambio de información del gobierno con otros países. Dicha métrica evalúa a los 194 países del mundo, a través de una ponderación 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.

Para fines de nuestro análisis, y observar la posición que ocupa América Latina respecto a otra regiones o conjunto de países, se agruparon el total de naciones incluidas en el GCI en ocho diferentes subconjuntos: 1) países miembros de la OTAN, 2) aliados estratégicos de la OTAN, 3) resto de Europa, 4) Asía, 5) Medio Oriente, 6) América Latina, 7) África y 8) Oceanía, de los cuales se obtuvo el promedio del total de la calificación asignada a cada país. Al mismo tiempo, se calculó una media global, obtenida de la calificación de los 194 países del mundo, que se muestra en la figura 5.

Figura 5. Media regional o de grupos de países en el desarrollo de cibercapacidades según el GCI (2018)



Fuente: Elaboración propia con base en GCI (2018)

La figura 5 muestra que el conjunto de naciones más aventajado en el desarrollo de cibercapacidades y comprometido con los cinco pilares de la AGCS son los países miembros de la OTAN. Dado que los integrantes de dicha alianza ostentan una calificación en grupo de 79.2%, ponderación que está por encima del 35.6% de la media global del resto de las naciones del mundo. En segunda instancia, se observa que sigue el grupo conformado por sus aliados estratégicos (64.7%), y en tercer puesto, el resto de los países de Europa (59.1%). Respecto al caso de América Latina, destaca que la región se encuentra hasta la sexta posición, con una calificación de 28.8% (14.8% por debajo de la media global), y solo por delante de regiones como África (25.2%) y Oceanía (11.9%).

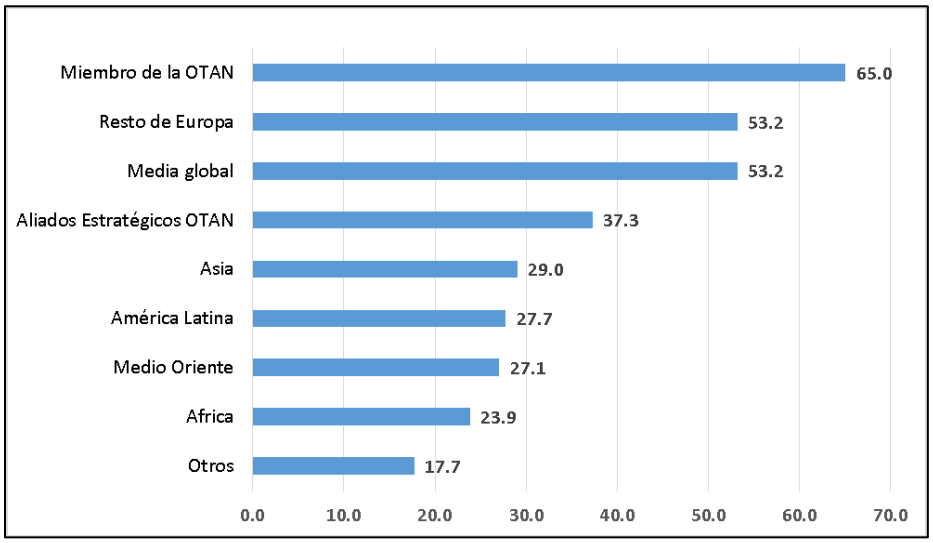
Respecto al NCSI (2019) de la *E-Governance Academy*, se destaca que esta medida evalúa la preparación de los países para prevenir ciberamenazas y gestionar ciberincidentes. En ese sentido, se expresa que el GCI (2018) mide el grado de compromiso e importancia que los Estados-Nación han dado al tema de la ciberseguridad en el desarrollo de su política de seguridad nacional. Mientras que el NCSI es un instrumento que mide sus capacidades de ciberdefensa. Asimismo, es importante mencionar que el NCSI (2019) se empata con el GCI (2018) en aspectos como el desarrollo de marco legal, medidas técnicas, estructura internacional y cooperación internacional. No obstante, posee un apartado más amplio en el desarrollo de cibercapacidades, dado que trata con mayor profundidad las habilidades para atender ciberincidentes y combatir amenazas.

El NCSI (2018) se compone de un total de doce indicadores, con una ponderación que va del 0 al 100, estas variables son: 1) Desarrollo de Política de ciberseguridad. 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 a nivel internacional. 5) Nivel de desarrollo digital del país. 6) Protección de servicios esenciales por el Estado como infraestructura nacional crítica. 7) Identificación electrónica y confidencialidad de servicios en la vida diaria. 8) Protección

de datos personales de personas, empresas, etc., y garantía de su privacidad.9) Respuesta a ciberincidentes por parte de equipos de emergencia informática (CSIRT, CIRT) ante un ciberincidente. 10) Capacidad de administración de cibercrisis del Estado-Nación. 11) Grado de compromiso del Estado para luchar contra el cibercrimen. 12) Capacidad de operaciones militares de las fuerzas armadas en el ciberespacio.

En ese sentido, se agrupó por regiones o conjunto de países las naciones incluidas en el NSCI (2019). No obstante, dado que el NCSI solo analiza un total de 100 Estados del mundo, estos fueron separados en nueve subgrupos. 1) Miembros de la OTAN, 2) Aliados de la OTAN, 3) Resto de Europa, 4) Asía, 5) América Latina, 6) Medio Oriente, 7) África, y 8) Otros países, como se muestra en la figura 6.

Figura 6. Media regional o de grupos de países en capacidades de ciberdefensa según el NSCI (2019)



Fuente: Elaboración propia con base en NSCI (2019)

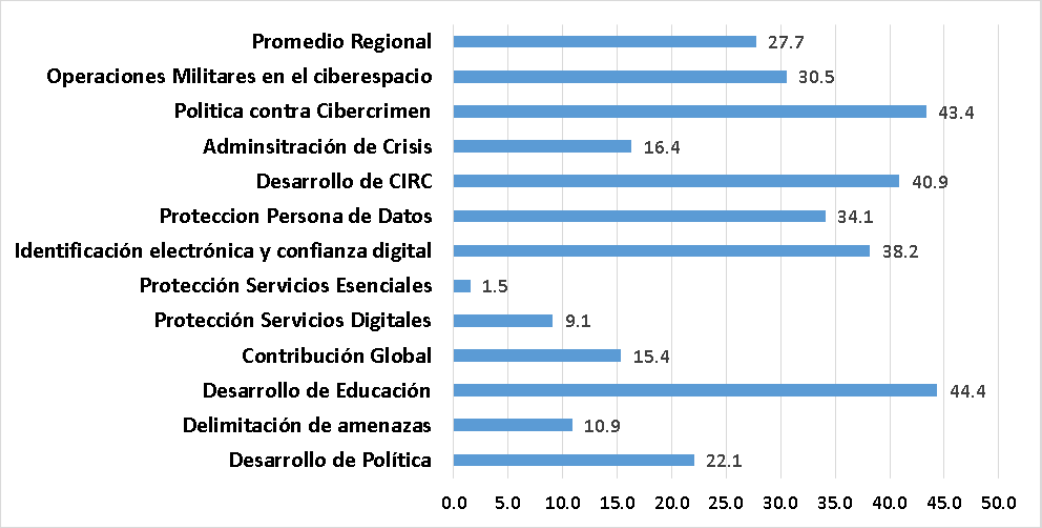
La figura 6 muestra de nuevo que los países de la OTAN son los más aventajados en la construcción de cibercapacidades de defensa, con una calificación de 65 puntos sobre 100. No obstante, un dato interesante derivado de la figura 6, es que mientras los países aliados estratégicos de dicho organismo, detenta la segunda posición en nivel de compromiso con la AGCS, en las cifras del NSCI (2019) son superados por el resto de Europa, por un total de 15.9 puntos, en los datos de esta métrica. Por último, destaca nuevamente que América Latina se encuentra en las últimas posiciones (en este caso en la quinta) y por debajo de la media mundial con 25.5 puntos en su ponderación (27.7).

Las carencias anteriores y la brecha de ciberseguridad de América Latina se reflejan en informes realizados por la OEA y el BID, publicados en la última década. En cifras concretas el incremento de ciberamenazas en la región fue de un 60% durante el bienio 2012-2013 (OEA/Symantec, 2014: 9-12). A la par que en 2015 el incremento de troyanos dirigidos al fraude bancario afectó al 92% de las entidades financieras con al menos un ciberataque, de los cuales 37% del total resultaron exitosos (OEA, 2018: 17-22). Del mismo modo el estudio

Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?, del BID expresa que América Latina y el Caribe 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 (BID, 2016: 20-22).

Respecto a reportes de firmas de ciberseguridad PandaLabs (2015: 12-15) expresó que, en 2014, países como Guatemala, Bolivia, Ecuador, Brasil y Perú se incluyeron entre las diez principales naciones con más computadoras infectadas por virus maliciosos a nivel global. Por su parte, IBM Security (2020) ubicó a la región cómo un punto que concentra el 5% de total de actividad cibercriminal de mundo y como un área específica en la que el delito de Ransomware tiene condiciones ventajosas para ejecutarse con mayor facilidad. Mientras que Deloitte (2019) realizó un estudio regional a 150 organizaciones de siete diferentes sectores, en 13 países de la región, y expresa que 4 de cada 10 organizaciones sufrieron un incidente de ciberseguridad el bienio 2018-2019. Así como el hecho de que 70% de éstas no tiene certeza de la efectividad de su proceso de respuesta ante ciberincidentes. Dado que solo un 31% de las organizaciones realiza inteligencia de amenazas y comparte información con otras organizaciones. Respecto a datos como los anteriores, se tomaron las 12 dimensiones del CNSI (2019), vinculadas a cibercapacidades para atender ciberamenazas y se obtuvo la media regional de América Latina y el Caribe (27.7), que se presenta en la figura 7.

Figura 7. Media de indicadores de cibercapacidades en América Latina según en NCSI (2019)



Fuente: Elaboración propia con base en el NCSI (2019)

La figura anterior presenta hechos de transcendencia para comprender las razones que explican la brecha de ciberseguridad en la región. Por ejemplo, destaca que las dos dimensiones entre las que mejor se encuentra posicionada la región son el desarrollo de política contra cibercrimen (43.4 puntos) y desarrollo de educación (44.4 puntos). Sin embargo, la región no ha logrado una definición concisa de qué tipos de ciberamenazas pueden afectar su seguridad nacional (10.9 puntos sobre un total de 100), a la par que su

desarrollo de ENCS aún tiene un valor bajo (22.1 puntos), al mismo tiempo que las capacidades de sus fuerzas armadas están aún en desarrollo para enfrentar ciberamenazas (30.5 puntos).

En relación a lo anterior, Moreno, Albornoz y Maqueo (2020: 32), expresan que América Latina y el Caribe está en una fase formativa de desarrollo de cibercapacidades con base en lo expresado al estudio del BID (2016: 20-22) que divide en cinco diferentes niveles de madurez el desarrollo de una ENCS y se explican en la figura 8, en la que se observa que los países de la región se encuentran en los tres primeros niveles, con 17 países en nivel inicial, 10 en formativo y 5 en establecido.

Figura 8. Nivel de madurez de las ENCS de América Latina según el BID

Nivel Inicial	Nivel Formativo	Nivel Establecido	Nivel Estrátegico	Nivel Dinámico
Características del Nivel				
No hay evidencia de la existencia de una ENCS	Se ha articulado un esquema de una ENCS y se han identificado actores clave (gobierno, públicos, privados).	Establecido: se ha establecido una ENCS y se ha establecido un mando específico para consultar los sectores estratégicos y la sociedad civil. Asimismo, existe comprensión de riesgos y amenazas.	La ENCS se implementa por todas las partes interesadas, y se conforman procesos de revisión y renovación de la estrategia para su mejora constante y toma de decisiones.	La ENCS se revisa constantemente para adaptarse a los riesgos cambiantes y entornos sociopolíticos de amenazas y tecnologías, se llevan a cabo medidas de transparencia y fomento de la confianza entre actores públicos-privados
Países en cada Nivel				
1. Antigua y Barbuda 2. Bahamas 3. Barbados 4. Belice 5. Bolivia 6. Ecuador 7. El Salvador 8. Granada 9. Guatemala 10. Guyana 11. Haití 12. Honduras 13. Nicaragua 14. República Dominicana 15. Saint Kitts y Nevis 16. Santa Lucía 17. Venezuela	1. Argentina 2. Brasil 3. Chile 4. Costa Rica 5. Dominica 6. México 7. Paraguay 8. Perú 9. San Vicente y las Granadinas 10. Surinam	1. Colombia 2. Jamaica 3. Panamá 4. Trinidad y Tobago 5. Uruguay	Ningún país de la región	Ningún país de la región

Fuente: Elaboración propia con base en Moreno, Albornoz y Maqueo (2020)

Presentados los datos anteriores, se argumenta que la hipótesis de la que parte esta investigación se ha verificado según el análisis presentado por el GCI (2018), el NCSI (2019) y el BID (2016). A la par de contextualizar el creciente riesgo de ciberamenazas en la región. No obstante, la nueva pregunta central, una vez verificada la hipótesis, es: ¿qué acciones y caminos debe seguir la región de América Latina y el Caribe para reducir esta brecha? Una respuesta es dada por Klimburg y Healey (2012: 70-74), que expresan que la estructuración y renovación de las ENCS debe ser alimentada por el establecimiento de metas estratégicas y un estudio conciso de los retos y ciberincidentes superados por cada país a lo largo del tiempo. Dicha evolución, puede verse en la cantidad y mejora de documentos centrados en

crear capacidades de ciberdefensa por los gobiernos, ya sean estos ENCS, legislaciones, protocolos o declaraciones de derecho internacional.

Sobre este punto, se revisó el apartado de *Estrategia y gobernanza,* de la biblioteca digital del CCDCOE Tallin (2020) y sistematizó el total de documentos de los 77 países que registra esta institución, en la que se encontraron un total de 210. Posteriormente, se calculó el promedio de documentos de los diferentes grupos de países para la construcción de cibercapacidades. Una vez más, se encontró una fuerte brecha entre el promedio de los países y aliados de la OTAN y otros países de Europa (3.8 documentos en promedio), con la media de América Latina y el Caribe (1.12 documentos), que se muestra en la tabla 2.

Tabla 2. Promedio de documentos y estrategias sobre el ciberespacio

Grupos de países	Promedio de documentos y ENCS.
Países y aliados de la OTAN y otros países de Europa.	3.8
Países de Asía.	2.3
Países de América Latina y el Caribe.	1.12
Países de Medio Oriente y África.	1.11

Fuente: CCDCOE Tallin (2020)

No obstante de la situación anterior y el contexto de rezago de la región, la publicación del reciente informe *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe,* elaborado en conjunto por la OEA y el BID, muestra un claro avance y compromiso regional en el desarrollo de cibercapacidades en los últimos cuatro años (OEA/BID, 2020: 45-179). Dicho informe mide cinco diferentes dimensiones, a través de 49 indicadores en una ponderación que va del 0 al 100, donde 0 es la peor calificación y 100 la mejor. En la tabla 3 se muestra cómo los Estados americanos han mejorado sus capacidades en el periodo 2016-2020. Dado que todos los países han presentado mejoras en la materia, la media regional se elevó a 39.88 puntos, lo que refleja un esfuerzo e interés regional en el tema. También, es importante destacar los esfuerzos individuales de los gobiernos de Brasil (con calificación 59.2), Chile (56.3), Colombia (59.2), Uruguay (69.4) y México (56.5), que han dado prioridad al tema y avanzaron más de 20 puntos en su calificación del 2016. No obstante de este modesto éxito, aún queda un largo camino a la región de América Latina para el desarrollo de sus cibercapacidades y alcanzar el nivel de madurez en sus ENCS.

Tabla 3. Evolución se cibercapacidades de países de América Latina y el Caribe en el periodo 2016-2020

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
6	República Dominicana	30.3	49.7	+19.4
7	Paraguay	26.6	45.7	+19.1
8	Brasil	40.1	59.2	+19.0
9	Trinidad y Tobago	30.3	49.3	+19.0
10	Costa Rica	26.4	42.7	+16.3
11	Panamá	26.7	41.7	+15.0
12	Argentina	34.3	48.5	+14.2
13	Jamaica	28.2	41.6	+13.4
14	Nicaragua	17.3	29.7	+12.5
15	Barbados	21.2	33.3	+12.1
16	Bolivia	23.7	35.6	+11.9
17	Ecuador	24.3	36.2	+11.8
18	Perú	28.7	40.5	+11.8
19	Honduras	18.8	30.6	+11.8
20	Bahamas	21.1	32.9	+11.8
21	Antigua y Barbuda	19.6	31.2	+11.7
22	Guatemala	21.5	32.9	+11.4
23	Surinam	20.9	31.4	+10.5
24	San Vicente y las Granadinas	19.8	30.0	+10.3
25	Saint Kitts y Nevis	22.3	31.8	+9.5
26	Santa Lucía	19.3	28.7	+9.4
27	Belice	22.3	31.3	+9.0
28	Granada	19.1	27.0	+7.9
29	Venezuela	24.6	32.3	+7.8
30	El Salvador	23.8	31.3	+7.5
31	Dominica	21.5	28.9	+7.4
32	Haití	19.2	24.5	+5.4

Fuente elaboración propia con base en OEA/BID (2020: 45-179)

MÉXICO: DOS BREVES CASOS DE ESTUDIO SOBRE LA BRECHA DE CIBERSEGURIDAD DE AMÉRICA LATINA

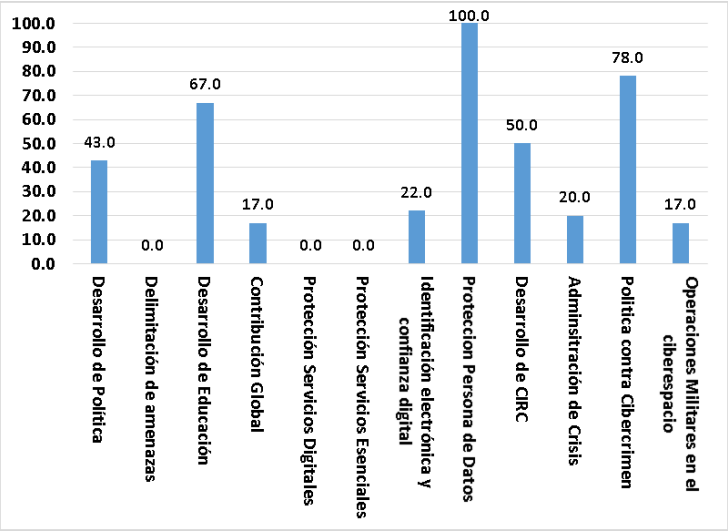
En el bienio 2019-2020, México sufrió dos importantes ciberincidentes que comprometieron la seguridad nacional del Estado mexicano. Cada uno mostró la importancia de elevar a carácter de esquema de seguridad nacional la construcción de cibercapacidades de defensa en esta nación, que son:

i. El ciberataque de *ramsonware* a la paraestatal mexicana Petróleos Mexicanos (PEMEX) en noviembre de 2019, empresa que está al centro de la política económica del Plan Nacional de Desarrollo (Ordaz, 2019). Y que está en un proceso de reestructuración y en plan de rescate para salvar sus finanzas ante la evaluación por parte de entidades financieras internacionales como las calificadoras *Fitch*, *Moody´s* y *Standar & Poor*. Dicho ciberataque afectó su operación para pago de deuda internacional y nomina, proceso que dañó su prestigio a nivel internacional, dado que el rescate que se pidió para regresar el control de la red de operaciones osciló en la cantidad 4.9 millones de dólares, uno de los más caros en la historia de América Latina (Riquelme, 2019).

ii. El ciberataque a la red interna de la Secretaría de Economía detectado el 24 de febrero de 2020, que según declaraciones de dicha institución gubernamental, solo afectó a correo electrónico y archivos de la red interna de la institución (Steve, 2020). Sin embargo, a pesar de que el ataque fue controlado, la dependencia tuvo que cesar sus trámites y procesos por 16 días, en lo que recuperaban el control de la red interna y la liberaban los sistemas informáticos de ciberamenazas, hasta el 10 de marzo de 2020 (Morales, 2020).

Los dos ciberincidentes descritos materializan la ausencia de capacidades de resiliencia y disuasión ante ciberataques, a pesar de la mejora presentada en el informe de la OEA/BID (2020). Dado que ambas instituciones tuvieron que cesar sus operaciones ante ambos incidentes. Y la materialización de capacidades de ciberresiliencia considera a una de sus características clave el seguir operando a pesar de sufrir un incidente de seguridad informática. Del mismo modo, el NSCI (2019) posiciona a México en el lugar 57 de 100 países evaluados y otorga una ponderación de 36.36 puntos sobre 100. Con calificaciones de 0 para indicadores como delimitación de amenazas, protección de servicios esenciales e identificación electrónica y confianza digital. Así como una calificación de 20 sobre 100 para administración de crisis. Hechos que se ajustan a lo acontecido en ambos incidentes, y que muestran una grave carencia en el desarrollo de disuasión y resiliencia para amenazas provenientes del ciberespacio. Por último, se presenta la ponderación de México en los 12 indicadores del NCSI (2019) en la figura 9.

Figura 9. Ponderación de México en indicadores del NCSI



Fuente: Elaboración propia con base en NCSI (2019: 24)

Conclusiones

El entorno actual de ciberamenazas y riesgos provenientes del ciberespacio es un reto para salvaguardar la seguridad del Estado-Nación en cualquier país del mundo. No obstante, la región de América Latina y el Caribe se encuentra rezagada en la construcción de cibercapacidades para enfrentar dicho contexto. En ese sentido, la primera acción que deben tomar los gobiernos de este conjunto de países es comprender el nivel de riesgos y amenazas a la seguridad nacional, que pueden emanar de este dominio para afectar al Estado-Nación.

A pesar de los avances regionales presentados por la OEA/BID (200) en lo últimos cuatro años, es importante que la región se comprometa más en términos de voluntad política y desarrollo real de cibercapacidades a través de la estructuración una ENCS adecuada, un marco jurídico para el combate de ciberdelitos, la creación de convenios multilaterales de cooperación y el desarrollo de programas de formación de profesionales en ciberseguridad. Sobre este asunto es importante que la región afiance sus responsabilidades y obligaciones con la AGCS, de la ITU, a la par de que se vincule con métricas como las presentadas por el GCI (2018) y el NCSI (2019), que le servirán para poder medir su nivel de avance en el desarrollo de cibercapacidades. También, es importante que estudie y analice la construcción, evolución y madurez de otras regiones que se han transformado en líderes en ciberdefensa, como los Estados miembros de la OTAN.

Si en el futuro cercano la región logra consolidar la fase inicial y medio del desarrollo de sus cibercapacidades, el siguiente paso será evaluar el cambio de sus ENCS de un nivel establecido a uno dinámico, que logre estar en aptas condiciones para encarar los retos actuales de la ciberseguridad a nivel global.

NOTA SOBRE EL AUTOR:

Juan Manuel Aguilar Antonio. Licenciado en Relaciones Internacionales por la UNAM. Maestro en Administración Pública y en Socioeconomía, Estadística y Cómputo Aplicado. Actualmente es candidato a Doctor en Ciencias Sociales, campo disciplinario Relaciones Internacionales, en la FCPyS de la UNAM.Es egresado del curso *Desarrollo de Políticas Cibernéticas* del Centro William J. Perry, de la Universidad de la Defensa en Washington D.C. Su publicación más reciente en temas de ciberseguridad es el artículo académico *Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad,* en la Revista Urvio, de la Red FLACSO, indexada y arbitrada, con sede Quito, Ecuador. Correo electrónico: jm.aguilar@casede.org

REFERENCIAS

Australian Attorney-General's Department -AAGD- (2009), *Cyber Security Strategy*: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/Cybersecurity

AON (2019), "2019 Cyber Security Risk Report: What´s Now and What´s Next", February 19: https://www.aon.com/cyber-solutions/thinking/2019-cyber-security-risk-report-whats-now-and-whats-next/

Benítez, Raúl (2011), "México, Centroamérica y Estados Unidos: migración y seguridad. Migración y seguridad: nuevo desafío en México", en Armijo, Natalia (Ed.), *Migración y Seguridad: Nuevo desafío en México*, México, D.F.: CASEDE, pp. 179-192.

Banco Interamericano de Desarrollo -BID- (2016), *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?*, Washington D.C.: BID.

CCDCOE Tallin (2020), "Strategy and Governance", *Cooperative Cyber Defence Centre of Excellence*, April 20: https://ccdcoe.org/library/strategy-and-governance/

Canadian Department for Public Safety -CDPS- (2010), *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada*: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-index-en.aspx

Chauvin, Justine M. (2016), *NATO Cyber Defence Policy An adaptation to the emerging threats of the 21st century, or the resurgence of Cold War logic in the "fifth battlefield"?*, Dissertation for the degree of Master of Arts in International Politics of the Internet. Aberystwyth University.

Digital Attack Map (2019), "Digital Attack Map", April 15: https://www.digitalattackmap.com/

Departamento de Seguridad Nacional -DSN- (2013), *Estrategia de Ciberseguridad Nacional*: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

— (2019), *Estrategia Nacional de Ciberseguridad*: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Cavelty, Myriam D. (2012), "The militarisation of cyberspace: Why less may be better," *4th International Conference on Cyber Conflict* (*CYCON 2012*), Tallin, pp. 1-13.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal & Zittrain, Jonathan (2008), *Access Denied: The Practice and Policy of Global Internet Filtering*, MIT Press.

Deloitte (2019), "Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019", 15 de abril: https://www2.deloitte.com/co/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

Executive Office of the President Washington -EOTPW- (2017), *National Security Strategy of the United States of America*: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Federal Government Germany -FG Germany- (2016), *White Paper on German Security Policy and the future of the Bundeswehr*: https://ccdcoe.org/uploads/2018/10/2016-White-Paper-1.pdf

GBA & ITRC (2018), "The Impact of Cybersecurity Incidents on Financial Institutions. Identity Theft Resource Center Generali Global Assistance", *Identity Theft Resource Center*, July 1: https://www.idtheftcenter.org/2018-data-breaches/

GCI (2018), "Global Cybersecurity Index", *International Telecommunication Union*, June 20: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Hackmageddon (2020), "2019 Cyber Attacks Statistics", April 20: https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/

Haffa Jr, Robert P. (2018), "The Future of Conventional Deterrence: Strategies for Great Power Competition", *Strategic Studies Quarterly*, Vol. 12, No. 4, pp. 94-115.

Haimes, Yacov Y. (2006), "On the definition of vulnerabilities in measuring risks to infrastructures", *Risk Analysis: An International Journal*, Vol. 26, No. 2, pp. 293-296.

Healey, Jason & van Bochoven, Leendert (2012), "Nato's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council of the United States*, February 27: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/natos-cyber-capabilities-yesterday-today-and-tomorrow/

Hughes, Rex B. (2009), "NATO and Cyber Defence : Mission Accomplished?", *Atlantisch Perspectief*, Vol. 33, No. 1.

IBM Security (2020), "X-Force Threat Intelligence Index 2020", May 21: https://www.ibm.com/account/reg/us-en/signup?formid=urx-42703

Kaspersky (2020), *The Kaspersky Lab Global IT Risk Report*, [online] Kaspersky lab: https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf [Accessed 20 June 2020].

Klimburg, Alexander (Ed.) (2012), *National Cyber Security Framework Manual*, NATO CCD COE Publication.

Klimburg, Alexander & Healey, Jason (2012), "Strategic Goals & Stakeholders", in Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, Tallinn: NATO CCD COE Publication, pp. 66 -107.

Lindstrom, Gustav & Luiijf, Eric (2012), "Political Aims & Policy Methods", in Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, Tallinn: NATO CCD COE Publication, pp. 44-65.

Mearsheimer, John J. (1985), *Conventional deterrence*, Cornell University Press.

Minister of Foreign Affairs -MFA- (2018), *Working Worldwide for the Security of the Netherlands*: https://www.government.nl/documents/reports/2018/05/14/integrated-international-security-strategy-2018-2022

Ministry of Economic Affairs and Communications -MEAC- (2019), *Cybersecurity Strategy: Republic of Estonia*: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Morales, Roberto (2020), "Secretaría de Economía suspende trámites por ataque cibernético", *El Economista*, 25 de febrero: https://www.eleconomista.com.mx/empresas/Secretaria-de-Economia-suspende-tramites-por-ataque-cibernetico-20200225-0027.html

Moreno, Jimena, Albornoz, María M. y Maqueo, María S. (2020), "Ciberseguridad: estado de la cuestión en América Latina", *Revista de Administración Pública INAP*, Vol. LIV, No. 1, pp.23-46.

Morgan, Steve (2019), "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021", *Cyber Crime Magazine*, June 10: https://cybersecurityventures.com/cybersecurity-market-report/#:~:text=The%20cybersecurity%20market%20grew%20by,period%20from%202017%20to%202021.

Ministry of Security and Justice -MSJ- (2017), *The National Cyber Security Strategy (NCSS)*: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf

NCSI (2019), "National Cyber Security Index. E-Governance Academy", *E-Governance Academy*, February 22: https://ncsi.ega.ee/

National Cyber Directorate -NCD- (2017), *Israel National Cyber Security Strategy in Brief*: http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf

Newmeyer, Kevin P. (2015), "Elements of national cybersecurity strategy for developing nations", *National Cybersecurity Institute Journal*, Vol. 1, No. 3, pp. 9-19.

Noonan, Eric (2016), "White House Unveils Color-Coded Scale for Cyber Security Threat", *Cybersheat Service International*, July 29: https://cybersheath.com/white-house-unveils-color-coded-scale-for-cyber-security-threats/

Organización de los Estados Americanos -OEA-/Symantec (2014), *Tendencias de Seguridad Cibernética en América Latina y el Caribe*, [online] OEA/Symantec: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf [Accessed 10 January 2019].

Organización de los Estados Americanos -OEA- (2018), *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe*, [online] OEA: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf [Accessed 10 April 2019].

Organización de los Estados Americanos -OEA- y Banco Interamericano de Desarrollo – BID-(2020), *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*, [online] OEA/BID: http://dx.doi.org/10.18235/0002513 [Accessed 07 May 2020].

Ordaz, Yeshua (2019), "¿Qué es el ransomware? El virus que atacó a Pemex", *Milenio*, 13 de noviembre: https://www.milenio.com/negocios/que-es-el-ransomware-el-virus-del-wannacry-que-ataco-pemex

Palfrey, John G. (2010), "Four Phases of Internet Regulation", *Social Research*, Vol. 77, No. 3, pp. 981-996.

Pandalabs (2014), *Informe Anual Pandalabs 2014*. [online] Panda: https://www.pandasecurity.com/es/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF-es.pdf [Accessed 1 April 2019].

PandaLabs (2015), Informe Anual": https://www.pandasecurity.com/spain/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF-es.pdf

Riquelme, Rodrigo (2019), "El rescate por el hackeo a Pemex es el segundo mayor por ransomware", *El Financiero*, 15 de noviembre: https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html#:~:text=Esta%20cifra%20asciende%20a%20alrededor,la%20infecci%C3%B3n%20que%20enfrent%C3%B3%20Pemex.&text=La%20ciudad%20hizo%20una%20contraoferta,neg%C3%B3%20a%20pagar%20el%20rescate.

Rühle, Michael (2011), "NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm," *American Foreign Policy Interests. The Journal of the National Committee on American Foreign Policy*, Vol. 33, No. 6, pp. 278-282: https://doi.org/10.1080/10803920.2011.632308

Sabillon, Regner, Cavaller, Victor & Cano, Jeimy (2016), "National Cyber Security Strategies: Global Trends in Cyberspace", *International Journal of Computer Science and Software Engineering*, Vol. 5, No. 5, pp. 67-81.

Samaan, Jean-Loup (2010), "Cyber command: The rift in US military cyber-strategy", *The RUSI Journal*, Vol. 155, No. 6, pp. 16-21: https://doi.org/10.1080/03071847.2010.542664

Sicherheitstacho (2019), "Overview of Current Cyber Attacks", *Deutsche Telekom*, April 10: https://sicherheitstacho.eu/start/main

Steve, Oscar (2020), "A dos semanas del ciberataque, Secretaría de Economía en México vuelve a funcionar (aunque no sabemos exactamente qué ocurrió)", *Xataka México*, 10 de marzo: https://www.xataka.com.mx/empresas-y-economia/a-dos-semanas-ciberataque-secretaria-economia-mexico-vuelve-a-funcionar-no-sabemos-exactamente-que-ocurrio

Szentgáli, Gergely (2013), "The NATO Policy on Cyber Defence: The Road so Far", *AARMS*, Vol. 12, No. 1, pp. 83–91.

Take, Ingo (2012), "Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS", *Regulation & Governance,* Vol. 6, No. 4, pp. 499-523: https://doi.org/10.1111/j.1748-5991.2012.01151.x

UK Cabinet Office (2011), *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

US Department of State (2020), "Major Non-NATO Ally Status", January 30: https://www.state.gov/major-non-nato-ally-status/

Verizon (2020), "2020 Data Breach Investigation Report", May: https://enterprise.verizon.com/resources/reports/dbir/

White House PPD (2016), "FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination", *White House Presidential Policy Directive*, July 26: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1