INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS DE LA ARMADA DE MÉXICO

DA 48/18
05/09/18

Maestro
Adolfo Arreola García[1]

Ciberseguridad Nacional en México y sus desafíos

RESUMEN

Debido a los avances tecnológicos los Estados enfrentan nuevos desafíos en la llamada Era de la Información. Estos desafíos están ligados a la falta de protección y al mal uso del ciberespacio, que se ha convertido en el quinto ámbito de la guerra. Visto desde la perspectiva de la seguridad nacional, la dependencia en las tecnologías de la información y comunicaciones (TIC) ha acelerado los procesos, pero aumentado las vulnerabilidades. Por ello, los Estados han buscado salvaguardar la ciberseguridad a través de medidas políticas, tecnológicas y estratégicas que incluyen claridad en los conceptos y atribuciones de los actores. Es decir, el concepto de seguridad ha evolucionado para incluir los aspectos tecnológicos que hoy predominan bajo el termino de ciberseguridad nacional. Por ello, los Estados han diseñado ciberestrategias para contrarrestar las diversas amenazas del ciberespacio y los desafíos que deben enfrentar en cuestiones de estrategia, recursos humanos y desarrollo tecnológico.

Palabras clave: ciberseguridad, ciberespacio, ciberguerra, ciberestrategia, ciberamenaza.

Abstract

Due to technological advances, States face new challenges in the so-called Information Age. These challenges are linked to the lack of protection and misuse of cyberspace, which has become the fifth domain of war. Seen from the perspective of national security, reliance on information and communication technologies (ICT) has accelerated processes, but it has also increased vulnerabilities. Therefore, States have sought to safeguard cybersecurity through political, technological and strategic measures that include clarity in the concepts and attributions of the actors. In other words, the concept of national security has evolved to include the predominant technological aspects of today´s world under the term of national cybersecurity.

[1] Es profesor investigador en la Universidad Anáhuac México Norte y profesor en la Facultad de Estudios Superiores Acatlán, de la Universidad Nacional Autónoma de México (UNAM). De igual manera se desempeña como consultor independiente en ciberseguridad estratégica. Sus líneas de investigación se enfocan en temas de seguridad nacional, ciberseguridad en todos los ámbitos y tecnología aplicada a la seguridad nacional. Es doctorando del Doctorado en Seguridad Internacional de la Universidad Anáhuac México Norte. Para contacto: adolfoarreola@yahoo.com.mx

Therefore, States have designed cyberstrategies to counter the different threats in the cyberspace and the challenges they must face in issues of strategy, human resources and technological development.

Key words: cybersecurity, cyberspace, cyberwar, cyberstrategy, cyberthreat

Este trabajo se basa en el análisis literario de discursos e histórico de diversos documentos oficiales, académicos, gubernamentales, tecnológicos y mediáticos que permiten abordar el tema desde perspectivas teóricas y mediático-realistas, esto es a partir de los acontecimientos que ocurren en el diario acontecer. Con ello se busca la correlación de los acontecimientos cotidianos con la explicación teórica de los mismos; ya que la historia, al ser fuente esencial de información, presenta una serie de indicadores y eventos repetitivos, así como recurrentes que dan oportunidad para anticiparse a los hechos al poner en práctica los preceptos teóricos.

El objetivo de este documento es identificar algunas de las medidas políticas, tecnológicas y estratégicas que incluyen claridad en los conceptos y atribuciones de los actores que toman parte en el sistema de ciberseguridad nacional. Se inicia con una discusión sobre la pertinencia de contar con definiciones claras de seguridad y ciberseguridad nacional para instrumentar las medidas de mitigación de riesgos que sean necesarias; posteriormente se hace una descripción de los elementos normativos de la seguridad nacional en México y el desafío que representa contar con tanto una definición de ciberseguridad como con una estrategia efectiva. Después de lo anterior, se menciona el propósito de la ciberestrategia en el contexto mexicano y además proponiendo un sistema de ciberseguridad nacional. Finalmente, se habla sobre la formación de capital humano profesional en temas de ciberseguridad y el desarrollo de tecnología propia con el fin de fortalecer la ciberseguridad nacional.

Introducción

En el siglo XXI, el empleo intensivo de sistemas computarizados por todos los actores de la sociedad, incluyendo las fuerzas armadas, ha tenido un crecimiento exponencial (García, 2014, p. 6). Sin duda alguna, la sociedad moderna emplea a las Tecnologías de la Información y Comunicaciones (TIC) como instrumentos de organización, control, gobierno y administración de la información. En respuesta, esta situación de dependencia en medios electromagnéticos ha traído consigo las vulnerabilidades inherentes de dichos sistemas digitales, poniendo en riesgo la seguridad de los Estados, organismos e individuos. El empleo intensivo de los medios digitales invita a pensar en una hiperconectividad (Dawson et al, 2016) y en nuevos desafíos que atentan contra la integridad, confiabilidad y disponibilidad de la información (Baheti y Gill, 2016) y ponen en riesgo la seguridad nacional.

Desde el contexto de la seguridad nacional, junto con la dependencia en las TIC en los diversos ámbitos del desarrollo de los Estados, existe una necesidad creciente de verificar la implementación segura de los

sistemas cibernéticos en campos como la salud, la educación, los servicios gubernamentales o la industria; es decir se deben construir capacidades para la ciberseguridad y la ciberdefensa con base en políticas públicas de largo alcance, así como en instituciones de carácter permanente que den vida a un sistema de ciberseguridad nacional. (Cano, 2011; Artiles, 2011; y Lynn, 2010)

En el caso de México los eventos por ciberataques[2] se han multiplicado (Farivar, 2009; Cruz, 2015), sin que el gobierno haya estructurado una política nacional de ciberseguridad integral. Esto último a pesar de las pérdidas reportadas por algunas organizaciones civiles/comerciales (Córdova, 2016), y los ciberataques reportados por instituciones como Petróleos Mexicanos, (¡Cuidado, Pemex, 2015) Comisión Federal e incluso la Presidencia de la República (Ángel, 2013).

En consecuencia, el presente trabajo se centra en tres elementos fundamentales para la ciberseguridad nacional: la evolución de la seguridad para dar vida al concepto de ciberseguridad, la ciberestrategia y la incorporación/creación de elementos humanos-institucionales.

De la seguridad física a la seguridad virtual

En el contexto internacional del siglo XXI, donde las TIC tienen un papel preponderante, es preciso contar con un concepto y una estrategia[3] de seguridad nacional que implementen acciones políticas y jurídicas para salvaguardar los recursos materiales en todos los ámbitos de combate[4] desde una perspectiva multidisciplinaria, multidimensional y multinivel. Recordando que, si bien la definición tradicional de seguridad nacional funcionó antes y durante la Guerra Fría, pero después del fin de esta lucha ideológica el concepto de seguridad muestra huellas de cansancio. En consecuencia, en el escenario internacional del presente existe un debate para reconceptualizar la seguridad e incorporar nuevos ámbitos, actores, factores y temas (Dalby, 1997).

Ampliar el concepto de seguridad ha permitido la incorporación de actores no estatales y temas no militares (Buzan, Wæver, & De Wilde, 1998: 2-3 y Ullman, 1983); y dicha ampliación ha traído consigo no sólo beneficios, sino también **nuevas amenazas**. Por lo tanto, en un entorno internacional interconectado es imperativo revisar ¿qué se entiende por seguridad?, ¿cuál es el objetivo de la seguridad?, ¿cuáles son las amenazas?, y ¿con qué medios se cuenta para tal efecto? Es decir, hay que buscar el éxito estratégico a través de un plan flexible, dinámico e incluyente que requiere de la inclusión del **ciberespacio** como el quinto

[2] No existe una definición universalmente aceptada para ciberataque; sin embargo, aquí debe ser entendido dicho concepto como: Un acto hostil que utiliza computadoras, redes o sistemas relacionados, y tiene la intención de interrumpir y/o destruir los sistemas, activos o funciones cibernéticos críticos de un adversario. Que es la definición de la doctrina estadounidense publicada en 2011.
[3] Nuestra propuesta para el concepto de estrategia es: serie de acciones meticulosamente estudiadas y proyectadas encaminadas a lograr un fin determinado. Aunque se deriva del uso militar, todas las acciones del hombre están llenas de ella, porque es la aplicación de la inteligencia, el conocimiento y el raciocinio.
[4] Existen cinco ámbitos del combate o de la guerra: aire, mar, tierra, espacio y ciberespacio.

ámbito de la guerra y las ciberamenazas -que son formas novedosas de atentar contra la seguridad de los Estados-. Es decir, la ciberseguridad nacional estará enfocada en la protección de los individuos, la sociedad e instituciones contra ataques que utilicen el ciberespacio.

Contar con una definición precisa de lo que se entiende por seguridad evita la incertidumbre y establece tanto los límites como los objetivos que debe cumplir. David A. Baldwin señaló la importancia de un concepto claro de seguridad o seguridad nacional diciendo que la "seguridad es un concepto importante, el cual ha sido utilizado para justificar la suspensión de libertades civiles, hacer la guerra, y reasignar recursos masivamente durante los últimos cincuenta años"[5] (Baldwin, 1997, p. 9).

Etimológicamente la palabra seguridad proviene del latín *Securitas* que significa sin temor o despreocupado (RAE, s.f). Lo que de manera sencilla establece un contexto difícil de satisfacer, ya que toda actividad implica un riesgo. En contraste, de acuerdo con *El Arte de la Guerra* (Sun Tzu, 1994) la guerra debe ser estudiada para garantizar la seguridad o supervivencia del Estado, por lo que el estudio detallado de las capacidades/debilidades propias y del enemigo es el elemento esencial de la seguridad que es potencializado con el ingenio e inteligencia del hombre. En su teoría, Sun Tzu (1994, p. 44) dice que el estudio de la guerra con una visión estratégica es vital para la preservación del Estado, por lo que recomienda conocer al enemigo como a sí mismo. En otras palabras, la seguridad y supervivencia del Estado se fundamenta en el conocimiento profundo de la estrategia y tácticas de guerra, así como en el manejo eficiente de los recursos (materiales, tecnológicos y humanos) para lograr la victoria con el mínimo esfuerzo en el menor tiempo.

Walter Lippman (1943, p. 51) escribió "Una nación está segura cuando no tiene que sacrificar sus legítimos intereses para evitar la guerra y cuando es capaz, si fuera necesario, de mantenerlos a través de la guerra". Esto lo retoma a Wolfers (1952, p. 484) quien dijo que la seguridad radica en la preservación de los valores esenciales[6] de una nación. Es aquí donde se funden los dos términos para generar el concepto de seguridad nacional [7]. Por su parte, Richard Ullman (1983) buscó ampliar el concepto de seguridad nacional, afirmando que ésta se ve amenazada por eventos que degradan la calidad de vida de un Estado o de algún actor internacional de manera repentina. Insiste en que se incluyan aspectos relativos a fenómenos naturales y generados por el hombre como: epidemias, inundaciones, terremotos y sequias. En su propuesta, incluye

[5] Traducción propia.
[6] Algunos de los valores esenciales que menciona Wolfers son: la soberanía y la integridad territorial. Agrega también valores marginales como las inversiones extranjeras, mercados, entre otros (para ampliar información ver Wolfers, 1952, p. 489).
[7] Wolfers previamente indica que el termino seguridad nacional está bien establecido en el discurso político y hace referencia a un objetivo político fácilmente distinguible del resto. (1952, p. 483)

solamente aquellos que generan cambios drásticos de manera repentina y evita el fenómeno de la *securitización*[8] irrestricta.

Para subsanar las deficiencias, el concepto de seguridad se ha vuelto más amplio toda vez que ahora las corrientes teóricas de seguridad, como la Escuela de Copenhague, incorporan otras dimensiones no militares al concepto de "seguridad" (Collins, 2007, p. 60). Aunque la propuesta del concepto ampliado de seguridad integra la seguridad militar, ambiental, societal, económica y política, (Buzan, Wæver, & De Wilde, 1998, pp. 1-5) no incorpora los riesgos que surgen por la tecnología. Las afectaciones de la tecnología para la seguridad es un tema que con la ciberseguridad nacional será atendido prioritariamente. No sólo en el plano internacional el concepto ha sido adaptado y ampliado; también en el contexto nacional ha sufrido una evolución.

La definición de seguridad nacional en el contexto mexicano

En el caso particular de México la definición de seguridad nacional aparece oficialmente hasta principios de los años 80´s. De acuerdo con lo presentado en la obra *Grandes temas del constitucionalismo mexicano* publicada por la Corte Suprema de Justicia de la Nación (2005) su evolución ha sido la siguiente:

> El tema de la seguridad nacional se trató por primera vez en el Plan Global de Desarrollo 1980-1982 como tema de interés de Estado. Y se clasificó ésta como "la herramienta para mantener la condición de libertad, paz y justicia social dentro del marco institucional". El régimen le otorgó a las fuerzas armadas, el rol de "colaborar y coadyuvar" en la seguridad nacional. En el plan de 1989-1994, se la consideró como "condición imprescindible para el mantenimiento del orden soberano, por lo que debe ser preservada tanto en el ámbito interno como en el de las relaciones internacionales, con base en la concertación interna y la negociación externa". En el plan 1995-2000 se mantuvo la definición apuntada y se materializó una política de seguridad nacional, cuyo principio rector consiste en el fortalecimiento de la soberanía a través de acciones internas y externas, mientras que su sucesor, el Plan 2001-2006, estimó que el tema "tiene como metas principales velar por la protección y preservación del interés colectivo, evitando en lo posible o minimizando cualquier riesgo o amenaza a la integridad física de la población y de las instituciones" (p. 86).

Palabras en donde es evidente que el concepto fue considerado como herramienta, condición imprescindible y medio de protección de la soberanía, de la seguridad física, así como del desarrollo nacional[9], pero no contempla amenazas provenientes de cambios o adelantos en ciencia y tecnología que atentan contra la seguridad virtual. La ley de Seguridad Nacional fue publicada en 2005, siguiendo estas definiciones y tendencias por lo que tampoco incluye específicamente el elemento tecnológico como amenaza a la seguridad. Evidentemente requiere de una revisión.

[8] La *seguritización o securitización* indica que existe un riesgo en la sobreampliación (o sobre dimensionar) el término de seguridad que puede colocar todo y por lo tanto nada en particular como un problema de seguridad. Es decir, si todo es tema de seguridad es difícil atender las prioridades.

[9] Esto coincide con las palabras de Koffi Annan (Secretario General de la ONU en el 2005) sobre la Declaración del Milenio mencionando que "no hay seguridad sin desarrollo, ni desarrollo sin seguridad". Mayor información en el siguiente sitio: http://www.un.org/spanish/largerfreedom/summary.html

Debido a la dependencia en sistema computarizados, los fenómenos recientes que atentan contra la seguridad de los Estados contemplan las ciberamenazas (Gribbon, 2013); es decir, aquellos actores y acciones que ponen en riesgo la seguridad de Estados, organizaciones, individuos e información en el ciberespacio. Gracias a los estudios críticos de seguridad las ciberamenazas pueden ser incluidas para su estudio, ya que la seguridad es multidimensional y multinivel (Collins, 2007, p. 135). Agregando que los medios utilizados para lograr la seguridad nacional incluyen: la diplomacia, la negociación, la alianza internacional, la promoción del comercio/democracia, las instituciones, el derecho internacional, las sanciones, la riqueza y el poder (Carlisle, 1997); a lo que se debe sumar la tecnología y la estrategia. En estas condiciones, la definición de seguridad debe ampliarse para incorporar temas de índole tecnológica a fin de responder a las nuevas realidades del entorno internacional. Por lo tanto, es conveniente definir la ciberseguridad.

La Ciberseguridad

Sin duda alguna, la sociedad moderna ha experimentado un crecimiento exponencial de las TIC como instrumentos de organización, control, gobierno y administración de la información. Tan intensivo es el empleo de los medios digitales para realizar las actividades en todos los sectores que se habla de una hiperconectividad. (Dawson *et al*, 2016) Si bien dichas herramientas tecnológicas han acelerado los procesos y análisis de los datos, mejorado la vida de las personas, o ampliado el acceso a conocimiento; también han traído consigo una serie de nuevos desafíos que atentan contra la integridad, confiabilidad y disponibilidad de la información (Baheti y Gill, 2016), que son propiedades elementales de la ciberseguridad. Estos desafíos son la base para distinguir la seguridad de la información y la ciberseguridad.

Definiciones de ciberseguridad

En el plano internacional existen múltiples intentos por definir la ciberseguridad (Maurer y Morgus, 2014) entre ellos destacan los realizados por la Unión Internacional de Telecomunicaciones (UIT), la Organización Internacional para la Estandarización (ISO), Ciberestrategia de la Unión Europea, Sociedad del Internet (IS), Estonia, Israel, EE.UU., Reino Unido y México –entre otros países- que han definido la ciberseguridad en sus documentos rectores y estrategias de la siguiente manera.

En primer lugar, la UIT define la ciberseguridad como sigue:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (UIT, 2010).

En segundo lugar, se tiene la definición establecida por la Organización Internacional para la Estandarización (ISO) que dice: ""Ciberseguridad" o "Seguridad del Ciberespacio" [es], definido como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio"[10] (ISO, 2011).

Tercero, la Unión Europea en su documento de Ciberestrategia establece la siguiente definición:

> La ciberseguridad se refiere comúnmente a las salvaguardias y acciones que se pueden utilizar para proteger el dominio cibernético, tanto en el ámbito civil como militar, de las amenazas que están asociadas o que pueden dañar sus redes e infraestructura de información interdependientes. La ciberseguridad se esfuerza por preservar la disponibilidad e integridad de las redes y la infraestructura y la confidencialidad de la información contenida en ellas11 (UE, 2013, p.3).

Cuarto, la Sociedad del Internet define la ciberseguridad de la siguiente manera:

> Como palabra clave, la seguridad cibernética es terriblemente inexacta y puede representar una lista casi interminable de diferentes problemas de seguridad, retos técnicos y "soluciones" que van desde lo técnico a lo legislativo. Si bien las palabras de moda como la ciberseguridad pueden hacer que los titulares sean buenos, las discusiones serias sobre seguridad e Internet requieren una comprensión compartida de lo que se entiende por ciberseguridad12...La ciberseguridad se define como cualquier cosa que incluye problemas de seguridad específicos de Internet y sus soluciones técnicas y no técnicas. (IS, 2012: 1 y 3)

En la tabla No. 1 se presentan algunas de las definiciones que han sido utilizadas por los gobiernos del mundo para referirse a la ciberseguridad.

Desde una perspectiva personal, la mejor definición es la propuesta por la IUT porque protege de manera integral personas, materiales y entorno. La definición de la estrategia nacional de ciberseguridad mexicana, aunque incorpora parte de algunas de las demás definiciones, no garantiza el empleo de tecnología ni la protección del ciberespacio o de los activos por ser imprecisa. La utilidad de la precisión en el concepto es mencionada por Carl G. Hempel (1952, p.12) diciendo las razones para definir y redefinir los conceptos:

> La explicación conceptual intenta especificar la estructura lógica de las expresiones dadas: apartándose de los significados habituales de los términos, la explicación tiene por objeto reducir las limitaciones, ambigüedades e inconsistencias de su uso ordinario proponiendo una reinterpretación destinada a mejorar la claridad y la precisión de los términos Sus significados, así como su capacidad para funcionar en hipótesis y teorías con fuerza explicativa y predictiva13.

---

[10] Traducción propia. El original dice "Cybersecurity" or "Cyberspace security" [is], defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". Obtenida de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[11] Traducción propia. El texto original dice: *Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*. Obtenida de: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[12] Traducción propia. Las palabras originales son: *As a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity…. cybersecurity is defined as anything that includes security problems specific to the Internet and their technical and non-technical solutions. Not every crime that occurs on the Internet is covered by the term cybersecurity*. Obtenida de https://www.internetsociety.org/wp-content/uploads/2017/08/bp-deconstructing-cybersecurity-16nov-update.pdf pp. 1 y 3.

[13] Traducción propia. El autor dijo "Conceptual explication attempts to specify the logical structure of given expressions: Taking its departure from the customary meanings of the terms, explication aims at reducing the limitations, ambiguities, and inconsistencies of

Los datos presentados son indicadores de la falta de consenso ya que existen diversas visiones sobre ciberseguridad tanto en el plano internacional como en el ámbito nacional. Es evidente, que la dificultad para definir seguridad (Ullman, 1983; Buzan y Hansen, 2010) se replica al definir ciberseguridad. Queda claro que la experiencia internacional está plagada de dificultades para encontrar una definición universalmente aceptada; sin embargo, casi todos los Estados cuentan con una definición de seguridad nacional que debe ser revisada para incorporar las nuevas amenazas que han surgido del mundo virtual.

Tabla No. 1 Comparación de definiciones de ciberseguridad

Estado	Definición	Obtenida de:
Estonia	Una condición previa esencial para la seguridad del ciberespacio es que cada operador de una computadora, red informática o sistema de información se dé cuenta de la responsabilidad personal de utilizar de una manera determinada y apropiada los datos y los instrumentos de comunicación de los que dispone. La estrategia de seguridad cibernética de Estonia busca principalmente reducir las vulnerabilidades inherentes del ciberespacio en el país como un todo.	Estonia, Cyber Security Strategy, 2008, p. 3 Sobresale la mención de la responsabilidad individual de todos los usuarios de la red y de la información para salvaguardar el ciberespacio.
Israel	Políticas, medidas de seguridad, acciones, directrices, protocolos de gestión de riesgos y herramientas tecnológicas designadas para proteger el ciberespacio y permitir que se tomen medidas al respecto.	Israel, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, p. 1
EE. UU.	La capacidad de proteger o defender el uso del ciberespacio contra ciberataques. El proceso de proteger la información al prevenir, detectar y responder a los ataques.	United States of America, Committee on National Security Systems National Information Assurance Glossary, 2010, p. 22 United States of America, Framework for Improving Critical Infrastructure Cybersecurity, 2014, p. 37 Los EE.UU. tienen múltiples definiciones.
Reino Unido	La ciberseguridad se refiere a las defensas contra ataques electrónicos lanzados a través de sistemas informáticos.	United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 1
México	Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.	Estrategia Nacional de Ciberseguridad. Glosario. p. 27

Fuentes: Elaboración propia con información de: United States of America, National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," U.S. Department of Commerce, 2014; United States of America, Committee on National Security Systems, "CNSS National Information Assurance Glossary," Committee on National Security Systems, 2010. Estrategia Nacional de Ciberseguridad de México. Traducción del autor.

their ordinary usage by propounding a reinterpretation intended to enhance the clarity and precision of their meanings as well as their ability to function in hypotheses and theories with explanatory and predictive force." Obtenido de Hempel, C. G. (1952). *Fundamentals of concept formation in empirical science*. Chicago University Press. p. 12.

Tal y como ocurrió con el concepto de seguridad, la amplitud del concepto de ciberseguridad también ha creado un mundo de ideas que no son parte de ella, lo cual según Wolfers (1952, p. 483) genera confusión en su comprensión y aplicación. La confusión existente con el concepto de ciberseguridad la exponen Trey Herr y Allan Friedman diciendo:

> La ciberseguridad es un término a menudo abusado y mal utilizado que una vez fue concebido para describir y ahora sirve mejor para confundir. Aunque inicialmente pretendía cubrir temas relacionados con la seguridad asociados con el "ciberespacio,"... se ha convertido en el pretexto para un conjunto asombrosamente diverso de temas. (Trey Herr y Allan Friedman 2015, p. 1)

Trey Herr y Allan Friedman (2015: 1) dicen que la ciberseguridad no es algo especial, que es resultado de una integración incierta de las actividades en internet y los actores en las políticas y leyes existentes. Los mismos autores agregan también que la complejidad de la *ciberseguridad*, en otras palabras, viene menos de los dispositivos que usamos y más de las personas detrás de ellos. Visión que atrae nuestra atención porque pone de manifiesto que el factor humano en la ciberseguridad sigue siendo un elemento determinante. Se puede asumir que el eslabón más débil de la ciberseguridad es el ser humano.

Como se ha expuesto, la problemática para definir la seguridad de manera precisa se ha transferido fácilmente a la ciberseguridad; ya que los organismos internacionales, los Estados e incluso los individuos tienen una visión divergente sobre lo que debe incorporar, proteger y limitar dicho concepto. En el caso de México el tema tiene mayores deficiencias porque no existe una definición de ciberseguridad en los documentos rectores de la política de seguridad nacional como son el Plan Nacional de Desarrollo y el Programa de Seguridad Nacional[14].

La ciberseguridad en el Plan Nacional de Desarrollo

Para México es necesario contar con una definición precisa, clara y concisa de seguridad, porque esto sirve como punto de partida y justificación para las acciones que deben emprenderse con el fin de garantizar su supervivencia. Si bien, el Artículo 3 de la Ley de Seguridad Nacional establece que la seguridad nacional se entiende como: “las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano que conlleven a: I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país” (Cámara de Diputados, 2005), no se menciona algo sobre la

[14] La ITU reporta que México ha tomado algunos pasos en la regulación de la ciberseguridad en dos documentos: El Código Penal Federal y La Ley de Firma Electrónica Avanzada. Al revisar dichos documentos se encontró lo siguiente: el Código Penal tipifica los delitos de: Espionaje (art.127), Violación de correspondencia (art.167 VI), Descifrado ilegal (art.168 bis), Revele secretos (art. 210-211bis), Acceso ilícito a sistemas y equipos de informática (art.211 bis 1-7), Ejercicio indebido del servicio público (art.214 IV), Ejercicio abusivo de funciones (art.220 II), por medio de los cuales se busca la seguridad de la información sin mencionar ni definir la ciberseguridad; y la Ley de Firma Electrónica Avanzada únicamente hace mención de las propiedades de la información digital que deben ser resguardadas diciendo en el artículo 27 … para garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada. En realidad, no brindan una definición clara de ciberseguridad; **solamente la Estrategia Nacional de Ciberseguridad brinda una definición acotada que debe ser revisada**.

ciberseguridad de manera precisa. Evidentemente, esta Ley deja fuera del concepto de seguridad al elemento tecnológico y por lo tanto requiere ser actualizada.

México no consideró la inclusión de una definición para la ciberseguridad en la Ley de Seguridad Nacional, pero refiere en el Artículo 7 que en el "plan nacional de desarrollo y en el programa que de él derive, se definirán temas de seguridad nacional, y será la base para la Agenda Nacional de Riesgos" (Cámara de Diputados, 2005). La existencia de la Agenda Nacional de Riesgos no es garantía de las prácticas de ciberseguridad, ya que de acuerdo con Gonzalo Monterrosa (2016) México es incapaz de prevenir y reaccionar ante incidentes cibernéticos. Además, Monterrosa (2016) indica que:

> La Agenda Nacional de Riesgos consigna que México padece un "riesgo alto" por la carencia de esquemas de protección, reacción y coordinación consolidados entre las autoridades competentes para hacer frente a los ataques cibernéticos que afecten las infraestructuras críticas o sensibles del país.

Es decir, México como otros Estados requiere además de una política de ciberseguridad y una ciberestrategia nacional.

El Plan Nacional de Desarrollo (PND) 2013-2018, elaborado por la administración del presidente Peña Nieto, plantea fortalecer las capacidades institucionales en el ciberespacio. Además, sobresale la intención de fortalecer las capacidades de inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la seguridad nacional. De igual forma dicho plan busca "impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad" (Presidencia, 2013: 107) lo cual debería ser acotado y precisado en el Programa de Seguridad Nacional, pero quedó inacabado.

Del texto del PND (203-218) se infiere que la seguridad del Estado mexicano es una tarea que se asume desde una perspectiva multidimensional y con sentido humano bajo un gobierno democrático. La ciberseguridad se menciona en ocho ocasiones y se ve como una amenaza a la seguridad nacional, como una prioridad de la política de seguridad nacional, como un sinónimo de seguridad de la información, o como la cuarta dimensión de operaciones de seguridad; todo lo cual abona más a la incertidumbre sobre su conceptualización. Es opinión personal que existe una confusión en los términos y su empleo en el PND. Primero, se debe aclarar que el ciberespacio es considerado como el quinto ámbito de la guerra (Lynn, 2010) y no solamente una dimensión de operaciones de seguridad; por lo que, debido a la falta de una definición precisa, la ciberseguridad podría definirse como lo hace la UIT.

Es claro que la ciberseguridad es un tema que requiere de capacitación y cooperación internacional, así como de una estrategia para generar cuadros con personal militar profesionales en ciberseguridad y ciberdefensa. Sin embargo, en ningún momento se define en el PND lo que se entiende por ciberseguridad

y la confunden con seguridad de la información, lo cual genera confusión e incertidumbre. Aunado a lo anterior, el PND habla de la Estrategia Digital Nacional 2013 que tiene por objetivo "aumentar la digitalización de México, para que con ello se maximice su impacto económico, social y político en beneficio de la calidad de vida de las personas" (Presidencia, 2013, p.15). Sin embargo, la ciberseguridad quedó en segundo plano a pesar de que se promueve el uso intensivo de las TIC.

En los párrafos anteriores se han presentado argumentos que sugieren que México no solamente está falto de una definición clara e integral de ciberseguridad nacional, sino también de una política de ciberseguridad nacional que permita la aplicación eficiente de la estrategia nacional de ciberseguridad. Tanto la definición como la estrategia de ciberseguridad son punto de partida y elementos guía para lograr la preservación de la seguridad en el espectro electromagnético y ámbito físico, ya que determinan cuál será el objeto de dicha protección y como se llevará a cabo. Esta negligencia gubernamental expone a la sociedad e instituciones a sufrir ataques contra su identidad, existencia y supervivencia.

Por ejemplo, la OEA (2014) reportó lo siguiente: "incidentes de acceso lógico no autorizado aumentaron aproximadamente 260%, las infecciones de malware aumentaron 323% y los incidentes de *phishing* aumentaron un 409%, mientras que los ataques de denegación de servicio disminuyeron 16%" (p. 68). A lo que habría que sumarle el incremento en las amenazas persistentes avanzadas (APT[15]) y el cibersecuestro por medio de *ransomware*[16]. Estos datos son evidencia de la existencia de una seria amenaza a la ciberseguridad nacional del Estado mexicano que debe ser atendida de manera eficiente. Las amenazas que enfrentan los Estados pueden proceder de actores no estatales y estatales quienes realizan actos de cibercrimen y ciberguerra. Dos temas que deben ser considerados de manera separada, pero complementaria.

Es por ello, que en respuesta a este aumento en el número y complejidad de los ciberataques México debe contar con políticas, planes, estrategias, organizaciones e infraestructuras adecuadas para garantizar la ciberseguridad del ciberespacio. Para tal efecto, necesita definir con precisión que entiende por ciberseguridad y posteriormente diseñar una ciberestrategia que ofrezca una doctrina y organización de ciberseguridad nacional para implementar un sistema de ciberdefensa multicapa y contar con la capacidad ciberofensiva o de ciberdefensa proactiva.

[15] Este tipo de amenaza son un conjunto de procesos informáticos sigilosos y continuos, con mucha frecuencia orquestados por humanos, que son dirigidos a penetrar la seguridad informática de una entidad específica y resistir algunos intentos de borrado.
[16] El *ransomware* (de *ransom* "rescate" y *software* "programa") es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes, accesorios o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Otra manera de llamarle es cibersecuestro. Los ciberdelincuentes utilizan esta técnica para bloquear sus dispositivos y exigir un rescate a cambio.

Los desafíos para la ciberseguridad nacional de México

Hoy en día, el empleo intensivo de sistemas computarizados, tanto por parte del gobierno como de las fuerzas armadas y diversas empresas de la iniciativa privada, han tenido un crecimiento exponencial (García, 2014, p. 6); sin embargo, esta misma situación de dependencia ha traído consigo las vulnerabilidades inherentes de dichos sistemas digitales, poniendo en riesgo la seguridad de los Estados, organismos e individuos. Para muestra de lo antes dicho, se tienen las filtraciones sobre los actos de espionaje estadounidense realizadas por Edward Snowden (Wu *et al*, 2015), Julian Assange y Bradley Manning (Gurkaynak *et al*, 2013). Por ello, es preciso determinar cuáles son las necesidades, actores y factores que impactan en la ciberseguridad de los Estados y sociedad en general a fin de garantizar las ventajas competitivas y comparativas en los nuevos escenarios del siglo XXI con amenazas como *Dragonfly* (Sysmantec, 2014), la cual se centró en realizar ciberataques contra instalaciones del sector energético en América del Norte y Europa principalmente.

En el caso de México, por medio de las reformas en telecomunicaciones y la Estrategia Digital Nacional (Presidencia, 2013), se ha dado prioridad a la digitalización de las actividades de gobierno y los servicios públicos, pero la ciberseguridad no ha recibido el mismo ímpetu. En consecuencia, la elaboración e implementación de estrategias y planes nacionales para el uso seguro del ciberespacio son prioritarias para aprovechar los beneficios de estas tecnologías (Rudner, 2013 y Cussas, 2011). En breve, los principales desafíos que enfrenta México son: redefinir su concepto de ciberseguridad, fortalecer las capacidades del Estado para garantizar la seguridad en el ciberespacio con base en una estrategia de ciberseguridad integral y, generar recursos tecnológicos/humanos apropiados para las nuevas condiciones de ciberseguridad.

¿Por qué definir con claridad ciberseguridad?

¿Por qué debe existir una definición clara de ciberseguridad en la legislación vigente de México? Básicamente porque los principios del gobierno democrático ciñen la actividad estatal a lo que se estipula en la norma. Y las normas o leyes se establecen para regular las relaciones de poder en sociedad, buscar el bien común y son promulgadas por la autoridad que tiene a su cargo el cuidado de la comunidad partiendo de conceptos claramente definidos.

En México la salvaguarda del bien común en el presente requiere de una estrategia de seguridad multinivel, multidisciplinaria y multidimensional para incorporar temas como la ciberseguridad. Como se ha dicho el gobierno de México, en el PND 2013-2018, ha dado prioridad al uso de las TIC, para que la digitalización contribuya al desarrollo del país (Presidencia, 2013, p.11), que si bien cual invita al uso generalizado de las TIC, deja en el limbo las políticas públicas y medidas de ciberseguridad que deben adoptarse.

De igual forma en el PND 2013-2018 bajo el rubro de México en Paz señala lo siguiente: “1.1. Promover y fortalecer la gobernabilidad democrática. Objetivo 1.2. Garantizar la Seguridad Nacional” (Presidencia, 2013,

p.5), en donde se presenta la supuesta estrategia y línea de acción que se debe seguir en cada uno de los temas; lo que refuerza nuestro argumento del actuar conforme a la norma del gobierno democrático. Por lo tanto, el gobierno mexicano debe acatar lo dispuesto en el PND 2013-2018 e iniciar con una política pública de ciberseguridad y diseñar la estrategia correspondiente que proteja los intereses del Estado mexicano en el ciberespacio y abone a la seguridad nacional. Algunas prioridades mencionadas en el PND que se deben resaltar en cuestión de seguridad nacional incluyen:

- La intención de fortalecer las capacidades de inteligencia, del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la seguridad nacional (Presidencia, 2013, p. 107).
- Una política integral de Seguridad Nacional del Estado Mexicano, en su aspiración por tutelar e impulsar los intereses estratégicos nacionales, deberá atender todos aquellos factores que puedan vulnerar el elemento humano del Estado (Presidencia, 2013, p. 31).
- Impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad[17] (Presidencia, 2013, p. 107).
- Diseñar e impulsar una estrategia de seguridad de la información, a efecto de garantizar la integridad, confidencialidad y disponibilidad de la información de las personas e instituciones públicas y privadas en México (Presidencia, 2013, p.108).

Lo anterior son algunas de las acciones que debía emprender el gobierno de México desde el 2013 en materia de ciberseguridad nacional, solamente falta evaluar su aplicación. De acuerdo con el Índice de Desarrollo Democrático México 2015 (IDD, 2015, p. 47) las evidencias sobre seguridad indican que "En México, la población percibe desde hace mucho tiempo… que la **inseguridad** afecta fuertemente el libre ejercicio de sus derechos y libertades." Lo que permite inferir que no existe una estrategia de seguridad eficiente ni integral. En breve, una definición clara y concisa de ciberseguridad daría certeza a las acciones del gobierno.

Propósito de una ciberestrategia para México

El Programa de Seguridad Nacional 2014-2018 establece "un panorama de los retos para la Seguridad Interior y la estrategia adoptada por esta Administración para enfrentarlos" (2014, p. 22). También establece que la seguridad de la información es uno de los temas que requiere de la elaboración de una estrategia para "asegurar y resguardar la integridad, confidencialidad y privacidad de la información de las personas e instituciones públicas y privadas" (Presidencia, 2014, p. 54). Lo que posteriormente se ve detallado en el apartado sobre riesgos y amenazas al declarar a la ciberseguridad como una de las amenazas a la seguridad que enfrenta México (Presidencia, 2014, p. 64).

[17] Es el único momento en que aparece la palabra en todo el documento y no se brinda una definición de dicho concepto.

Es decir, se tiene claro que existen potenciales enemigos que utilizan el ciberespacio para atentar contra la seguridad del Estado mexicano, que la ciberseguridad es una prioridad para la seguridad nacional, y que se requiere tanto de una política como de una estrategia para obtener el grado de ciberseguridad deseado. El reconocimiento de la falta de una política y estrategia de ciberseguridad nacional se presenta en el texto del Programa para la Seguridad Nacional 2014-2018 como sigue:

> …es necesario que el Gobierno de la República desarrolle una política de Estado en materia de ciberseguridad y ciberdefensa, para garantizar así la defensa de los intereses económicos, políticos y militares de México en el ciberespacio. Es necesario generar y poner en marcha una estrategia que evite afectaciones a las capacidades nacionales de comunicación y a la funcionalidad de los sistemas de información estratégicos gestionados por las autoridades y el sector privado. El propósito central de la estrategia debe ser el fortalecimiento de la cuarta dimensión de las operaciones de seguridad: la ciberseguridad y la ciberdefensa (Presidencia, 2014, p. 64).

Palabras en donde se pone énfasis en la ciberseguridad y ciberdefensa como elementos clave para la ciberseguridad nacional. La falta de estrategia por algunos países ha sido reconocida e informada por la OEA (2016, p. ix) en su informe sobre ciberseguridad, diciendo que “Cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica” Aunque México la presentó en 2017, sus objetivos deben ser revisados ya que la estrategia no se alinea con los objetivos nacionales. Recordando que el principal propósito de una estrategia de ciberseguridad es contar con un plan de acción que determine las funciones, alcances, medios, formas y objetivos.

Las mejores prácticas de ciberseguridad que pueden ser adoptadas por los Estados (Luiijf, Besseling, y De Graaf, 2013; Shackelford, 2016), incluyen planes y programas, así como estrategias para prevenir y mitigar los efectos de las diversas amenazas digitales que atentan contra la seguridad de los individuos, organizaciones y Estados. Contar con una ciberestrategia permite revalorar la situación y corregir vulnerabilidades. De forma general la estrategia se define como un plan estudiado a conciencia para lograr un objetivo. Esto ha sido estipulado por la OEA (2016) como sigue:

> Una estrategia nacional integral de seguridad cibernética identifica los intereses y roles de una gama de actores que contribuyen a, tienen la responsabilidad de o se ven afectadas por la seguridad cibernética con el propósito de crear un marco coordinado y cohesionado. Esta estrategia en ocasiones incluye varias áreas temáticas e identifica los roles y responsabilidades de varios actores que participan en la seguridad cibernética, incluida la industria, la sociedad civil y personas naturales, y destacará la importancia de los mecanismos para abordar sus necesidades y aprovechar su experiencia (p. 124).

Definición detallada de lo que debe estar incluido en una estrategia integral de ciberseguridad (componente civil) para la salvaguarda de la seguridad nacional de los Estados cuando se complementa con la estrategia de ciberdefensa[18] (componente militar). La ciberestrategia se convierte en el plan de acción detallado para

[18] Puede haber eventos que repercuten en los intereses de seguridad nacional relacionados con la seguridad de la red, la capacidad de recuperación cibernética, la respuesta a incidentes y el intercambio de información, que requieren la participación de los ministerios y organismos de defensa. Por lo tanto, se necesita la preparación de una estrategia que coordine a todas las organizaciones participantes para garantizar un enfoque integrado para hacerle frente a las amenazas a la seguridad nacional. Esta evaluación no

lograr la ciberseguridad nacional por medio de dos partes complementarias: la ciberseguridad y la ciberdefensa. Una prioridad para México es la construcción de un sistema de ciberseguridad nacional para implementar la estrategia de ciberseguridad nacional.

En este sentido el gobierno de México ha tomado algunas acciones entre las que se incluyen la creación de un Sistema Nacional de Inteligencia (Presidencia, 2014) y un Centro de Operaciones del Ciberespacio[19] (SEDENA, 2013 y SEMAR, 2013). En el 2016 fue reportado el inicio de las operaciones de dicho Centro en el Cuarto Informe de Gobierno (2015-2016), quedando pendiente la propuesta de SEMAR para construir el Centro de Control de Ciberdefensa y Ciberseguridad (CCCC).

La falta de una estrategia nacional de ciberseguridad integral da como resultado una escueta capacidad de prevención y casi nula de reacción ante ciberataques (ITU, 2014), que son operaciones con potencial para comprometer infraestructuras críticas del país e información sensible de las instituciones y las personas (Monterrosa, 2016). En breve, para que el gobierno mexicano pueda dar respuesta eficiente a las nuevas demandas de seguridad de la Era de la Información debe contar con una ciberestrategia nacional integral. De esta forma puede estructurar un sistema de ciberseguridad nacional como el que se muestra a continuación.

Tabla No. 2. Propuesta de un sistema de ciberseguridad nacional para México

Fuente: elaboración propia

pretende examinar la capacidad técnica o militar, sino que se centra en los atributos fácilmente observables, tales como planificación estratégica, organización y coordinación. (ver OEA, 2016, p.127)

[19] El centro tiene por misión: planear, coordinar, dirigir y ejecutar los esfuerzos del Ejército y Fuerza Aérea Mexicanos para identificar las amenazas provenientes del ciberespacio y mitigar sus efectos, así como prevenir y responder a incidentes que atenten contra la información e infraestructura crítica soportada en sus tecnologías de la información y comunicaciones.

Sistema en el cual se define a la policía como el elemento bisagra o de enlace entre la ciberseguridad y la ciberdefensa. Si México no toma las medidas pertinentes para fortalecer la democracia, incrementar el nivel de aceptación del gobierno y construir instituciones fuertes, podría profundizarse la debilidad del Estado en el mundo material y virtual. Por lo tanto, es preciso que en cuestiones de seguridad nacional y ciberseguridad fortalezca las atribuciones de las agencias existentes encargadas de dichas funciones y/o diseñe aquellas instituciones de las cuales carezca.

La estrategia de ciberseguridad permite concentrar en un documento guía las actividades de ciberdefensa y de ciberseguridad, partiendo de una política de Estado clara sobre los objetivos que se buscan en el tema de la seguridad del ciberespacio. Representa la oportunidad de diseñar una política y estrategia (Cussac, 2011 y Sabillon *et al*, 2016) de ciberseguridad propositivas con base en el estudio de los ciberataques más importantes contra infraestructura crítica que han ocurrido contra México (Monterrosa, 2016). Considerando que de acuerdo con el Centro de Inteligencia y Seguridad nacional (CISEN) se debe establecer de forma clara la diferencia entre las acciones de seguridad nacional y las de seguridad pública[20] para determinar las atribuciones en la materia de cada uno de los niveles de gobierno.

Según la Constitución Política en México las decisiones de seguridad nacional son competencia exclusiva del poder ejecutivo[21] con el apoyo de la administración federal y las fuerzas armadas. (Cisen, s.f.) Por lo tanto, con base en lo antes mencionado y lo dispuesto en el PND 2013-2018 así como en el PSN 2014-2018 el presidente de México, con el apoyo del consejo de seguridad nacional, es el responsable de la organización de una fuerza de ciberseguridad nacional. Es el encargado de diseñar la política y estrategia de ciberseguridad para que el Estado sea garante de la seguridad (Collins, 2007, p. 150) con instituciones fuertes. De acuerdo con Richard Jackson (Collins, 2007, p. 149) los Estados débiles son carentes de las atribuciones fundamentales como son las instituciones efectivas.

Hasta el momento los esfuerzos realizados para la construcción de un sistema de ciberseguridad y ciberdefensa han visto algunos avances a través de organismos como la policía científica, el CISEN y de las fuerzas armadas. En México la policía federal es "la principal autoridad operacional en lo que respecta a iniciativas relativas a la seguridad y el delito cibernético en México, pero muchas otras instituciones

[20] De conformidad con lo dispuesto por el artículo 21, párrafo noveno de la Constitución Política de los Estados Unidos Mexicanos, la Seguridad Pública es concebida como: "…una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas…"; que se ve ampliada por la Ley General del Sistema Nacional de Seguridad Pública, publicada en el Diario Oficial de la Federación el 2 de enero de 2009, que agrega en su artículo 2, que los fines de la Seguridad Pública son: "…salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos, la investigación para hacerla efectiva, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del individuo…"

[21] Plasmado en la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en los artículos 73 fracción XXXIX y 89b fracción VI.

gubernamentales también desempeñan un rol activo" (OEA, 2014, p. 67). Dentro de las fuerzas armadas, México ha tomado algunas acciones entre las que se incluyen la creación de un Sistema Nacional de Inteligencia (Presidencia, 2014) y un Centro Nacional de Operaciones del Ciberespacio con la participación de la Secretaria de Defensa Nacional y de la Secretaría de Marina (SEDENA, 2013 y SEMAR, 2013).

En el mismo tenor el gobierno de México cuenta con un Equipo de Respuesta a Incidentes de Seguridad Informática del país, que está muy involucrado en la protección de la Infraestructura Crítica Nacional (ICN). Estas instituciones se ven reforzadas por las buenas prácticas en ciberseguridad. Aunque existen esfuerzos a nivel nacional para impulsar la ciberseguridad, como la creación del CERT-MX o la operación de la División Científica de la Policía Federal (SEGOB, s.f.), entre otras cosas, México aún sigue rezagado con un impacto negativo. De acuerdo con el Índice Global de Ciberseguridad 2015 (UIT, 2015), México (0.328) contaba con un bajo nivel de preparación ante ciberamenazas por lo que podría considerarse como un blanco fácil para los ciberdelincuentes y otros ciberejércitos. En el Índice Global de Ciberseguridad 2017 (UIT, 2017) las principales debilidades se ubicaron en la falta de capital humano, de documentos oficiales que guíen el esfuerzo nacional y de una cooperación sólida para compartir información. México (con un índice de 0.660 de un máximo de 1.0) fue el primer país en América Latina y el Caribe, y el tercero en América del Norte muy por debajo de EE.UU. (0.91) y Canadá (0.81).

A pesar de que el gobierno de México ha informado la puesta en operación del Centro de Operaciones del Ciberespacio en junio del 2016 (Presidencia, 2015-2016, p. 85), para atender cuestiones de ciberdefensa y complementar las tareas realizadas por la Policía Federal, es un trabajo inacabado que requiere del compromiso gubernamental para llevar a buen término aspectos esenciales de la política de ciberseguridad como la revisión de la ciberestrategia, el fortalecimiento de las instituciones de ciberseguridad y la generación de una cultura/tecnología de la ciberseguridad.

Formación de factor humano y tecnología

La formación de recursos humanos eficientes y profesionales es un elemento clave en toda empresa. En ese sentido:

> El Plan Nacional de Desarrollo es la hoja de ruta que sociedad y gobierno hemos delineado para caminar juntos hacia una nueva etapa del país. Este documento traza los grandes objetivos de las políticas públicas, establece las acciones específicas para alcanzarlos y precisa indicadores que permitirán medir los avances obtenidos (Presidencia, 2013, p. 9).

Por ello, es preciso tomar en cuenta el factor humano para coordinar políticas desde el ámbito educativo y formar ciudadanos conscientes de los riesgos del ciberespacio. La preparación de estos **superindividuos** sería en áreas que fueron recomendadas por Platón en su obra clásica **La República** (2006), esto es cuerpo, corazón y mente. Con miras a lograr este objetivo, los programas de formación, quizás no sólo los de las

instituciones de ciberseguridad, sino los de todo el sistema educativo nacional, deben estar orientados a fomentar lo siguiente:

- El fortalecimiento de la cultura de ciberseguridad.
- El crecimiento espiritual/moral por medio de la reflexión filosófica, así como gracias a la formación y práctica de valores.
- El desarrollo intelectual haciendo uso de métodos de alta calidad educativa, sobre todo en temas de ciencia y tecnología (para el caso temas cibernéticos y de sistemas digitales).

Tradicionalmente, el capital humano es esencial para la productividad de una sociedad, así como para el funcionamiento de sus instituciones, no sólo políticas, sino sociales y culturales. En este sentido, comprender la situación actual del factor humano y su capacidad, es fundamental para cualquier persona, organización o Estado; ya que de ello depende su eficiencia profesional. De acuerdo con la OEA

> Los esfuerzos del gobierno [mexicano] por generar conciencia sobre seguridad cibernética incluyeron la organización de varias conferencias para instituciones gubernamentales y educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas. (OEA, 2014, p. 68)

De acuerdo con el Índice de Competitividad 2016-2017, México mejoró en sus condiciones de competitividad en gran medida debido a sus ganancias por eficiencia de mercado, aunque la calidad de la educación primaria y la institucional continúan siendo sus más grandes debilidades (WEF, 2016, p.30). Es decir, la mala calidad de la educación básica tiene repercusiones de largo alcance, que impactaran en el desarrollo de una fuerza de ciberseguridad. En el pilar de educación y habilidades México obtuvo las siguientes posiciones: 87 en educación y habilidades; 78 en habilidades de su fuerza laboral actual; y, 87 en habilidades de su fuerza laboral futura. Finalmente, en el pilar de educación superior y capacitación obtuvo la posición 112 en la calidad de la educación y la posición 120 en calidad de la educación en matemáticas y ciencias. Algo que debe ser mejorado prioritariamente.

Ya en cuestiones de ciberseguridad el Índice Global de Ciberseguridad 2014 (UIT, 2015, p. 3) clasifica a México en la posición 18 a nivel mundial; pero, en cuestiones de construcción de capacidades menciona que: hay **poca investigación sobre mejores prácticas**, el personal de la policía científica recurre a capacitaciones en el exterior, el gobierno hace esfuerzos por generar una conciencia sobre la ciberseguridad, no se cuenta con una estadística sobre los profesionales y las instituciones del sector público certificados por una entidad internacional. Todo ello es evidencia de la falta de un sistema educativo y de capacitación formal en temas de ciberseguridad; aunque tanto instituciones gubernamentales como educativas ofrecen conferencias sobre ciberseguridad. También están disponibles algunas oportunidades de capacitación para empleados, incluyendo programas de certificación a través del sector privado (OEA, 2016, p. 86). Es por ello que se remarca lo siguiente:

> A pesar de los importantes avances logrados, lo más importante que la experiencia de 2013 deja como lección es la necesidad de que todos los involucrados redoblen sus esfuerzos en lo que concierne a reformar leyes y políticas, desarrollar capacidad técnica, generar mayor conciencia, compartir información y cooperar con otras partes interesadas. (OEA, 2014, p. 8)

Hacer frente a los retos del sistema educativo mexicano actual en materia de ciberseguridad requiere un replanteamiento esencial e integral de lo que significa aprender, trabajar y cumplir con todo el potencial que poseemos como individuos. Además, implica planes para que las empresas y los gobiernos inviertan en talento, y diseñen un sistema educativo de calidad. Requiere que los gobiernos atiendan este tema a largo plazo y planifiquen las necesidades de las generaciones del mañana, particularmente en un mundo donde las TIC se han convertido en una oportunidad el desarrollo y en una amenaza para la ciberseguridad de los Estados.

México ha puesto en marcha diversos esquemas de capacitación y formación de cuadros especializados en materia de ciberseguridad y ciberdefensa. Todo ello en seguimiento a lo dispuesto en PND (2013-2018) en su apartado de Educación y formación de profesionales. (Presidencia, 2013, p. 6) De esta manera se asume que la capacitación en ciberseguridad es un tema que requiere de una amplia cooperación internacional y tecnología especializada que permita defender la red y/o contener a los transgresores en el menor tiempo posible. Sin embargo, las acciones oficiales no serán de mucho provecho, sino se cuenta con la participación consciente y activa de la sociedad en su conjunto. Como bien lo señala la OEA:

> …autoridades nacionales deben promover la creación de una cultura de la seguridad cibernética y emprender acciones de concientización en esa materia para proteger a los usuarios…para desarrollar una cultura en seguridad cibernética se requiere la colaboración de todas las partes interesadas a nivel nacional. (OEA, 2014: 4)

Educar, hoy se ha convertido en una forma de encontrar la ciberseguridad que requiere un enfoque multidisciplinario, multinivel y proactivo.

Tecnología

El aumento de las amenazas vinculadas con la gestión del ciberespacio se ha convertido en una preocupación constante para todos los actores internacionales. Las actividades cibernéticas con propósitos agresivos/desastrosos son una forma de criminalidad en rápida expansión la cual no conoce fronteras (Choo, 2011; y Rudner, 2013). De igual forma el incremento en el número de ataques contra infraestructura crítica, intereses económicos, las redes de comunicaciones e información, así como las áreas estratégicas de los gobiernos de naciones específicas, es evidencia de la existencia de gobiernos, grupos criminales y organizaciones dispuestas a explotar las bondades del ciberespacio para lograr sus objetivos. Para hacer frente a este tipo de amenazas, es necesario que México redoble sus esfuerzos en la materia implementando un sistema de ciberdefensa basado en tecnología propia.

El PND (2013-2018) "traza los grandes objetivos de las políticas públicas, establece las acciones específicas para alcanzarlos y precisa indicadores que permitirán medir los avances obtenidos" (Presidencia, 2013, p. 9). Y en su apartado de: México con Educación de Calidad. Objetivo 3.5 menciona sus aspiraciones por lograr avanzar en proyectos de ciencia y tecnología que abonen al desarrollo y seguridad nacionales (Presidencia, 2013, p.6). Lo anterior se hace con miras a reducir la brecha tecnológica mencionada por la OEA en cuestiones de ciberseguridad, cuando declara:

> Persiste un notable desequilibrio en lo que respecta a la situación de cada país en términos de desarrollo vinculado con la seguridad cibernética. En algunos países, se han desarrollado avanzadas capacidades técnicas y de investigación integrados, y se encuentran en vigor las leyes necesarias para utilizar a pleno tales fortalezas. Otros, en cambio, se encuentran aún en el punto de partida o muy cerca de él, y todavía lidian con los retos que entraña determinar qué acciones poner en práctica, quiénes deben participar y cómo distribuir del mejor modo recursos humanos y financieros limitados. (OEA, 2014, p. 8)

Es decir, no es suficiente que el incremento en la conectividad a Internet sea sostenible; también es necesario que dicha conectividad sea segura y resistente. Todo sistema de ciberseguridad que se considere *seguro* debe ser de desarrollo, diseño e implementación propios; debe contar con sistemas de protección de acceso a internet y una defensa multicapas. Por lo cual la investigación y desarrollo en ciberseguridad se convierte en una prioridad para la seguridad nacional.

En este sentido Virginia Hernández (2015) reportó que México contaría con un centro de desarrollo tecnológico enfocado en la "detección y análisis de vulnerabilidades informáticas, así como el desarrollar tecnología para el segmento de la ciberseguridad y el ciberespacio". En este esfuerzo confluirían el gobierno, la iniciativa privada y la academia para lograr conjuntar lo mejor de todos. Con esto se puede atender la siguiente recomendación hecha por la OEA:

> Ni siquiera los países más avanzados de la región pueden correr el riesgo de adoptar una actitud de complacencia. Los datos proporcionados por las autoridades nacionales y recopilados por Symantec correspondientes a América Latina y el Caribe, muestran sin lugar a dudas incrementos significativos del volumen de delitos cibernéticos, ataques y otros incidentes en casi todos los países del hemisferio. (OEA, 2014, p. 8).

No se puede dejar de lado el hecho de que la seguridad debe incluir entre sus elementos fundamentales para su definición y aplicación a la tecnología; que desde el inicio de la historia del hombre ha sido el factor decisivo en la lucha por la supervivencia.

Conclusiones

La problemática para definir la seguridad de manera precisa se ha transferido fácilmente a la ciberseguridad; ya que los organismos internacionales, los Estados e incluso los individuos tienen una visión divergente sobre lo que debe incorporar, proteger y limitar dicho concepto en el ciberespacio. En el caso de México, la ciberseguridad es aún un tema con graves deficiencias porque no existe una definición integral única en los documentos rectores de la política de seguridad nacional. Por lo que, considerando los valores fundamentales

que debe proteger el Estado para su supervivencia, se debe redefinir la seguridad nacional para incorporar el concepto integral de ciberseguridad nacional.

Es necesario que Estados como México diseñen una política de ciberseguridad y pongan en marcha una ciberestrategia que prevenga afectaciones a las capacidades nacionales de comunicación y a la funcionalidad de los sistemas estratégicos de información, comunicación y control (infraestructura crítica), bajo el cuidado de las instituciones públicas y privadas. La ciberestrategia debe tener por objetivo el fortalecimiento de las operaciones de seguridad la ciberseguridad y la ciberdefensa con una visión estratégica, proyectiva y prospectiva. Además, dicha ciberestrategia debe estar acompañada por un plan de desarrollo de ciencia y tecnología de defensa para contar con los recursos materiales y humanos necesarios para la salvaguarda del ciberespacio.

Implementar un sistema de ciberseguridad nacional eficiente trae consigo desafíos técnicos, educativos, culturales, políticos, legislativos y humanos que deben ser atendidos con presteza. Encontrar una fórmula para cubrir déficit tanto de recursos humanos como de tecnologías seguras se ha convertido en una prioridad para los gobiernos, las organizaciones y las industrias. Es evidente que la creación de la fuerza de ciberseguridad nacional requiere de la conciliación entre las ciencias sociales-políticas y la tecnología para construir una visión holística de la ciberseguridad. Sin duda, la tecnología es la base del progreso de los pueblos y la esencia de la ciberseguridad.

La solución a los desafíos de la ciberseguridad no es solamente de carácter tecnológico, se trata también de la concientización, educación y capacitación. Por lo que los problemas de la ciberseguridad dependen de tres elementos principales: la tecnología, los procesos y las personas, debido a que el individuo es quién cierra el círculo de las fortalezas y vulnerabilidades; el usuario se considera no sólo la primera línea de defensa, sino también el mayor riesgo a la ciberseguridad.

BIBLIOGRAFÍA

Aguayo, S., & Bagley, B. (1990). *En busca de la seguridad perdida. Aproximaciones a la seguridad nacional*. Siglo XXI.

Ángel, A. (28 de octubre de 2013). Se registra un ciberataque a Presidencia cada 5 minutos. *24 horas*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio http://www.24-horas.mx/se-registra-un-ciberataque-a-presidencia-cada-5-minutos/

Animal Político. (18 de enero de 2017). Gasolinazo sume al gobierno de Peña en su nivel más bajo de aprobación; Morena gana puntos. *Animal Político*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.animalpolitico.com/2017/01/gasolinazo-encuesta-pena-popularidad/

Anónimo. (2017). Estrategia Nacional de Ciberseguridad. *gob.mx*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio https://www.gob.mx/mexicodigital/articulos/hacia-la-estrategia-nacional-de-ciberseguridad?idiom=es

Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia,* (149), 165-214.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology*, 12, 161-166.

Baldwin, D. A. (1997). The concept of security. *Review of international studies*, 23(01), 5-26.

Bloomberg. (12 de junio de 2015). ¡Cuidado, Pemex! El blanco predilecto de los hackers es el sector energético. *El Financiero*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio http://www.elfinanciero.com.mx/bloomberg/sector-energetico-el-blanco-predilecto-de-los-hackers.html

Buzan, B., & Hansen, L. (2010). *Defining-redefining security* (Vol. 2). Wiley-Blackwell in association with the International Studies Association.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: a new framework for analysis*. Lynne Rienner Publishers.

Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *SISTEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS)*, *119*, 4-7.

Cámara de Diputados. (26 de diciembre de 2005). Constitución Política de los Estados unidos mexicanos. *Congreso de la Unión*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.diputados.gob.mx/LeyesBiblio/pdf/1_240217.pdf

Cámara de Diputados. (26 de diciembre de 2005). Ley de Seguridad Nacional. *Congreso de la Unión*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

Carlisle, H. J. (1997). *The Changing Ends, Ways, and Means of National Security*. ARMY WAR COLL CARLISLE BARRACKS PA.

Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731

Cisneros, I. H. (2014). *De la razón de estado al gobierno democrático: Norberto Bobbio*. Instituto Electoral y de Participación Ciudadana del Estado de Jalisco.

Collins, A. (2016). *Contemporary security studies*. Oxford university press.

Condusef. (s.f.). Robo de identidad un delito en aumento. *Condusef*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

Confederación Patronal de la República Mexicana (COPARMEX). (2015). Índice de Desarrollo Democrático. COPARMEX. [Edición digital]. Recuperado el 18 de abril de 2017, del sitio http://www.idd-mex.org/2015/informes/2015/index.html

Córdova, Y. (18 de agosto de 2016). Ciberataques en México cuestan 24 millones de dólares al año: Lockton. *El Economista*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio http://eleconomista.com.mx/finanzas-publicas/2016/08/18/ciberataques-mexico-cuestan-24-millones-dolares-ano-lockton

Cruz, S. N. (22 de junio de 2015). Pemex y Cenace se blindan contra los ciberataques. *El Universal*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio http://archivo.eluniversal.com.mx/finanzas-cartera/2015/impreso/pemex-y-cenace-se-blindan-contra-los-ciberataques-120056.html

Dalby, S. (1997). Contesting an essential concept: Reading the dilemmas in contemporary security discourse. *Critical security studies: concepts and cases*, *3*, 31.

Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). *Security Solutions for Hyperconnectivity and the Internet of Things*. IGI Global.

Diccionario de la Real Academia Española (RAE). (s.f.). Seguridad. *RAE*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://dle.rae.es/srv/fetch?id=XTrIaQd

European Union, High Representative of the European Union for Foreign Affairs and Security Policy. (2013). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://ec.europa.eu/digitalagenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunitycyber-security

Farivar, C. (2009). A brief examination of media coverage of cyberattacks (2007-Present). *The virtual battlefield: Perspectives on cyber warfare*, 182-188.

García, L. F. H. (2014). Ciberseguridad; Respuesta global a las amenazas cibernéticas del s. XXI las ciberamenazas, un nuevo reto para la jefatura de información de la guardia civil. *3ª ÉPOCA*, 5.

Gribbon, L. (2013). *Cyber-security threat characterisation. A rapid comparative analysis*.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885.

Hempel, C. G. (1952). *Fundamentals of concept formation in empirical science*. Chicago University Press. p. 12

Hernández, V. (19 de mayo de 2015). Crearán un centro de desarrollo tecnológico. *www.elsiglodetorreon.com.mx* [Edición digital]. Recuperado el 20 de agosto de 2018, del sitio https://www.elsiglodetorreon.com.mx/noticia/1116138.crearan-un-centro-de-desarrollo-tecnologico.html

Herr, T., & Friedman, A. A. (2015). Redefining Cybersecurity. *The American Foreign Policy Council*.

Instituto Nacional de Estadística y Geografía (INEGI). (2016).Encuesta nacional de victimización y percepción sobre Seguridad Pública (ENVIPE) 2016. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales/especiales2016_09_04.pdf

International Organization for Standardization (ISO). (2012). "ISO/IEC 27032:2012." *ISO*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Internet Society. (2012). "Some Perspectives on Cybersecurity: 2012." *Internet Society*. [Edición digital]. Recuperado el 25 de agosto de 2018, del sitio https://www.internetsociety.org/wp-content/uploads/2017/08/bp-deconstructing-cybersecurity-16nov-update.pdf

Krause, M. (2016). *Índice de Calidad Institucional*. Red Liberal de América Latina.

Lippmann, W. (1943). *US foreign policy: Shield of the republic*. Boston Little Brown and Company.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 6, 9(1-2), 3-31.

Lynn, W. J. (2010). Defending a new domain: the Pentagon's cyberstrategy. *Foreign Affairs*, 89(5), 97-108.

Martini, B., & Choo, K. K. R. (2014). *Building the next generation of cyber security professionals*.

Maurer, T., & Morgus, R. (2014). Compilation of Existing Cybersecurity and Information Security Related Definitions. *New America*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://preview.newamerica.org/downloads/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions_Updated122015.pdf

Mitosfky. (2015). México: Confianza en Instituciones 2015. *Mitosfky*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://consulta.mx/index.php/estudios-e-investigaciones/mexico-opina/item/575-confianza-en-instituciones

Monterrosa, G. (18 de septiembre de 2016). México, indefenso ante ciberataques. *Contralínea*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio http://www.contralinea.com.mx/archivo-revista/index.php/2016/09/18/mexico-indefenso-ante-ciberataques/

Morgenthau,H. (1986). Política entre las naciones: la lucha por el poder y la paz. Buenos Aires: Editor Latinoamericano.

Organización de Estados Americanos (OEA). (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? *OEA y Banco Interamericano de Desarrollo BID*. [Edición digital]. Recuperado el 12 de abril de 2017, del sitio https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

Organización de Estados Americanos (OEA). (junio de 2014). Tendencias de Ciberseguridad en América Latina y el Caribe. *OEA y Sysmantec*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Platón. (2006). *La República*. Editorial Grupo Tomo.

Presidencia. (2014). 4º. Informe de Gobierno (2015-2016). *Presidencia de la República*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.presidencia.gob.mx/cuartoinforme/

Presidencia. (2014). Programa de Seguridad Nacional. *Presidencia de la República*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.presidencia.gob.mx/wp-content/uploads/2014/05/Programa-para-la-Seguridad-Nacional-Versio%CC%81n-Final.pdf

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, 26(3), 453–481

Secretaria de la Defensa Nacional (SDENA). (2013). Programa Sectorial de Defensa Nacional. *SEDENA*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.sedena.gob.mx/archivos/psdn_2013_2018.pdf

Secretaria de Marina (SEMAR). (2013). Programa Sectorial de Marina. *SEMAR*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www.semar.gob.mx/informes/programa_sectorial_13.pdf

Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk. *Chap. L. Rev*., 19, 445.

Sun Tzu. (1994). *El Arte de la Guerra*. México: Editorial Gemika.

Suprema Corte de Justicia de la Nación. (2005). Grandes temas del constitucionalismo mexicano. La Soberanía Nacional. Serie 4. Suprema Corte de Justicia de la Nación. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://sistemabibliotecario.scjn.gob.mx/sisbib/po2007/59129/59129_2.pdf

Sysmantec y Organización de Estados Americanos (OEA). (junio de 2014). Tendencias de Ciberseguridad en América Latina y el Caribe. *OEA y Sysmantec*. [Edición digital]. Recuperado el 01 de marzo de 2017, del sitio https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Sysmantec. (2016). Informe Norton sobre Ciberseguridad 2016. *Sysmantec*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

Ullman, R. H. (1983). Redefining security. *International security*, 8(1), 129-153.

Unión Internacional de Telecomunicaciones (UIT). (2010). Resolución 181. Recomendación UIT–T X.1205. *UIT*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Unión Internacional de Telecomunicaciones (UIT). (2015). Índice Global de Ciberseguridad. *UIT*. [Edición digital]. Recuperado el 25 de agosto de 2018, del sitio https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

Unión Internacional de Telecomunicaciones (UIT). (2017). Índice Global de Ciberseguridad. *UIT*. [Edición digital]. Recuperado el 25 de agosto de 2018, del sitio https://www.itu.int/pub/D-STR-GCI.01-2017

Unión Internacional de Telecomunicaciones (UIT). (2015). Annual Internet Threat Report 2015. *UIT*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf

Unit, E. I. (2016). Democracy index 2010. *The Economist*. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://pages.eiu.com/rs/783-XMC-194/images/Democracy_Index_2016.pdf

Waltz, K. (1979). *Theory of International Politics*. Addison Wesley Publising Company.

Wolfers, A. (1952). ""National Security" as an ambiguous symbol." *Political Science Quarterly*, 67. 481-502.

Muehlberghuber, M., Gürkaynak, F. K., Korak, T., Dunst, P., & Hutter, M. (2013, June). Red team vs. blue team hardware Trojan analysis: detection of a hardware Trojan on an actual ASIC. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy* (p. 1). ACM.

Wu, A., Ma, W. W., & Chan, W. W. (2015). "Whistleblower or Leaker?" Examining the Portrayal and Characterization of Edward Snowden in USA, UK, and HK Posts. In *New media, knowledge practices and multiliteracies* (pp. 53-66). Springer, Singapore.

Cussac, J. L. G. (2011). Estrategias legales frente a las ciberamenazas. *Cuadernos de estrategia*, (149), 83-127.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*, 5(5), 67.

Somuano Ventura, M. F., & Ortiz, R. Y. O. (2014). IDD-Mex: Índice de Desarrollo Democrático 2015. [Edición digital]. Recuperado el 28 de agosto de 2018, de *www. idd-mex. org*.

World Economic Forum (WEF). (2016). Índice de Competitividad 2016. *WEF*. [Edición digital]. Recuperado el 14 de abril de 2017, del sitio http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf