Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional

*Juan Manuel Aguilar-Antonio**

Resumen: La presente investigación se centra en analizar la importancia de comprender el ciberespacio como un nuevo espacio de conflicto entre las naciones, un dominio que necesita una gramática de seguridad para la defensa de la soberanía y el papel que éste ocupa dentro de la estrategia de seguridad nacional, con énfasis en América Latina y, en especial, en México. En el primer apartado se realiza una breve discusión en torno a la comprensión del ciberespacio desde la teoría de la guerra, el constructivismo y el neorrealismo. En la segunda se expone en qué momento el internet sufre un proceso de securitización, el ciberespacio se integra como un dominio vital para garantizar la seguridad nacional, así como una definición en torno a ciberamenazas al Estado. En el tercero se presentan una contextualización sobre los entornos regionales y globales de ciberseguridad y la brecha de América Latina. Por último, se presenta una propuesta para la creación de la Agencia Nacional de Ciberseguridad, desde el enfoque prospectivo de los escenarios VUCA, que puede servir a México en el futuro para enfrentar los retos de la ciberseguridad.

Palabras clave: seguridad cibernética, seguridad interior, seguridad nacional, estrategia nacional de ciberseguridad.

***** Juan Manuel Aguilar-Antonio. Candidato a doctor por la Facultad de Ciencias Políticas y Sociales (FCPyS) de la Universidad Nacional Autónoma de México. Investigador del Colectivo de Análisis de la Seguridad con Democracia AC (Casede). Correo electrónico: jm.aguilar@casede.org

Revista Legislativa de Estudios Sociales y de Opinión Pública, vol. 13, núm. 29, sept.-dic. de 2020, pp. 83-120. Fecha de recepción: 31 de agosto de 2020. Fecha de aceptación: 16 de diciembre de 2020.

Present and future of cybersecurity challenges in Mexico, a proposal for national security

Abstract: This research focuses on analyzing the importance of understanding cyberspace as a new space of conflict between nations, a domain that needs a securitization compression for the defense of sovereignty and the role it occupies n the national security strategy, with an emphasis on Latin America and especially in Mexico. In the first section, there is a brief discussion about the understanding of cyberspace from the Theory of War, Constructivism and Neorealism. In the second, it is exposed when the internet undergoes a securitization process, cyberspace is integrated as a vital domain to guarantee national security, as well as a definition around cyber threats to the State. The third section presents the gap of the regional and global cybersecurity environments in relation with Latin American. Finally, a proposal is presented for the creation of the National Cybersecurity Agency, from the prospective approach of the VUCA scenarios that can serve to Mexico in the near future to face the challenges of cybersecurity.

Keywords: Cybersecurity, homeland security, national security, national cyber security strategy.

Introducción

Los ciberataques de Tallin, Estonia (2007), sentaron el primer caso de trascendencia que involucra al ciberespacio como un instrumento capaz de vulnerar la seguridad nacional de un Estado-nación. La relevancia de este evento promovió la inclusión de este dominio como una arena de securitización de trascendencia para la salvaguarda de la soberanía. En el ámbito de la academia, en específico en los estudios de relaciones internacionales, ciencia política y seguridad nacional, la utilización del internet y los flujos de información como medio para vulnerar a un gobierno hicieron que se considerara a esta red de comunicación como un mecanismo capaz de promover una revolución en la política internacional (Kello 2010), en señalar al ciberespacio como una nueva arena de confrontación e influencia de las naciones (Hughes, 2010) y expresarse de él como una esfera que necesita la construcción de una gramática de seguridad para su uso y regulación (Hansen y Nissenbaum, 2009).

Dicho debate, en primera instancia, promovió entre las naciones miembros de la Organización del Tratado del Atlántico Norte (OTAN) la necesidad de crear una Estrategia Nacional de Ciberseguridad (ENCS), que forme parte de la estrategia global de Seguridad Nacional del Estado. Para 2011, un total de 20 países, de los 29 que conforman esta alianza, ya contaban con su primera versión de este documento, en el que presentaban su definición de ciberseguridad y una delimitación de las ciber amenazas consideradas con capacidad de vulnerar la seguridad nacional. Con el pasar de los años, la acción de crear una ENCS se ha extendido a múltiples regiones del mundo. En la actualidad el Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN registra que un total de 77 naciones, en regiones como África, América Latina y el Caribe, Asia y Oceanía, han creado documentos, legislaciones o al menos una primera versión de una ENCS centrada en la regulación del ciberespacio (CCDCOE Tallin, 2019).

No obstante, las amenazas y los retos emanados del ciberespacio para la seguridad nacional avanzan a mayor velocidad que las acciones de los gobiernos para contenerlas. Tan sólo en 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 (GBA & ITRC, 2018). Al momento que se escribe este texto, de acuerdo con *T-Sec Radar* de *Deutsche Telekom* detecta que se dan 60,312 ciberataques cada minuto, lo que representa 3,712,960 por hora, y 79,390,302 en un solo día (Sicherheitstacho, 2019). Por su parte, la plataforma *Digital Attack Map* (2019) lleva el registro diario de los ataques *DDoS* o negación de servicio en el mundo, que son accesibles a cualquier individuo, empresa o gobierno por tan sólo 150 dólares. Por lo que este sitio se encarga de detectar su origen y país destino, los cuales alcanzaron cifras de más de 8,000 por día durante el último año. A la par que el *Cyberthreat Real-Time Map*, de la empresa Kapersky (2019), contabiliza minuto a minuto ocho diferentes tipos de ciber incidentes alrededor del mundo, además de registrar los cinco países con más infecciones cibernéticas, a través de sus sistemas y aplicaciones antivirus. En ese sentido, el presente artículo se centra en analizar la importancia de comprender

al ciberespacio como un nuevo espacio de conflicto entre las naciones, un dominio que necesita una gramática de seguridad para la defensa de la soberanía y el papel que éste ocupa dentro de la estrategia de seguridad nacional, con énfasis en América Latina, y en especial en México.

La comprensión del ciberespacio desde la teoría de la guerra, el constructivismo y el neorrealismo

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 factor crucial para determinar la superioridad de un Estado sobre otro en una confrontación bélica. En su obra clásica, *De la guerra*, Clausewitz delinea 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 comprensión de otros campos de batalla en los años consecuentes a la publicación de los textos de Clausewitz. En 1890, Alfred Tayer Mahan expandió la teoría de la guerra al espacio marítimo y determinó los factores estratégicos para la superioridad del poder naval (Nye, 2010). Para 1921, Giulio Douhet publicó su obra *El dominio del aire* y estableció los principios y ventajas del poder aéreo (Clodfelter, 2006). 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 y Sloan, 1999). Asimismo, el desarrollo de las armas estaría determinado por el medio geográfico en que serían utilizadas —tierra, mar, aire, etcétera— y debían de estructurarse para causar daño e impacto al enemigo en cada una de estas arenas (Kello, 2010: 23-32).

Las ideas anteriores, de capacidades y factores 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, 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 tanto, se vieron limitados a desarrollar un amplio margen de poder marítimo (Bolivia, Bielorrusia, Suiza, Kenia, etcétera). La misma condición aplicó para el campo aéreo o espacial, en los que el poderío de un Estado es determinado por la cantidad de arsenal (aeronaves) o desarrollo tecnológico (programa espacial) para detentar superioridad en estas esferas.

La comprensión 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 (Guzzini y Leander, 2005; Wendt, 1992). 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. Por otra parte, las interacciones entre los actores del sistema internacional y las capacidades intersubjetivas de cada Estado, u otros actores,

ayudan a delimitar su interés nacional o particular, así como su papel dentro de la estructura.

Las ideas vertidas anteriormente nos llevan a presentar 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. Está visión es cercana al paradigma neorrealista, escuela de la Ciencia Política que atendió el problema del ciberespacio y el concepto del *ciberpoder* desde 2010, a tres años del primer caso trascendental de análisis de los estudios de ciberseguridad (Estonia, 2007) y en vísperas del surgimiento de las ENCS en casi la mayoría de los países del mundo. Con la publicación del artículo *Cyber Power,* Joseph Nye (2010: 3-11) generó un esquema teórico que definió a este nuevo campo de influencia y acción política desde la perspectiva del poder del Estado-nación. Para este autor, la emergencia del ciberespacio como campo para ejercer el ciberpoder se asocia más a un proceso de *difusión de poder* que a una *transición de poder.* Esta transición está vinculada a la posesión o manipulación de información por parte de los gobiernos, función para la que está prácticamente diseñado el internet, y permite modificar la polaridad del poder en la estructura internacional, al menos en el ciberespacio. En ese sentido, los rápidos y vertiginosos avances de las tecnologías de información y la tajante disminución del costo, procesamiento y transmisión de éste hacen necesario que el Estado regule y controle la arena del internet, así como que construya doctrinas que consideren a éste como un elemento crucial para salvaguardar la integridad de la soberanía, interés y seguridad nacional en el ciberespacio.

Securitización del internet, inclusión de la ciberseguridad en la seguridad nacional y definición de ciber amenazas

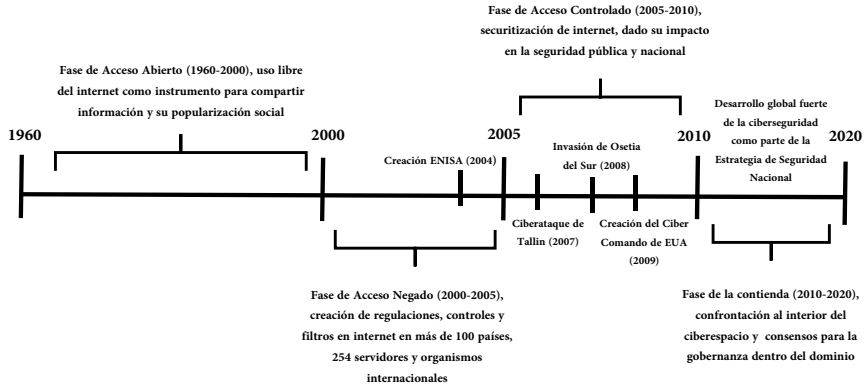
Para Palfrey (2010: 981-993) la securitización del internet fue una consecuencia del proceso de globalización y liberalización económica, que aconteció en la última década del siglo XX. En ese sentido,

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, Zitrain y Palfrey (2007: 16-19) documentaron que en ese periodo 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 cien países establecieron en sus códigos de justicia y sistemas penales definiciones sobre los ciber crímenes 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 intento de una armonización de ciber delitos (Palfrey, 2010; Klimburg; 2012, Take, 2012). Más tarde, surgió el primer conjunto de instituciones para prevenir ciber incidentes 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 la ciberseguridad en un aspecto clave de la 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 como se muestra en la Figura 1.

Figura 1. Fases de regulación del internet
e inclusión en la seguridad nacional



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

En la actualidad, la materialización de ciber incidentes es una constante de la rutina diaria y cotidianidad 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. 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 ciber amenazas, con relación a los efectos que tengan estos en el ciberespacio y el espacio físico, los cuales se presentan en el Cuadro 1.

De esta forma, los diferentes tipos de *malwares* o ciber armas pueden ser utilizados a diferentes escalas, ya que un ataque DDoS puede afectar desde un sistema informático de un individuo hasta

Cuadro 1. 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 Daña disponibilidad de acceso a sistemas o servicios
Compromiso	Roba información sensible. Comete un crimen financiero
Preparación	Causa molestia negando acceso a servicio o interrumpiéndolo

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

bloquear completamente una red gubernamental y un sistema bancario (Chauvin, 2016), o una brecha de información puede afectar desde la reputación de una persona hasta causar tensiones diplomáticas entre dos gobiernos (Benítez, 2011), por lo cual el grado de afectación de los diferentes tipos y modalidades de ciberataques no están condicionados por el medio 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 2, que afectan la estabilidad, seguridad e interés nacional del Estado-nación.

Entornos regionales y globales de ciberseguridad y la brecha de América Latina

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 para el Estado-nación. En ese sentido, un aspecto central de este documento es mostrar cómo América Latina se encuentra rezagada en el desarrollo de sus ciber capacidades 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 cien 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 ciber crimen, ENCS y consolidación de Equipos de Repuesta de Emergencia Informática (CERT), con el fin de mejorar las ciber capacidades 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 ciber capacidades 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

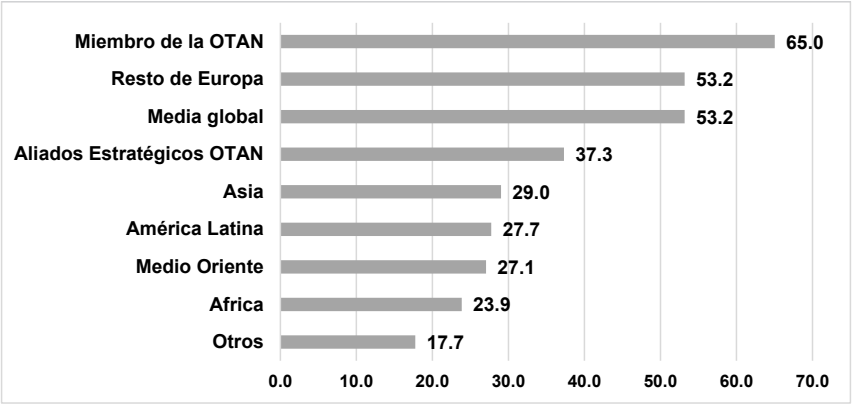
mundo con los cinco pilares de la Agenda Global de Ciberseguridad (AGCS), creada por la ITU, en 2007 (GCI, 2018: 8-10). Los objetivos del GCI son medir: 1) el tipo, nivel y evolución a lo largo del tiempo del compromiso de ciberseguridad en los países miembros de la ITU; 2) el progreso y seguimiento en el grado de compromiso de 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.

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 ciber crimen; 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 ciber capacidades, y 5) *Cooperación internacional*. Existencia de asociaciones, marcos cooperativos y redes de intercambio de información del gobierno.

La métrica evalúa a los 194 países del mundo a través de una ponderación que va del 0 al 100%, en la que 100 representa 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) Asia; 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. También se calculó una media global, obtenida de la calificación de los 194 países del mundo, que se muestra en la Gráfica 1.

La Gráfica 1 muestra que el conjunto de naciones más aventajado en el desarrollo de ciber capacidades y comprometido con la AGCS son los países miembros de la OTAN. Dado que los integrantes de

Gráfica 1. Media regional o de grupos de países en el desarrollo de cibercapacidades según el GCI (2018)



Fuente: Elaboración propia con base en GCI (2018).

dicha alianza ostentan una calificación en grupo de 79.2%, ponderación que está por encima 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 sólo por delante de regiones como África (25.2%) y Oceanía (11.9%).

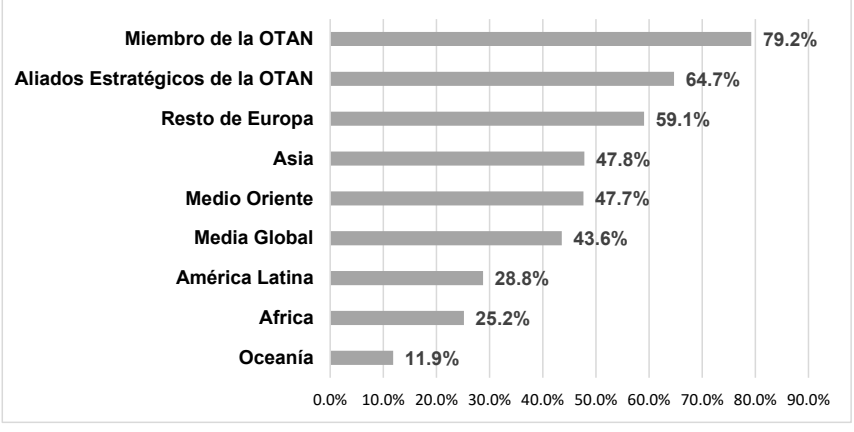
Respecto al NCSI (2018) de la *E-Governance Academy*, se destaca que esta medida evalúa la preparación de los países para prevenir ciber amenazas y gestionar ciber incidentes. En ese sentido, se expresa que el GCI (2018) mide el grado de compromiso e importancia que los Estados-nación han dado al tema de la ciberseguridad en el desarrollo de su política de seguridad nacional, mientras que la NCSI (2018) se compone de 12 indicadores, con una ponderación 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 ciber seguridad

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 ciber incidentes por parte de equipos de emergencia informática (CSIRT, CIRT) ante un ciber incidente; 10) capacidad de administración de ciber crisis del Estado-nación; 11) grado de compromiso del Estado para luchar contra el ciber crimen, y 12) capacidad de operaciones militares de las fuerzas armadas en el ciberespacio.

En ese sentido, se agrupó por regiones o conjunto de países a las naciones incluidas en la NSCI (2018). No obstante, dado que la NSCI sólo analiza un total de cien estados del mundo, éstos fueron separados en nueve subgrupos, como se muestra en la Gráfica 2.

La Gráfica 2 muestra de nuevo que los países de la OTAN son los más aventajados en la construcción de ciber capacidades de defensa, con una calificación de 65 puntos sobre 100. No obstante, un

Gráfica 2. Media regional o de grupos de países en capacidades de ciber defensa según la NSCI (2019)



Fuente: Elaboración propia con base en la NSCI (2019).

dato interesante derivado de la Figura 5 es que mientras los países aliados estratégicos de dicho organismo detentan la segunda posición en nivel de compromiso con la AGCS, en las cifras de la NSCI (2018) 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 Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), publicados en la última década. En cifras concretas, el incremento de ciber amenazas en la región fue de 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 a 92% de las entidades financieras con al menos un ciber ataque, 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 ciber capacidades para combatir amenazas provenientes del ciberespacio (BID, 2016: 20-22).

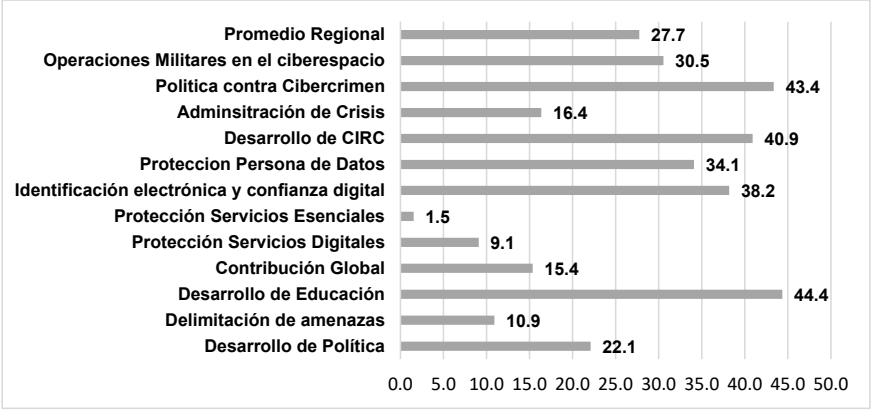
Respecto a reportes de firmas de ciberseguridad, PandaLabs (2015: 12-15) expresó que en 2014 países como Guatemala, Bolivia, Ecuador, Brasil y Perú se incluyeron entre las 10 principales naciones con más computadoras infectadas por virus maliciosos a escala global. Por su parte, IBM Security (2020) ubicó a la región como un punto que concentra 5% del total de actividad cibercriminal del 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 en 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 ciber incidentes, dado que sólo 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 de la NCSI (2018) vinculadas a ciber capacidades para atender ciber amenazas y se obtuvo la media regional de América Latina y el Caribe (27.7), que se presenta en la Gráfica 3.

La gráfica 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 ciber crimen (43.4 puntos) y desarrollo de educación (44.4 puntos). Sin embargo, la región no ha logrado una definición concisa de qué tipos de ciber amenazas 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 ciber amenazas (30.5 puntos).

Con relación a lo anterior, Moreno, Albornoz y Maqueo (2020: 32) expresan que América Latina y el Caribe están en una fase formativa

Gráfica 3. Media de indicadores de ciber capacidades en América Latina según la NCSI (2018)



Fuente: Elaboración propia con base en la NCSI (2018).

de desarrollo de ciber capacidades con base en lo expresado en el estudio del BID (2016: 20-22), que divide en cinco diferentes niveles de madurez el desarrollo de una ENCS y se explican en el Cuadro 2, en el 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.

Presentados los datos del Cuadro 2, se argumenta que la hipótesis de la que parte esta investigación se ha verificado según el análisis presentado por el GCI (2018), la NCSI (2018) y el BID (2016),

Cuadro 2. Nivel de madurez de las ENCS de América Latina según el BID

Nivel inicial	*Nivel formativo*	*Nivel establecido*	*Nivel estratégico*	*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 y privados).	Se ha establecido una ENCS y un mando específico para consultar los sectores estratégicos y la sociedad civil. Asimismo, existe una comprensión de riesgos y amenazas.	La ENCS se implementa por todas las partes interesadas y se conforma en 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 confianza entre las partes interesadas.
		Países en cada nivel		
1. Antigua y Barbuda	1. Argentina	1. Colombia	Ningún país de la región	Ningún país de la región
2. Bahamas	2. Brasil	2. Jamaica		
3. Barbados	3. Chile	3. Panamá		
4. Belice	4. Costa Rica	4. Trinidad y Tobago		
5. Bolivia	5. Dominica	5. Uruguay		
6. Ecuador	6. México			
7. El Salvador	7. Paraguay			
8. Granada	8. Perú			
9. Guatemala	9. San Vicente y las Granadinas			
10. Guyana	10. Surinam			
11. Haití				
12. Honduras				
13. Nicaragua				
14. República Dominicana				
15. Saint Kitts y Nevis				
16. Santa Lucía				
17. Venezuela				

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

a la par de contextualizar el creciente riesgo de ciber amenazas 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? Klimburg y Healey (2012: 70-74) dan una respuesta que expresa 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 ciber incidentes 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 ciber defensa 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), que 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 muestran en la Tabla 1.

Tabla 1. 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 Asia	2.3
Países de América Latina y el Caribe	1.12
Países de Medio Oriente y África	1.11

Fuente: CCDCOE Tallin (2020).

Crítica a la ENCS de México

Contexto del internet y ciberespacio en México

En México la penetración del internet alcanza a 60% de la población, lo que representa 71.3 millones de usuarios. El principal medio de acceso se da por *Smartphones* (89.7 % del total) y computadoras de escritorio y portátiles (34%) (Inegi, 2018). En el ámbito de las dinámicas del ciberespacio y ciber amenazas, durante 2017 las pérdidas económicas vinculadas a la ciberseguridad alcanzaron una cifra de 7.7 billones de dólares (Norton, 2018), mientras que durante los años que van del 2013 al 2016 los ciber ataques mostraron un incremento del 300%, al pasar de 20,000 a 60,000, a la par que se detectaron 5,000 páginas de ciber fraude en el dominio de México (Parraguez, 2016).

Por su parte, Norton (2018) resalta que los usuarios de internet gastaron 55.1 horas, en promedio al año, para resolver los problemas vinculados a infecciones o amenazas provenientes del ciberespacio. Y el principal medio de infección de computadores en el país es a través de *malwares*[1] (98%) y el resto se da por medio de *spear-pishing* (Espinosa, 2015). Vinculado a estas dos modalidades de ciber infección, resalta el incremento anual de efectividad de ambas durante 2015, con una tasa de crecimiento de 323% para el *malware* y 409% para *spear-pishing* (OEA/Symantec 2014), lo que denota que la ciberseguridad es débil en sectores privados y gubernamentales, e incluso alcanza el plano individual de los ciudadanos.

Ciberseguridad en el marco de la ENCS de México

La ciberseguridad es un tema presente en la agenda del gobierno de México. Desde 2013 existen por lo menos tres documentos que abordan el tópico: el *Plan Nacional de Desarrollo* (2013-2018), el

[1] Programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Programa de Seguridad Nacional (2014-2018) y el *Programa Nacional de Seguridad Pública* (2014-2018). Asimismo, en 2017 se creó la *Estrategia Nacional de Ciber Seguridad* (ENCS), con lo cual México se convirtió en el octavo[2] país en Latinoamérica en crear un documento de esta naturaleza. En el plano operativo, hasta 2018 la ENCS se coordinó por múltiples instituciones gubernamentales como la Comisión Nacional de Seguridad (CNS), la Secretaría de Gobernación (Segob), Policía Federal (PF), con División de Policía Científica, la Secretaría de la Defensa Nacional (Sedena) y la Secretaría de Marina (Semar). En acciones de ciberseguridad, datos de la Policía Científica destacan que hasta 2017 se atendieron 51,000 denuncias ciudadanas, más de 200,000 incidentes cibernéticos; desactivaron 17,000 sitios fraudulentos y emitieron más de 2,000 alertas de ciberseguridad (ENCS México, 2017).

También, esta división de la Policía Federal gestiona el Equipo de Respuesta de Incidentes Informáticos (*CERT*[3] *MX,* por sus siglas en inglés), el cual es miembro del Foro Global para Equipos de Respuesta a Incidentes y Seguridad (*FIRST*[4]). Otro elemento importante es el hecho de que las agencias gubernamentales utilizan el *Manual Administrativo General de Gestión de Tecnologías de la Información, Comunicaciones y Ciberseguridad*, de estándares ISO 27001. Por otra parte, el Instituto Nacional Mexicano de Acceso a la Información, Transparencia, Protección de Datos Personales (INAI) colabora en esfuerzos por una mayor transparencia y disponibilidad de información y sensibiliza a los ciudadanos de sus derechos como usuarios de internet.

En indicadores internacionales, la Unidad de Inteligencia Económica de la Consultora Booz Allen Hamilton, que evalúa el ciberpoder entre las naciones que conforman el Grupo de los 20 (G20), posicionó a México en el décimo primer lugar a través de una

[2] De acuerdo con Parraguez (2018), los otros países, según el orden de creación de una ENCS, son: Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Colombia (2011 y 2016), Paraguay, Chile, y Costa Rica (2017).

[3] CERT, del inglés *Computer Emergency Response Team* es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

[4] Siglas en inglés de *Forum of Incident Response and Security Teams.*

medición de 39 indicadores en atributos que contemplan aspectos como el marco legal, regulatorio, económico y social, la tecnología implantada y la aplicación industrial (García, 2018). Por otra parte, el Índice Global de Ciberseguridad (GCI, por sus siglas en inglés) de la Unión Internacional de Telecomunicaciones (ITU), que es considerado una referencia confiable que mide el compromiso de los países con la ciberseguridad a escala mundial (GCI, 2018), posicionó a México en el lugar 63, de un total de 153 países, en su más reciente informe, mientras que el Índice Nacional de Ciberseguridad (*National Cyber Security Index* o *NCSI* en inglés) o de la *E-Governance Academy* de Estonia, que es una medida encargada de evaluar la construcción de capacidades de defensa en el ciberespacio, calificaron a México en el lugar 57, de un total de cien países NSCI (2018). A pesar de que estas mediciones consideran que México detenta capacidades intermedias en cuestiones de ciberseguridad, es necesaria una crítica para mejorar la capacidad de acción de la ENCS del país y su capacidad de enfrentar ciber amenazas.

Revisión de la ENCS de México

La ENCS de México tiene como objetivo general:

> Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas el uso y aprovechamiento de las Tecnología de Información de la Comunicación (TIC) de manera responsable para el desarrollo sostenible del Estado Mexicano (ENCS México, 2017).

De acuerdo con Aguilar (2019), esta cita contiene múltiples elementos vinculados a la creación de capacidades de resiliencia en el ciberespacio, tales como su comprensión multidimensional (en la esfera social, económica y política) o la coordinación y cooperación de entidades públicas o privadas. A pesar de esto, en la segunda parte del objetivo general existe una confusión en la estrategia,

dado que está concentrada en incrementar la penetración del internet y consolidar su uso como un derecho universal, más que en crear capacidades de resiliencia ante ciber amenazas. Esta conclusión es más visible en el Cuadro 3, que presenta su estructura.

Cuadro 3. Estructura de la ENCS de México

Objetivos estratégicos	I. Sociedad y derechos. II. Economía e innovación. III. Instituciones públicas. IV. Seguridad pública. V. Seguridad nacional.
Principios rectores	1. Perspectiva de derechos humanos. 2. Enfoque basado en gestión de riesgos. 3. Colaboración multidisciplinaria y de múltiples actores.
Ocho ejes transversales	I. Cultura de ciberseguridad. II. Desarrollo de capacidades. III. Coordinación y colaboración. IV. Investigación, desarrollo e innovación TIC. V. Estándares y criterios técnicos. VI. Infraestructuras críticas. VII. Marco jurídico y autorregulación. VIII. Medición y seguimiento.

Fuente: ENSC México (2017).

El Cuadro 3 muestra cómo los objetivos estratégicos y los principios rectores de la ENCS se concentran en aumentar el uso del internet en México, aspecto que se vincula al concepto de *brecha digital,* que representa la separación que existe entre las personas que utilizan el internet y las tecnologías de la información como parte de su vida diaria y quienes no tienen acceso a ellas o no saben utilizarlas (Navarro *et al.,* 2018).La aún baja penetración del internet en México

explica el énfasis que pone el documento en mejorar su uso y acceso. La primera crítica a la ENCS que se identifica oscila en esta condición, dado que la reducción de la brecha digital entre usuarios y no usuarios corresponde a otro tipo de política pública, que no engloba una ENCS y no está vinculada con la seguridad nacional y la defensa de la soberanía del Estado-nación.

Por otro lado, el apartado de la ENCS más vinculado al desarrollo de capacidades de resiliencia en el ciberespacio se concentra en sus ocho ejes trasversales. Entre estos destacan: *a*) desarrollo de capacidades; *b*) coordinación y colaboración; *c*) infraestructuras críticas, y *d*) marco jurídico y autorregulación. No obstante, la ENCS se presenta más como un documento en construcción que no ha alcanzado la madurez necesaria para construir una cultura de ciberseguridad ni para transformarse en una política de ciberseguridad que contemple protocolos o mecanismos para consolidar capacidades de resiliencia y disuasión por parte del Estado-nación desde el ciberespacio.

También, se destaca que los apartados de desarrollo de capacidades, coordinación y colaboración, contienen oraciones ambiguas que no se concretan en indicadores, objetivos concretos o medibles, a la par que estas secciones deben incluir un organigrama de la política de cooperación entre las instituciones del gobierno encargadas de la ciberseguridad (como la División Científica, Sedena, Semar, Segob, etcétera), entre las que destaquen las facultades de cada una en la ENCS (Espinosa, 2015). Otra labor pendiente es identificar los vínculos y a los actores de la industria privada interesados en colaborar con el gobierno. En este sentido, resalta que, durante 2017, el mismo año de la publicación de la ENCS, la Cámara Nacional de la Industria Electrónica, Telecomunicaciones y Tecnologías de la Información (Canieti) presentó un informe relacionado con el tema, en el que solicitó al gobierno el establecimiento de una Agencia Nacional de Ciberseguridad que coordine la ENCS entre actores gubernamentales y privados, y establezca una ruta crítica para la gobernanza de internet en México (Parraguez, 2018).

Un aspecto de interés es que en el eje transversal de ICN se cita la Ley Nacional de Seguridad como el documento rector de la po-

lítica de ciberseguridad (ENCS, 2017). Sin embargo, no destaca acciones fundamentales para su protección como la actualización del catálogo de INC de México, así como la diferenciación entre cuáles deben ser administradas por entidades públicas y privadas. Del mismo modo, no se sugiere la elaboración de guías y estándares para su protección (Calderón, 2019).

Por último, en el eje de marco jurídico y autorregulación, destacamos la necesidad de una actualización de las legislaciones nacionales que engloban el ciberespacio con base en lo establecido en el Convenio de Budapest (García, 2018), una actualización sobre la clasificación de ciber delitos punibles (Espinosa, 2015) y la armonización de todas las leyes sobre delitos informáticos (Parraguez, 2018). En el Cuadro 4 se presentan varias legislaciones nacionales que requieren una armonización en el marco de la ENCS de México.

La crítica realizada a la ENCS de México devela que existe una marcada distancia entre el entorno actual de ciber amenazas a escala global y la configuración de este documento. Asimismo, no hay una concordancia o revisión para el aprendizaje de experiencias internacionales para comprender el potencial del ciberespacio como un instrumento para vulnerar la seguridad pública o nacional, en una escala local, nacional o internacional, que comprenda que las crisis surgidas en esta arena pueden brincar del espacio virtual al material.

Como propuesta de análisis para la promoción de una agenda de ciberseguridad presentaremos la categoría de *hecho ciberfísico* (Aguilar, 2019), que explicaremos a través del ciber ataque de Tallin (2007) para la comprensión de las características del régimen híbrido del ciberespacio, que deben ser incorporadas en la visión estrategia de la ENCS de México.

Cuadro 4. Leyes susceptibles de homologación en el marco de la ENCS de México

Legislación o Código	*Artículo/ Fracción*	*Temática*
Constitución Política de los Estados Unidos Mexicanos.	Art. 16	Inviolabilidad de las comunicaciones y la protección de los datos personales.
Código Penal Federal	Arts. 167, Fracc. VI, y 177	Sanción por la interrupción, interferencia e intervención de comunicaciones electrónicas.
Código Penal Federal	Arts. 202 y 202 Bis	Almacenamiento y difusión de pornografía infantil por medios electrónicos.
Código Penal Federal	Art. 211 Bis 1-7	Acceso ilícito a equipos y sistemas de informática.
Código Penal Federal	Art. 424 Bis	Creación de programas para desactivar la protección de otros.
Ley Federal del Derecho de Autor	Título IV, Capítulo IV	Regulación de la copia, alteración y reproducción de software y bases de datos.
Ley Federal de Protección al Consumidor	Arts. 18 Bis y 76 Bis	Regulación sobre el envío de publicidad no deseada (*spam*) y los derechos en las transacciones a través de medios electrónicos.
Ley Federal de Instituciones de Crédito	Art. 112 Bis, Fracc. IV y VI	Tipificación de la alteración, copia o reproducción de la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquier instrumento de pago.
La Ley Federal de Telecomunicaciones y Radiodifusión	Art. 298, Inciso B, Fracc. I; D, Fracc. III y V	Pena al bloqueo del servicio de internet; intercepción de la información transmitida en redes públicas y no adopción de medidas para garantizar la confidencialidad y privacidad de comunicaciones.

Fuente: Elaboración propia con base en Espinosa (2015), García (2018) y Parraguez (2018).

Propuesta de mejora de la ENCS en México y la creación de la Agencia Nacional de Ciberseguridad

Entornos VUCAH

La discusión anterior sirve para demostrar los retos que enfrentan los países latinoamericanos frente a los riesgos emanados del ciberespacio y la necesidad de construcción de capacidades de defensa, resiliencia y disuasión en este dominio. De esta forma, nuestra crítica de la ENCS y la presentación de la categoría de ciberfísico se vinculan con nuevos retos a la seguridad nacional como la migración, las pandemias, el cambio climático, crimen organizado, etcétera, que son fenómenos que tienen convergencia de sistemas ciber-físicos basados en tecnologías emergentes como la inteligencia artificial, internet de las cosas, big data, drones, impresión 3D, tecnología 5G, computación cuántica, etcétera.

Estas mega tendencias se enmarcan en entornos VUCAH (acrónimo en inglés de las palabras (*Volatility*, *Uncertainty*, *Complexity*, *Ambiguity*) que, si bien sus orígenes se remontan a la década de 1990 (Bennett y Lemoine, 2014) para definir el escenario surgido tras la Guerra Fría en un espacio físico conocido, en años recientes se ha añadido un factor más a este enfoque prospectivo (*Hiperconnectivity*) respecto a la conexión entre dispositivos y tecnologías en un ciberespacio muchas veces desconocido (MacManus, 2014). Estos entornos en el uso y aprovechamiento de los sistemas ciber-físicos sin duda pueden representar fortalezas y capacidades para mejorar los productos y servicios de los Estados, pero también representan una gran amenaza y riesgo, ya que al hablar de un ciberespacio, inherentemente se habla también de vulnerabilidades. Es por ello que los Estados deben de preservar la condición de seguridad, considerando la protección de las ciber amenazas y fomentar una prosperidad económica en un entorno conectado por sistemas ciber-físicos a través del uso y aprovechamiento de la tecnología. Este primer análisis nos invita a prepararnos y anticiparnos como países, organizaciones y personas para preservar una condición de ciberseguridad y para incluir un análisis prospectivo

como el planteado por el enfoque VUCAH ante los retos de la ciberseguridad que se vislumbran en el futuro en México y América Latina.

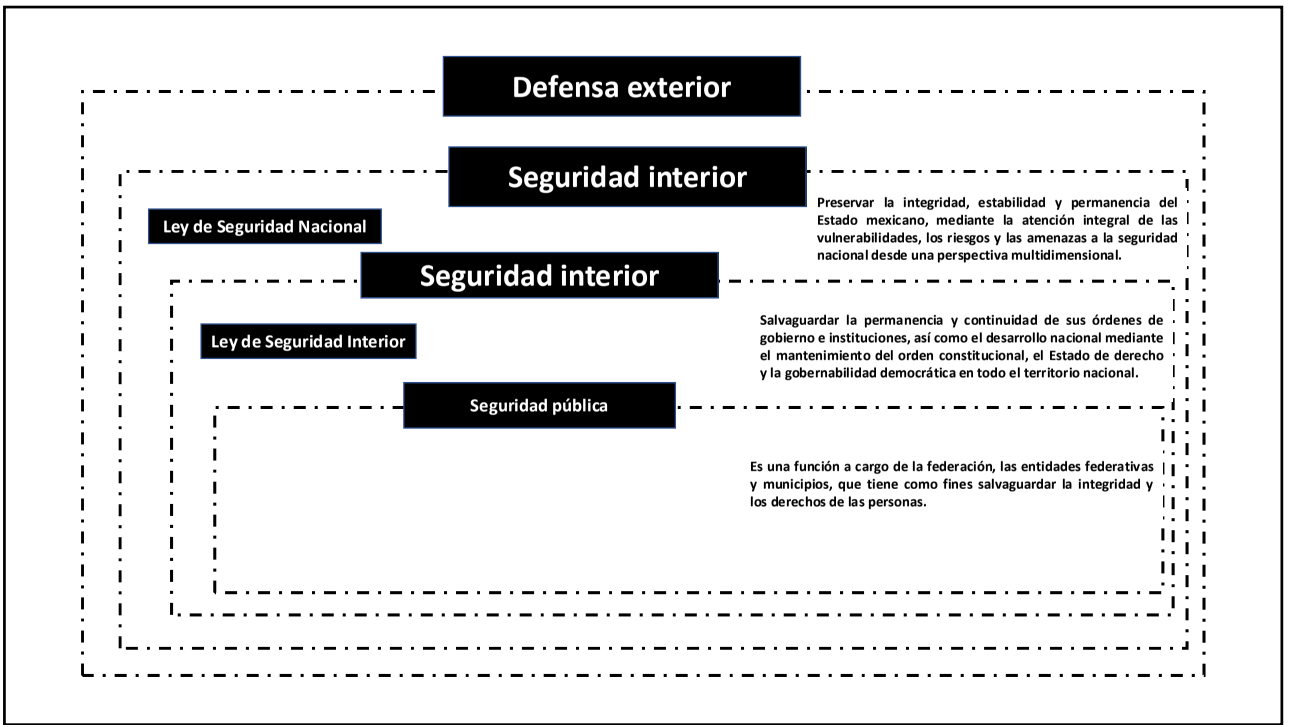
Ciberseguridad en el sistema de seguridad nacional en México

En la actualidad, existe una confusión en la utilización de términos como *ciberseguridad* y *ciberdefensa*, que a menudo se usan indistintamente, y confunden la noción certera de lo que es la ciberseguridad, como es el caso de México y gran parte de las ENCS de la región de América Latina. En ese sentido, se especifica que la ciberseguridad hace referencia a la protección del ciberespacio de forma general, y la ciberdefensa se refiere a la protección del ciberespacio de una nación. Asimismo, otro término que se utiliza en el desarrollo de capacidades de defensa en el ciberespacio es la categoría de *ciberpoder*, el cual se refiere al poder nacional que tiene un país para poder usar este dominio con el fin de salvaguardar la integridad de la nación y perseguir sus intereses nacionales (Nye, 2010).

En el análisis de la ciberseguridad en México, resulta relevante analizar desde el enfoque multidimensional del modelo de seguridad actual en México, como se presenta en la Figura 2. Este modelo pretende ejemplificar los conceptos de defensa exterior, seguridad nacional, seguridad interior y seguridad pública de acuerdo a los alcances de acuerdo al marco normativo vigente en México. Para el caso de la ciberseguridad se propone ubicarlo en el nivel de seguridad nacional, donde tiene la función de preservar la integridad, estabilidad y permanencia del Estado mexicano, mediante la atención integral de las vulnerabilidades, los riesgos y las amenazas a la Seguridad Nacional, desde una perspectiva multidimensional.

La ventaja de ubicar la ciberseguridad en el nivel de seguridad nacional tiene una razón de perspectiva multidimensional, además de retomar la atención integral de las vulnerabilidades, riegos y amenazas a la seguridad nacional que puedan ocurrir en el ciberespacio. Asimismo, esta visión se conjunta con la visión de las gramáticas de seguridad presentadas en el análisis del caso de Tallin (2007), que demuestran que un ciber incidente o una agresión

Figura 2. Sistema de seguridad en México



Fuente: Elaboración propia.

cibernética puede saltar de la esfera de la seguridad pública a la nacional, e incluso internacional, a la par de contemplar que por las características del régimen híbrido del ciberespacio es necesario tener una perspectiva multidimensional que contemple a este dominio como una esfera de la que pueden emanar amenazas a la seguridad nacional en todos sus niveles.

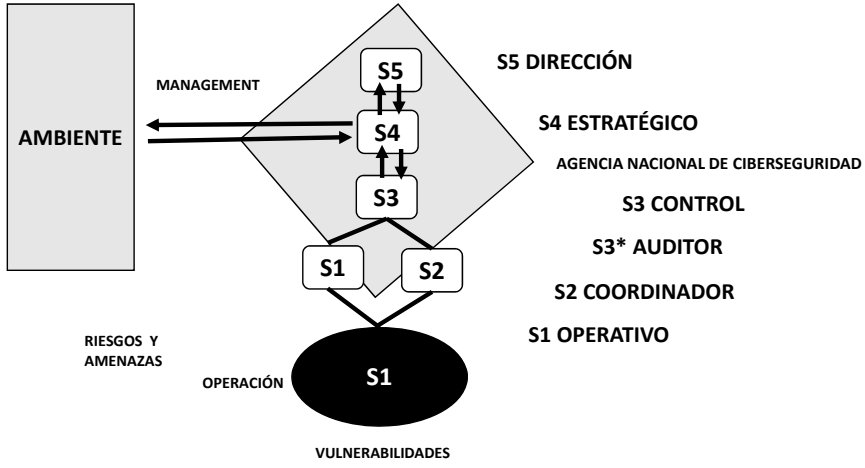
Hacia una agencia de ciberseguridad en México

Dentro del presente artículo se analizó la diversidad de puntos de vista y comprensiones en espacios académicos, legislativos y ENCS, sobre la necesidad de contar con una institución que sea la encargada de coordinar la ciberseguridad en México. Debido a su complejidad y a la participación de múltiples actores del Estado mexicano, se plantea la posibilidad de construir un sistema orgánico que distinga al subsistema conducente de la política de ciberseguridad encargado de realizar la planeación, anticipación, dirección e inteligencia, así como un sistema conducido encargado de realizar la ejecución y coordinación de los proyectos y programas en ciberseguridad.

Para que este sistema orgánico funcione deberá de existir un intercambio de conocimiento (*top down*) del subsistema conducente al sistema conducido, y viceversa, en un intercambio de información (*bottom up*) del subsistema conducido al subsistema conducente. Para el diseño de este sistema orgánico del sistema de ciberseguridad se retoma el *Modelo de Sistemas Viables* propuesto por Stafford Beer basado en el enfoque cibernético que potencia el intercambio de información y control entre áreas y funciones sustantivas (Ríos *et al.*, 2008), que se presenta en la Figura 3.

En esta propuesta de modelo de seguridad cibernética se propone la creación de una Agencia Nacional de Ciberseguridad (ANC) que sea la entidad que realice la función de identificar los riesgos y amenazas que derivan del entorno, además de contribuir a la cooperación, coordinación y permanencia constante con las diferentes unidades operativas de las fuerzas de seguridad, fuerzas armadas y

Figura 3. Sistema orgánico de ciberseguridad



Fuente: Elaboración propia.

aquellas dependencias encargadas de salvaguardar las infraestructuras críticas. Para estas unidades operativas se propone que estén conformadas por las Direcciones de Tecnologías de la Información y Comunicaciones (TIC´s), donde se encuentran los especialistas en el tema, quienes serán los encargados de ejecutar programas y proyectos de prevención, protección, mitigación, respuesta y restablecimiento ante probables riesgos y amenazas complejas en el ciberespacio, lo cual ayudaría al desarrollo de ciber capacidades como la resiliencia y disuasión por parte del Estado mexicano para encarar el contexto global de ciber amenazas que existen en la actualidad. En la Figura 2 se denota la importancia de contar con hilos conductores de comunicación bilateral, desde la dirección de la política de ciberseguridad, la planeación estratégica, el control, hasta la auditoría y la operación, que se traduzcan en proyectos y programas para preservar la condición de seguridad en el ciberespacio.

Hacia un modelo prospectivo de la ciberseguridad

En el análisis a la ENCS se identificaron las principales variables que permiten proponer un modelo prospectivo de ciberseguridad en México hacia el año 2030 con base en la adopción y complejidad en la materia (estas variables se representan en la Figura 4). Dicho modelo puede aplicase a los países latinoamericanos a partir de las similitudes y coincidencias políticas, sociales, técnicas, económicas y culturales desde sus instituciones, instrumentos y tecnología disponible.

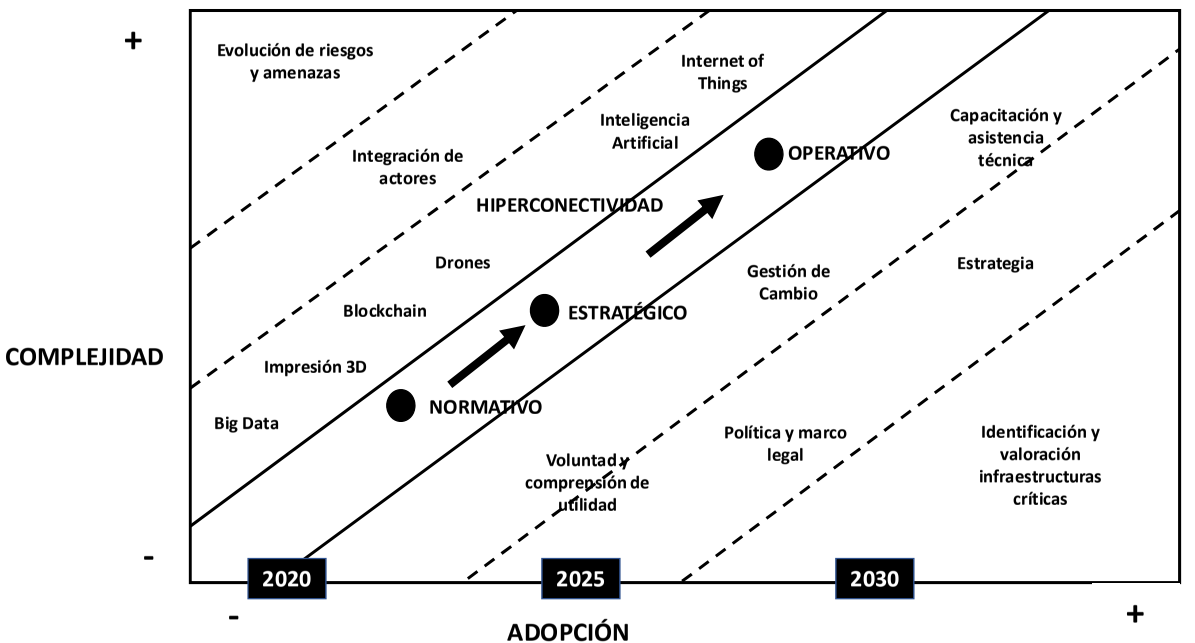
El presente modelo versa sobre el incremento de la adopción y la complejidad de la ciberseguridad con respecto al paso del tiempo, donde el Estado mexicano deberá prepararse con instrumentos normativos, estratégicos y operativos para hacer frente a la hiperconectividad entre las tecnologías exponenciales, lo cual derivará en la inclusión de actores e instituciones con la finalidad de realizar una gestión de riesgos y amenazas al ciberespacio, visión que puede ayudar al desarrollo y fortalecimiento de sus cibercapacidades.

Los retos de la ciberseguridad en México

La presente investigación cierra con la contextualización de tres casos de ciber amenazas que ha enfrentado el Estado mexicano, los cuales muestran la importancia de elevar a carácter de esquema de seguridad nacional la construcción de ciber capacidades de defensa por parte de nuestro país, que son:

- El *Cablegate* de la organización hacktivista Wikileaks, en 2011, de más de 250,000 cables de seguridad e inteligencia del departamento de Estado, en los que se vertió información sobre la estrategia de combate al crimen organizado en México, así como información de la descoordinación de los actores al frente de las instituciones de seguridad del país (Benítez, 2011). Dicha filtración causó una breve crisis diplomática que culminó con la declaración de persona *non*

Figura 4. Modelo prospectivo de ciberseguridad hacia el 2030



Fuente: Elaboración propia.

grata del embajador de Estados Unidos en México, Carlos Pascual, ese mismo año (Flores y Magallanes, 2011).

- Los dos importantes ciberataques al Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México (BM) en 2018. El primero detectado en abril e involucró a tres bancos privados, una casa de bolsa y una caja de ahorro popular, en el que se estima hubo pérdidas de alrededor de 300 millones de pesos (Valdelamar, 2018). El segundo fue ejecutado en octubre, a través de la aseguradora AXA, institución privada, mediante la cual los agresores infiltraron el SPEI y realizaron múltiples operaciones anómalas que elevaron a rojo el nivel de alerta de seguridad informática en las operaciones del SPEI (Estañol, 2018) y que, de acuerdo con la firma de ciberseguridad Fire Eye, se detectó que los culpables del incidente fueron el equipo de hackers APT38, una cédula norcoreana encargada de ejecutar ciberataques a bancos de naciones extranjeras para obtener recursos para su país, famosos por haber vulnerado 16 instituciones bancarias en 11 países y extraído 100 millones de dólares (Lara, 2018).
- El ciberataque de *ramsonware* a la paraestatal mexicana Petróleos Mexicanos (Pemex) durante noviembre de 2019, empresa que está al centro de la política económica del Plan Nacional de Desarrollo (Ordaz, 2019) y se encuentra en un proceso de reestructuración y plan de rescate para salvar sus finanzas, proyecto que está en evaluación por parte de entidades financieras internacionales como las calificadoras internacionales *Fitch, Moody´s* y *Standar & Poor,* y que con dicho ciberataque afectaron su operación para el pago de deuda internacional y nómina, proceso que puede afectar su calificación y prestigio a escala internacional, dado que el rescate que se pidió para regresar el control de la red de operaciones por parte de los hackers osciló entre 4.9 millones de dólares, uno de los más caros en la historia de América Latina (Riquelme, 2019).

Conclusiones

Con base en lo analizado en el presente artículo, más que una estrategia en ciberseguridad, lo más importante y necesario es formular una visión prospectiva y estratégica que responda a los retos de la ciberseguridad a nivel global y en México. En ese sentido, resultan vitales cuestionamientos como qué, para qué, quién, cuándo y hacia dónde se dirige la política de ciberseguridad en nuestro país, así como cuáles son los esfuerzos para mejorarla en aras de construir capacidades de ciberdefensa que garanticen la seguridad nacional y la soberanía del Estado mexicano.

De esta forma, es necesario comprender que el ciberespacio es un nuevo espacio de confrontación e influencia entre los Estados-nación, así como una esfera que debe regularse para garantizar la seguridad nacional. Para ello es necesario que haya una declaración de intención hacia el futuro que pueda socializarse desde el gobierno y las instituciones de seguridad del país, en conjunto con los actores y partes interesadas, y que ésta se traduzca en una política de ciberseguridad en México, que deberá influir en nuevas reformas legales en materia de seguridad nacional y ciberseguridad en aras de construir capacidades de defensa en el ciberespacio.

Referencias bibliográficas

Aguilar, J. (2019), "Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad", *Urvio. Revista Latinoamericana de Estudios de Seguridad*, núm. 25, diciembre-mayo, Flacso, pp. 24-40.

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

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

—— (2005), *Seguridad hemisférica: debates y desafíos* (vol. 4), México, UNAM.

—— (2011), "México, Centroamérica y Estados Unidos: migración y seguridad", en *Migración y seguridad: nuevo desafío en México*, México, Colectivo de Análisis de la Seguridad con Democracia.

Bennett, N. y Lemoine, J. (2014), "What VUCA really means for you", *Harvard Business Review*, núm. 92 (1/2).

Buzan, B., Wever O. y De Wilde, J. (1998), *Security: A new framework for analysis*, Boulder, Lynne Rienner.

Calderón, J. (2018), Infraestructura crítica en México: el enfoque hacia el futuro, 03/05/2018. Disponible en: https://bit.ly/35kO3eE

CCDCOE Tallin (2020), Strategy and Governance. Cooperative Cyber Defence Centre of Excellence. Disponible en: https://bit.ly/37I-0jrm

Chauvin, J. (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'"?, tesis para obtener el grado de Master of Arts in International Politics of the Internet, Aberystwyth University.

Clodfelter, M. (2006), *The limits of air power: The American bombing of North Vietnam*, University of Nebraska Press.

Cornaglia, S. y Vercelli, A. (2017), "La ciberdefensa y su regulación legal en Argentina (2006-2015)", *Urvio. Revista Latinoamericana de Estudios de Seguridad*, núm. 20, pp. 46-62.

Curtis, S. (2011), "Global cities and the transformation of the International System", *Review of International Studies*, vol. 37, núm. 4, pp. 1923-1947.

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

Digital Attack Map (2019), *Digital Attack Map*. Disponible en https://bit.ly/2qPHqCe

ENCS México (2017), Estrategia Nacional de Ciberseguridad, 12/12/2019. Disponible en https://bit.ly/2AEvAtU

Espinosa, I. (2015), "Hacia una estrategia nacional de ciberseguridad en México", *Revista de Administración Pública*, vol. 50, núm. 1, pp. 115-147.

Estañol, A. (2018), "La aseguradora AXA sufre un ciberataque en el Sistema de Pagos Electrónicos", *Expansión*, 23/10/2018. Disponible en https://bit.ly/2KrDtdL

Flores, A. y Magallanes, C. (2011), WikiLeaks in Mexico: a penetrated State, the fall of an ambassador and a frustrated president.

García, A. (2018), "CiberMéxico: voluntades y acciones en el ciberespacio", IUS Literarus.

GBA & ITRC (2018), The Impact of Cybersecurity Incidents on Financial Institutions. Identity Theft Resource Center Generali Global Assistance. Disponible en https://bit.ly/373fHOR

GCI (2018), Global Cybersecurity Index. International Telecommunication Union. Disponible en https://bit.ly/34rPZ4C

Gray, C. S. y Sloan, G. (eds.) (1999), *Geopolitics, Geography and Strategy*, Londres, Frank Cass.

Guzzini, S. y Leander, A. (2005), *Constructivism and international relations: Alexander Wendt and his critics*, Londres, Routledge.

Hansen, L. y Nissenbaum, H. (2009), "Digital disaster, cyber security, and the Copenhagen School", *International Studies Quarterly*, vol. 53, núm. 4, pp. 1155-1175.

Hoerder, D. (2010), "Recent methodological and conceptual approaches to migration: Comparing the globe or the North Atlantic world?", *Journal of American Ethnic History*, vol. 29, núm. 2, pp. 79-84.

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

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

Inegi (Instituto Nacional de Estadística y Geografía) (2018), "Comunicado de Prensa Núm. 105/18", 12/12/2019. Disponible en https://bit.ly/2MWpoab

Kapersky (2019), Cyberthreat Real-Time Map. Disponible en https://bit.ly/2XQbn17

Keeling, D. (2004), "Latin American development and the globalization imperative: New directions, familiar crises", *Journal of Latin American Geography*, vol. 3, núm. 1, pp. 1-21.

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

Klimburg, A. (2011), "Mobilising cyber power", *Survival*, vol. 53, núm. 1, pp. 41-60.

Klimburg, A. y Healey, J. (2012), "Strategic Goals & Stakeholders", en Klimburg, A. (ed.), *National Cyber Security Framework Manual*, Tallinn, Estonia, NATO CCD COE Publication, pp. 66 -107.

Lindstrom, G. y Luiijf, E. (2012), *2. Political Aims & Policy Methods. Studies*, (Cambridge, Cambridge University Press, 2009).

MacManus, T. (2014), "Civil society and state-corporate crime: A case study of Ivory Coast", *State Crime Journal*, vol. 3, núm. 2, pp. 200-219.

Martínez, R. (2007), "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE", *El País*, 18/05/2007. Disponible en https://bit.ly/2OQ034c

Martins, M. (2009), "International Law as Glocal Law. Proceedings of the Annual Meeting", *American Society of International Law*, núm. 103, pp. 475-476.

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

Navarro, D., López, R., Domínguez, M. y de León Castañeda, C. (2018), "La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México", *Entreciencias: Diálogos en la Sociedad del Conocimiento*, vol. 6, núm. 16, pp. 49-64.

NCSI (2018), National Cyber Security Index. E-Governance Academy. Disponible en https://bit.ly/2XS1eAR

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

Noonan, E. (2016), "White House Unveils Color-Coded Scale for Cyber Security Threat", Cybersheat Service International, 29 de

julio. Disponible en https://cybersheath.com/white-house-unveils-color-coded-scale-for-cyber-security-threats/

Nye, Joshep (2010), *Cyber power*, Cambridge, Harvard University Press.

OEA (Organización de los Estados Americanos) (2018), Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. Disponible en: https://bit.ly/2Z1ZBUa

OEA (Organización de los Estados Americanos) / Symantec (2014), "Tendencias de seguridad cibernética en América Latina y el Caribe". Disponible en https://bit.ly/2Kz0sT2

Ordaz, Y. (2019), "¿Qué es el ransomware? El virus que atacó a Pemex", *Milenio*, 13/11/2019. Disponible en https://bit.ly/36zoVRx

Palfrey, J. (2010), "Four phases of Internet regulation", *Social Research*, vol. 77, núm. 3, pp. 981-996.

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

Parraguez, L. (2018), "Quo Vadis? Mexico's National Cybersecurity Strategy", Wilson Center, 03, 31 de mayo. Disponible en https://bit.ly/2TpovYY

Peck, J. y Tickell, A. (1994), "Searching for a new institutional fix: the after-Fordist crisis and the global-local disorder", en Ash Amin (ed.), *Post-Fordism: A reader*, Cambridge, Mass., Blackwell, pp. 280-315.

Pessiri, P. (2019), "2018: A year of cyber attacks", Hackmageddon, 15 de enero de 2019. Disponible en https://bit.ly/2Da7k7d

Ríos, J., Mayoral, P. y Regaliza, J. (2008), "Sistemas de Información y Cibernética Organizacional", en *II International Conference on Industrial Engineering and Industrial Management* (pp. 417-428).

Riquelme, R. (2019), "El rescate por el hackeo a Pemex es el segundo mayor por ransomware", *El Financiero*, 15/11/2019. Disponible en https://bit.ly/2YIIwMx

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

Sicherheitstacho (2019), Overview of Current Cyber Attacks. Deutsche Telekom. Disponible en https://bit.ly/2OeLLGH

Sidaway, J. (2006), "On the Nature of the Beast: Re-Charting Political Geographies of the European Union", *Geografiska Annaler*, Series B, Human Geography, vol. 88, núm. 1, pp. 1-14.

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

Tamkin, E. (2017), "10 years after the landmark attack on Estonia. Is the world better prepared for cyber threats?", *Foreign Policy*, 27/04/2017. Disponible en: https://bit.ly/2HCvY4H

Taylor, P. J. (1996), "Embedded statism and the social sciences: Opening up to new spaces", *Environment and Planning A*, vol. 28, pp. 1917-1928.

Valdelamar, J. (2018), "5 entidades y 300 mdp, involucrados en ciberataque: Banxico", *El Financiero*, 16/05/2018. Disponible en https://bit.ly/2YEdb0J

Van Wijk, J., y Bolhuis, M. (2017), "Awareness trainings and detecting jihadists among asylum seekers: A case study from The Netherlands", *Perspectives on Terrorism*, vol. 11, núm. 4, pp. 39-49.

Wendt, A. (1992), "Anarchy is what states make of it: The social construction of power politics", *International organization*, vol. 46, núm. 2, pp. 391-425.

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

Zittrain, J., y Palfrey, J. (2007), *Access denied: The practice and policy of global Internet filtering*, Oxford Internet Institute.