Desafíos a las Estrategias de Ciberseguridad en América
Challenges to Cybersecurity Strategies in America

Resumen

En el mundo hiperconectado del presente, los Estados deben contar con una estrategia que garantice el uso seguro del ciberespacio. Particularmente porque el impacto y frecuencia de los eventos que atentan contra la ciberseguridad se han multiplicado atentando no sólo contra la privacidad de los individuos, sino incluso poniendo en jaque la seguridad nacional. Por lo tanto, es preciso identificar las fortalezas y debilidades de los documentos rectores de la ciberseguridad en el continente americano para identificar los desafíos que enfrentan y reestimar las maneras para darles respuesta. El diseño de una Estrategia Nacional de Ciberseguridad otorga algunas de las herramientas necesarias para no solamente buscar, mantener o incrementar el ciberpoder en el nuevo campo de batalla de la era tecnológica, sino también para establecer un sistema de defensa activa.

Palabras clave

Seguridad Nacional, Ciberestrategia, Ciberseguridad Nacional, Ciberpoder, Ciberespacio

Abstract

In the current hyperconnected world, States must have a strategy that guarantees the use of cyberspace with security. Particularly because the impact and frequency of the events which attends against cybersecurity have been multiplied threatening not only the individual privacy, but also putting the national security in check. Therefore, it is necessary to identify the strengths and weaknesses of the cybersecurity guide documents in the American continent in order to identify the challenges that they face and re-estimate the manners for giving them an answer. The design of a National Cybersecurity Strategy provides some of the necessary tools to not only seek, maintain or increase the cyberpower in the new battlefield of the technological era, but also to establish an active defense system.

Key words

National Security, CyberStrategy, National Cybersecurity, Cyberpower, Cyberspace

Maestro
Adolfo Arreola García

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.

correo: adolfoarreola@yahoo.com.mx

Artículo recibido el 20 de octubre de 2019. Aprobado el 5 de diciembre de 2019.

Los errores remanentes son responsabilidad de los autores.
El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamete coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Metodología

El presente trabajo se basa en el análisis literario, de discurso e histórico de diversos documentos oficiales, académicos, gubernamentales, tecnológicos y mediáticos que permiten abordar el tema desde perspectivas teóricas y mediático-realistas, es decir desde los acontecimientos que ocurren en el día a día. Lo anterior teniendo por objetivo 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 recurrentes que permiten anticiparse a los hechos aplicando los preceptos teóricos.

En la estrategia todo resulta muy simple, pero no por ello muy fácil.
Carl von Clausewitz

Introducción

En el mundo hiperconectado de la actualidad es imperativo contar con una estrategia para obtener las mayores ventajas y sufrir los menores daños en las operaciones diarias en el ciberespacio. Esta necesidad estratégica ha evolucionado debido a que en años recientes el número de incidentes que comprometen la ciberseguridad de los Estados ha ido en aumento poniendo en riesgo la integridad de la información, la confiabilidad de la red, la seguridad de los usuarios y la ciberseguridad nacional. El impacto de los ciberataques ha cruzado el Rubicón entre el mundo material y el virtual (Johnson y Tierney, 2011). A pesar de los numerosos métodos de ataque, las amenazas provienen de dos categorías de eventos adversos que podrían encajonarse en: 1) operaciones de ciberguerra y 2) actividades del cibercrimen.

Por un lado, de acuerdo con Manuel R. Torres (2010: 339) las acciones bélicas (ciberataques) icónicas de las últimas décadas son: la explosión en el sistema de distribución de gas en la Unión Soviética en 1982, el ciberataque contra empresas estadounidenses conocido como *Titan Rain* entre 2003 – 2005, el ciberataque contra Estonia del 2007, el ciberataque contra las defensas aéreas de Siria en 2007, las acciones de ciberguerra durante la guerra en Osetia del Sur en Georgia durante el 2008 y el ciberataque con Stuxnet contra el programa nuclear iraní descubierto en 2010. En general, los efectos y poder destructivo de la ciberguerra (entendido como conflicto entre fuerzas de dos Estados) se logra por medio de la manipulación de los sistemas de control y por el engaño de las ciberdefensas; es evidente, que la superioridad en el ciberespacio brinda la libertad de acción y la ventaja ofensiva por medio de la sorpresa.

Por el otro lado, en 2016, un informe conjunto de la Organización de los Estados Americanos (OEA) y del Banco Interamericano de Desarrollo (BID) señaló que el cibercrimen cuesta al mundo 575,000 millones de dólares lo que equivale a un 0.5% del PIB mundial. De esta cantidad el monto total correspondiente para América Latina es de 90,000 millones de dólares anuales (BID y OEA, 2016). El cibercrimen

engloba acciones como: la suplantación de identidad, el robo de información o de capitales, la venta de productos y servicios ilegales en internet, la pornografía infantil, el grooming, el ciberespionaje, entre muchas otras.

Sin importar si los eventos cibernéticos adversos son efectuados por Estados, organismos o individuos estos conllevan una serie de características particulares que han contribuido a su proliferación. Entre otras cosas, los ataques en el ciberespacio son de bajo costo, difíciles de rastrearse y no pueden ser atribuidos de manera precisa, lo que los convierte en una alternativa para generar daños importantes contra un enemigo sin ser castigado o ni siquiera ser identificado/detectado. Por lo tanto, para evitar ser culpados, algunos Estados inclusive han recurrido a la creación de grupos paramilitares o hacktivistas que sumados a los cibermercenarios han realizados acciones en favor de sus intereses sin establecer un vínculo identificable de manera fácil, precisa y oportuna.

Ante esta realidad compleja, en la cual la atribución de los ataques es la principal limitante para la respuesta de la víctima, los Estados en América cuentan con una capacidad de respuesta ya instalada. Sin embargo, solamente 10 han diseñado una estrategia de ciberseguridad nacional para proteger el ciberespacio y en su caso contar con elementos suficientes de ciberpoder.

El objetivo del presente trabajo es destacar los desafíos que enfrentan las diez primeras Estrategias de Ciberseguridad que se han aprobado en el Continente Americano poniendo énfasis en los aspectos técnicos, administrativos, de atribución, organizacionales y de recursos humanos necesarios para la lograr seguridad en el ciberespacio. Del mismo modo se hará referencia a las estructuras institucionales a cargo de la implementación y seguimiento de las distintas Estrategias. Todo lo anterior representa un ejercicio para identificar y mitigar los potenciales riesgos que pudieran surgir por un diseño inadecuado de los documentos rectores de la ciberseguridad nacional de los Estados.

El trabajo incluye primeramente una revisión de las características del ciberespacio y el ciberpoder, así mismo una propuesta de definición de ciberseguridad nacional a fin de establecer su importancia dentro de las Estrategias Nacionales de Ciberseguridad; posteriormente, se detallan las características de las Estrategias Nacionales vigentes en el continente americano; en el tercer apartado se definen algunos de los muchos desafíos que enfrentan las estrategias de ciberseguridad de los Estados de América y, finalmente; se presentan algunas conclusiones sobre el tema.

El ciberespacio, el ciberpoder y la ciberseguridad nacional

Ciberespacio

El ciberespacio ha sido considerado como el quinto ámbito de la guerra (Lynn, 2010) por lo tanto las operaciones militares se realizan utilizando el ciberespacio no solamente como el medio por excelencia, sino también como el campo de batalla (Arreola, 2016). De hecho, de acuerdo con Arreola (2016: 109) «el ciberespacio se ha convertido en un ámbito de la guerra en donde las vulnerabilidades del enemigo

son explotadas sin necesidad de la fuerza» ya que la tecnología, la información y el espectro electromagnético se convierten tanto en armas de ataque y destrucción de largo alcance y omnipresentes que ponen en práctica el ciberpoder, como en los medios esenciales para instalar una defensa en profundidad de la información e instalaciones críticas.

Es decir, sin importar si las operaciones en el ciberespacio son ofensivas o defensivas, según marque la estrategia de ciberseguridad nacional, el ciberespacio será la constante. En otras palabras, el ciberespacio facilita que los eventos bélicos escalen desde un ámbito regional a uno global, debido ya sea a daños colaterales en las actividades o ciberinfraestructuras internacionales, o por su capacidad para movilizar a los gobiernos y a la opinión pública mundial. De acuerdo con David Betz and Tim Stevens (2011: 39) la ocurrencia simultánea de la causa y el efecto en el ciberespacio tiene ramificaciones en el ejercicio del poder, ya que a pesar de la distancia física el efecto es casi inmediato permitiendo que el número de actores afectados por el ciberpoder se multiplique. Siendo el ciberespacio además una creación humana, es preciso reconocer las capas que lo componen para el reconocimiento de sus detalles. De acuerdo con Martin Libicki (2009: 12 y 13) el ciberespacio se compone de tres capas: física, sintáctica y semántica.

- En la capa física se integran todas los componentes y cableado, esta capa es esencial para la existencia del ciberespacio porque si se remueve desaparece el ámbito virtual.
- La capa sintáctica está compuesta por las instrucciones que tanto los diseñadores como los usuarios dan a las máquinas, así como por los protocolos que utilizan las computadoras para interactuar entre sí. Es nuestra visión que es en esta capa donde los hackeos tienen lugar y los ataques virtuales o ciberataques pueden realizarse con mayor impacto debido al uso del engaño, la invisibilidad y la sorpresa.
- La capa superior es la semántica que es donde se encuentra la información que se encuentra en la máquina en forma clara o en lenguaje de programación.

De hecho, la información que se encuentra en las computadoras se puede clasificar en aquella que sirve para manipular el sistema, aquella que controla a las máquinas y la información para el usuario. En otras palabras, una parte de la información que se encuentra en las computadoras sirve para manipular el sistema (aunque es sintáctica en su propósito es semántica en su forma), otra información incluye instrucciones o control de procesos que sirve para el control de las máquinas o procesos controlados por computadora y, finalmente; el resto de la información tiene significado únicamente para las personas ya que se encuentra en un lenguaje claro.

Además, el ciberespacio tiene una serie de características principales que permiten sentir sus efectos no sólo dentro del ciberespacio, sino en el resto de los ámbitos de la guerra y por ende en el ser humano. De acuerdo con John Sheldon (2011: 96-100) las principales características del ciberespacio son que: depende del espectro electromagnético, requiere de objetos fabricados por el hombre, puede ser constantemente replicado, es de bajo costo, la ofensiva es predominante, y consiste de cuatro capas (lo que complementa lo que fue afirmado por Libicki al agregar una capa para la infraestructura), todo lo anterior permite que el ciberpoder sea ubicuo/generalizado, complementario y furtivo.

Figura 1. Elementos del ciberespacio

Elaboración propia

Aunque el ciberespacio es el cúmulo de tecnologías desarrolladas por la sociedad de la información que ha revolucionado los asuntos militares y todas las actividades sociales, difiere de sus predecesores tecnológicos porque de acuerdo con Daniel T. Kuehl (2009: 28) se ha convertido en el medio predominante para crear, almacenar, modificar y explotar la información. Lo que remarca su diferencia con los anteriores dispositivos electrónicos que solamente transmitían y recibían información. Estas características han llevado a que las tecnologías de la información y comunicación permeen todas las actividades generando nuevas vulnerabilidades y creando el contexto estratégico para el empleo del ciberpoder. Sheldon (2011: 101) dice que «Esta expansión, profundización y dependencia cada vez más generalizada del ciberespacio es parte del mosaico del cambiante entorno geopolítico y económico mundial» que conforma el contexto estratégico internacional actual en donde el ciberpoder tiene y tendrá un papel preponderante.

Ciberpoder

A nivel global se están dando nuevos alineamientos geopolíticos que de acuerdo con Philip Stephens darán lugar a un mundo multipolar. En las palabras de Stephens (2010) esto es:

> Un mundo multipolar ha sido pronosticado durante mucho tiempo, pero siempre pareció estar posado con seguridad en el horizonte. Ahora se ha precipitado de repente al presente. . . La forma perezosa de describir el nuevo paisaje geopolítico es una disputa entre Occidente y el resto: entre las democracias liberales occidentales y las autocracias de economía de mercado oriental. A pesar de lo ordenadas que pueden parecer estas divisiones, extrañan las complejidades. Ninguno está más determinado, por ejemplo, que Rusia y China para evitar que India obtenga un asiento permanente en el Consejo de Seguridad de la ONU. Pocos están más preocupados que India por el crecimiento militar de China. . . Las naciones en ascenso premian el poder estatal sobre las

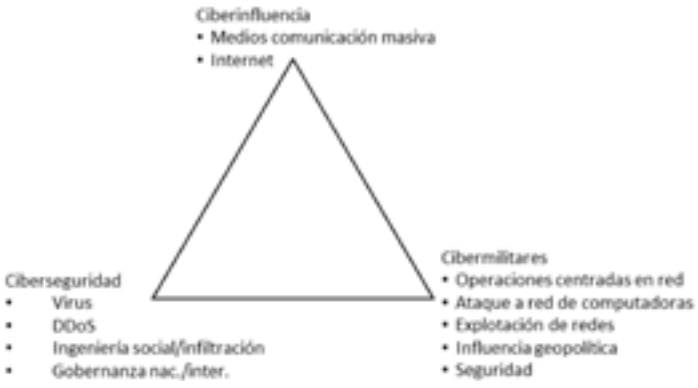
> reglas internacionales, la soberanía sobre el multilateralismo. Es probable que la transición a un nuevo orden vea más rivalidad y competencia que cooperación. Los hechos de la interdependencia no pueden ser desechados, pero ciertamente serán probados. Va a ser un viaje lleno de baches.

Es evidente que existe una lucha en el contexto internacional para modificar el juego geoestratégico. Sin duda, el «ciberpoder se puede utilizar en la paz y la guerra porque, entre sus muchos otros atributos, es sigiloso y encubierto, relativamente barato, y su uso favorece la ofensiva y es difícil de atribuir al autor» (Sheldon, 2011: 101) y se convertirá en una ventaja comparativa para los Estados técnicamente avanzados. Lo que se ve apoyado por el pensamiento de Bertrand Rusell (2004: 23) que dice que el poder debe ser visto como «la producción de los efectos pretendidos» que sería la percepción de los estrategas que piensan que la estrategia es desatar el poder inherente en las capacidades nacionales para que impacten en los resultados del interés nacional que compite con el resto de los actores de la sociedad internacional.

En el caso del ciberpoder, de acuerdo con Betz y Stevens (2011: 45-51) este se clasifica en obligatorio (uso directo de la coerción), institucional (control indirecto de actores por medio de las instituciones), estructural (mantiene las estructuras entre actores) y, productivo (produce y refuerza los discursos existentes – quizás el más importante de todos debido a la diplomacia pública y comunicación estratégica). La recomendación es utilizar las diversas formas combinadas en una fórmula flexible, dinámico y eficiente; es decir, «Sólo un trato redondeado de las diversas formas de ciberpoder proporcionará una base adecuada para otras consideraciones de lo que podría constituir el ciberpoder nacional como un componente integral de la estrategia nacional» (Betz y Stevens, 2011: 53).

En breve, el ciberpoder es la manifestación del poder en el ciberespacio, en donde el poder se entiende de acuerdo con Max Weber (Gerth y Mills, 1948: 180) como «la oportunidad de un hombre o de varios hombres de realizar su propia voluntad en una acción comunitaria, incluso contra la resistencia de otros participantes de la misma acción». Las actividades del ciberpoder incluyen: la ciberinfluencia, las operaciones cibermillitares y la ciberseguridad.

Figura 2. Actividades de ciberpoder



Ciberseguridad Nacional

Desde el punto de vista 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).

Por lo tanto, ya que en el contexto internacional del siglo XXI las tecnologías de la información y comunicaciones tienen un papel preponderante, es preciso contar con un concepto y una estrategia[1] de ciberseguridad nacional que implementen acciones políticas y jurídicas para salvaguardar los recursos materiales en todos los ámbitos de combate[2] con un enfoque multidisciplinario, multidimensional y multinivel. Esta propuesta se hace como parte integral de la reconceptualización de la seguridad nacional e internacional que permite incorporar nuevos, ámbitos, actores, factores, temas y condiciones (Dalby, 1997).

Por ello, partiendo del concepto de ciberseguridad diseñado por la Unión Internacional de Telecomunicaciones (UIT, 2010) se propone que la ciberseguridad nacional se entienda como: las 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 informáticos de la nación, resguardar la infraestructura crítica o activos estratégicos, implementar la ciberseguridad pública, organizar la ciberdefensa, proteger la información y cuidar a los usuarios en el ciberentorno contra amenazas internas o externas. Que establece la división de la ciberseguridad nacional en dos ramas: la ciberseguridad pública (cibercrimen) a cargo de los organismos policiales y la ciberdefensa (ciberseguridad nacional) responsabilidad de las fuerzas armadas.

Las Estrategias Nacionales de Ciberseguridad en América

Ante la realidad que se vive en el mundo digital y los efectos crecientes de los ciberataques, hasta principios de 2018, en la región de América Latina y el Caribe un total de ocho países habían adoptado una Estrategia Nacional de Ciberseguridad. A los ocho anteriores hay que sumarles a EE.UU. y Canadá en la región de América del Norte (sin contar a México). Según Leiva (2015) el hecho de que para 2015 sólo seis Estados de América Latina hayan adoptado una Estrategia Nacional de Ciberseguridad fue resultado de dos factores que impidieron su adopción: primero, la falta de recursos dedicados a este tema; y segundo, la falta de experiencia práctica y conocimientos especializados para diseñar e implementar una estrategia nacional con eficacia. No obstante, la Organización de Estados Americanos (OEA) ha jugado un papel preponderante en lo que se refiere al apoyo técnico, y en casos como México también en apoyo administrativo.

1 La 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.

2 Existen cinco ámbitos del combate o de la guerra: aire, mar, tierra, espacio y ciberespacio.

Las Estrategias se enmarcan en la resolución de la OEA AG/RES. 2004 (XXXIV-O/04) denominada «Adopción de una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética» y la declaración sobre el «Fortalecimiento de la Ciberseguridad en las Américas» en marzo de 2012. De igual forma buscan cumplir con tratados internacionales como la Convención de Budapest que fue publicada en 2001.

Como se dijo anteriormente, hasta inicios de 2018, en América Latina y el Caribe eran ocho los Estados con una Estrategia Nacional de Ciberseguridad. El último en presentar su estrategia fue México (13 noviembre de 2017), uniéndose a Colombia (2011 y 2016), Panamá (2013), Paraguay (abril de 2017), Chile (abril de 2017) y Costa Rica (abril de 2017). Los dos países del Caribe que cuenta con una Estrategia Nacional de Ciberseguridad son Trinidad y Tobago (2013) y Jamaica (2015). Sin duda, tanto EE.UU. (2003) y Canadá (2018) son líderes en la región de América del Norte en el diseño e implementación de sus estrategias respectivas. En resumen, en 2017 solamente 10 Estados del total del Continente Americano contaban con una estrategia de ciberseguridad, lo que denota la poca consideración que se le da al tema en dicha esfera geográfica a pesar del incremento en el número e impacto de los ciberataques. En junio de 2018 Guatemala y República Dominicana publicaron su Estrategia Nacional de Ciberseguridad, pero no serán incluidas. Brasil no tiene estrategia, pero cuenta con una política robusta en temas de ciberseguridad.

América del Norte

Canadá

Una versión inicial fue creada el 2010. Ahora la Estrategia Nacional de Ciberseguridad cuenta con una versión que fue presentada en 2018 (Department of Public Safety and Emergency Preparadness, 2018). Busca atender los riesgos que han llegado con el uso intensivo de la tecnología en la vida diaria, creando confianza en el mundo digital con un sistema de ciberseguridad que acompañe a la innovación y sea el protector de la prosperidad. La Estrategia busca cumplir con los objetivos y prioridades de los canadienses en materia de ciberseguridad. La Estrategia de Canadá cuenta con tres pilares de acción: dar seguridad a los sistemas gubernamentales, hacer sociedad fuera del gobierno federal para asegurar los sistemas cibernéticos vitales y, ayudar a la sociedad canadiense a estar segura cuanto trabaja en línea. Menciona también los siguientes objetivos estratégicos: dar seguridad y resiliencia a los sistemas canadienses, innovación en cuestiones cibernéticas, así como liderazgo y colaboración.

La Estrategia canadiense menciona que existen tres tendencias que representan las áreas que deben ser fortalecidas para garantizar la ciberseguridad nacional. La primera tendencia engloba el apoyo al esfuerzo de las agencias de aplicación de la ley para combatir el cibercrimen al mismo tiempo que se respeta la privacidad; la segunda, menciona la necesidad imperiosa de contar con personal profesional con mejor conocimiento y habilidades en cuestiones de ciberseguridad; y la tercera, pide

el liderazgo absoluto del gobierno federal para impulsar la cooperación nacional, las inversiones, salvaguardar la información, cuidar los derechos humanos y las libertades de los ciudadanos.

De acuerdo con la Estrategia Nacional de Ciberseguridad de Canadá (2018) los principales desafíos que enfrenta son: el incremento del número de ciberataques y su impacto en los diferentes sectores del quehacer humano, el dilema que existe para brindar seguridad sin afectar la privacidad ya que la libertad requiere tanto de seguridad como de privacidad, y la reorganización de sus fuerzas para integrar un solo centro de mando y control. Por lo tanto, el gobierno canadiense propone generar un cultura de la ciberseguridad a nivel nacional, fortalecer los sistemas de ciberseguridad bajo control del gobierno, mejorar las capacidades de reacción de las fuerza pública para mitigar el impacto de los eventos cibernéticos adversos y responder al cibercrimen, procurar que los medios para lograr un sistema de ciberseguridad en todos los niveles y sectores productivos estén disponibles a precios accesibles, y aplicar las capacidades cibernéticas del gobierno para implementar una defensa activa de la infraestructura crítica. Para dar cumplimiento a los objetivos se tiene al Centro de Ciberseguridad de Canadá, la Unidad Nacional de Coordinación sobre Cibercrimen, que trabajan en conjunto con el Department of Public Safety and Emergency Preparadness.

EE.UU.

La Estrategia Nacional para asegurar el Ciberespacio (2003) es parte de esfuerzo nacional de EE.UU. para proteger su nación que fue presentado por el presidente George W. Bush. Define que el buen funcionamiento del ciberespacio es esencial para la economía y la seguridad nacional. Tiene como propósito involucrar y capacitar a los estadounidenses para asegurar las partes del ciberespacio que poseen, operan, controlan o con las que interactúan. Menciona tres objetivos estratégicos: prevenir ciberataques contra la infraestructura crítica estadounidense, reducir la vulnerabilidad nacional a ciberataques y, minimizar el daño y el tiempo de recuperación en caso de sufrir un ciberataque.

Esta estrategia posteriormente evoluciona con el presidente Barack Obama dando lugar a la Cyberspace Policy Review (2009), International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (2011), Draft Strategy for Improving Critical Infrastructure Cybersecurity (2014), President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity (2013) y, The Department of Defence Cyber Strategy (2015). El último de los documentos mencionados será considerado como la última versión de un esfuerzo nacional para garantizar la ciberseguridad (Carter, 2015). Actualmente, aunque cuenta con una amplia legislación sobre ciberseguridad no cuenta con una Estrategia Nacional de Ciberseguridad (Starks, 2018).

La ciberestrategia del Departamento de Defensa (DoD) tiene los siguientes objetivos estratégicos: Construir y mantener las fuerzas y capacidades listas para realizar operaciones en el ciberespacio; defender la red de información del DoD, asegurar los datos del Departamento de Defensa y mitigar los riesgos para las mi-

siones del Departamento de Defensa; estar preparado para defender a EE. UU. y sus intereses vitales contra ciberataques disruptivos o destructivos de consecuencias importantes; crear y mantener opciones cibernéticas viables y planificar el uso de esas opciones para controlar la escalada de conflictos y configurar el entorno de conflicto en todas las etapas; y crear y mantener asociaciones y alianzas internacionales sólidas para disuadir las amenazas compartidas y aumentar la seguridad y la estabilidad internacional.

La estrategia de seguridad de EE.UU. menciona que para ganar la superioridad estratégica se debe obtener el control del ciberespacio. Particularmente, la Estrategia Militar Nacional para las Operaciones Cibernéticas de 2005 menciona de manera explícita que «es una aproximación estratégica amplia para emplear las ciberoperaciones con el objetivo de asegurar la superioridad estratégica para EE.UU. en dicho dominio» (DoD, 2005: vii). La superioridad en el ciberespacio brindará la libertad de acción a las fuerzas amigas y la negará al enemigo. Es decir, el ciberespacio es un medio eficaz para lograr la superioridad estratégica tan necesaria para avanzar o lograr los objetivos políticos. A lo anterior hay que agregar los imperativos estratégicos que son definidos por el DoD (2005: 10) como «las consideraciones que se deben tomar en cuenta para operar exitosamente en el ciberespacio». Estos imperativos son: operaciones ofensivas/defensivas, integración, compartir información, habilidad para operar en situación degradada, relaciones de mando, mando y control, configuración de la gestión, aplicación de políticas y normas, comprender el ciberespacio y la defensa de EE.UU.

Lo anterior coincide con la visión de Sheldon (2011: 95) quien considera que el ciberpoder tiene como propósito estratégico alcanzar los objetivos políticos. Este propósito se desarrolla alrededor de la «habilidad tanto en la paz como en la guerra para manipular las percepciones del contexto estratégico para la ventaja propia al mismo tiempo que se degrada la habilidad del adversario para comprender dicho contexto». Lo que hace recordar que la transformación de los efectos del ciberpoder en objetivos de política es el arte y la ciencia de la estrategia, definida como «el manejo del contexto para lograr la ventaja continua según la política» (Dolman, 2005: 6). Lo anterior se sustenta con las palabras de Clausewitz (1976: 177) que considera la estrategia como «el uso de los combates para el objetivo de la guerra».

Para atender las necesidades de ciberseguridad EE.UU. cuenta con la dirección del Asesor Principal en cuestiones Ciber, que tendrá a su cargo el desarrollo de la política y estrategia de ciberseguridad del DoD. Dentro de las fuerzas armadas se ha organizado el Cibercomando de EE.UU. Además, cuenta con un total de 133 equipos de ciberdefensa y ciberdisuasión en el ciberespacio agrupados en Equipos Nacionales, Equipos de Ciberprotección, Equipos de Misiones de Combate y Equipos de Apoyo (DoD, 2018). Todos ellos se enfocan en el cumplimiento de las tres misiones principales: defender las redes, sistemas e información del DoD, defender la patria estadounidense y los intereses de EE.UU. contra ciberataques y, brindar apoyo a los planes de contingencia y operacionales de las fuerzas armadas.

México

La Estrategia Nacional de Ciberseguridad (ENC) de México identifica tres principios rectores, establece un objetivo general y cinco estratégicos, define ocho ejes trasversales e identifica a los actores involucrados. México presentó su ENC a finales de 2017 enlistando los siguientes tres principios rectores: 1) Perspectiva de derechos humanos, 2) Enfoque basado en gestión de riesgos y, 3) Colaboración multidisciplinaria y de múltiples actores. Por otro lado, la ENC de México tiene por 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 TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. (Gobierno de México, 2017: 16).

Definición que se queda corta al mencionar solamente que el uso de las TIC será con responsabilidad sin aclarar que debe ser también con seguridad, no incluir la protección del ciberentorno, dejar fuera la ciberdefensa y ciberseguridad nacional, estar desvinculada de los objetivos estratégicos y no brindar una guía clara sobre las medidas que deben adoptarse. Los cinco objetivos estratégicos son: Sociedad y Derechos, Economía e Innovación, Instituciones Públicas, Seguridad Pública y Seguridad Nacional. Dicha ENC además comprende ocho ejes transversales (cultura de ciberseguridad; desarrollo de capacidades; coordinación y colaboración; investigación, desarrollo e innovación en TIC; estándares y criterios técnicos; infraestructuras críticas; marco jurídico y autorregulación; y, medición y seguimiento) que buscan cumplir con los siguientes cinco objetivos estratégicos.

En lo referente a la estructura institucional en 2017, se creó la Subcomisión de Ciberseguridad (Gobierno de México, 2018) compuesta por varias entidades y dependencias de la Administración Pública Federal, para velar por la ciberseguridad con el liderazgo de la Policía Federal Científica. Recientemente el Índice Global de Ciberseguridad 2017 que publicó la Unión Internacional de Telecomunicaciones (UIT), colocó a México como el tercer país mejor posicionado de América, sólo detrás de Estados Unidos y Canadá, ubicándolo por encima de todos los países de la región latinoamericana y en el lugar 28 de 165 países considerados por el estudio, lo cual es una cuestión que genera escepticismo entre los especialistas, y genera preguntas sobre sí ¿verdaderamente estamos preparados?

América Latina

Colombia y su Política Nacional de Seguridad Digital

Colombia fue el primer país latinoamericano en contar con una Estrategia Nacional de Ciberseguridad. Dicho documento fue aprobado en 2011; en el 2016 realizaron la primera revisión y modificación que dio lugar a la Política Nacional de Seguridad Nacional (CONPES, 2016). En esta nueva versión se pone énfasis en la reducción de la efectividad de las amenazas por medio del fortalecimiento de las

capacidades de los diversos actores.

La Estrategia establece un establece objetivo general, cinco objetivos específicos y 18 estrategias que se implementarán para lograrlos; además incluye un cronograma de implementación y un esquema detallado para su financiamiento. Los cuatro principios fundamentales de la Estrategia son: Salvaguardar los derechos humanos y los valores fundamentales, Adoptar un enfoque incluyente y colaborativo, Asegurar una responsabilidad compartida, y Adoptar un enfoque basado en la gestión de riesgos. Por otro lado, las cinco dimensiones estratégicas son: Gobernanza de la seguridad digital, Marco legal y regulatorio de la seguridad digital, Gestión sistemática y cíclica del riesgo de seguridad digital, Cultura ciudadana para la seguridad digital, y fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital.

El gobierno en esta Política ha identificado que la ciberseguridad es una responsabilidad de todos y no solamente del gobierno. El objetivo general de la Estrategia es el de:

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (CONPES, 2016: 47).

Para cumplir con dicho objetivo fueron diseñados cinco objetivos específicos y dieciocho estrategias delimitadas por las cinco dimensiones estratégicas mencionadas anteriormente. Los cinco objetivos específicos son: Establecer un marco institucional para la seguridad digital, Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos, Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos, y Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional.

Lo interesante de esta Política es que cuenta con un plan detallado de las estrategias, los tiempos requeridos y las instituciones responsables y los recursos necesarios para lograr tal objetivo. En resumen, la Política Nacional de Seguridad Digital incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital y, establece que las instituciones encargadas de ejecutar la Estrategia son el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Nacional de Planeación y la Dirección Nacional de Inteligencia.

Costa Rica

En el 2017 Costa Rica presentó su Estrategia Nacional de Ciberseguridad (MICITT, 2017), documento que marca la pauta a seguir en materia de ciberse-

guridad atendiendo los potenciales retos que se deben vencer. Dicho documento estratégico cuenta con un objetivo general, ocho objetivos específicos y 20 líneas estratégicas. El objetivo general busca:

> Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país. (MICITT, 2017: 38).

Los cuatro principios rectores son: Las personas son prioridad, Respeto a los Derechos Humanos y la Privacidad, Coordinación y corresponsabilidad de múltiples partes interesadas y, Cooperación Internacional. El objetivo general se apoya en ocho objetivos específicos que son: Coordinación Nacional, Conciencia Pública, Desarrollo de la Capacidad Nacional de Seguridad Cibernética, Fortalecimiento del Marco Jurídico en Ciberseguridad y TIC, Protección de Infraestructuras Críticas, Gestión de Riesgo, Cooperación y Compromiso Internacional e, Implementación, Seguimiento y Evaluación.

Desde 2010 cuenta con la Comisión Nacional de Seguridad en Línea (CNSL). El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el encargado de supervisar la implementación y hacer el seguimiento de las tareas que se le hayan asignado a cada uno de los actores implicados en la Estrategia. Además, dicho organismo cuenta con el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT – CR) para hacer frente a los incidentes de ciberseguridad. Del mismo modo, el MICITT es responsable de evaluar el cumplimiento de los objetivos. Por disposición de ley la estrategia debe ser revisada cada dos años.

Chile

Chile presentó su Política Nacional de Ciberseguridad (PNC) en 2017, documento en el cual expone de manera detallada las tareas que serán emprendidas en el corto y mediano plazo, así como las instituciones encargadas de la implementación de dicha política. Sus objetivos tienen como límite el 2022, pero la estrategia incluye un total de 41 medidas de política pública que deberán ser alcanzadas en el periodo 2017-2018. Los objetivos para el 2022 son seis que a su vez tienen diversos objetivos específicos (un total de 22) como se cita a continuación.

1. Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad. Con los objetivos específicos siguientes. Identificación y gestión de riesgos, llevando a cabo medidas de monitoreo a fin de generar un ciberespacio resiliente; Protección de la infraestructura de la información; Identificación y jerarquización de las infraestructuras crítica de la información; Contar con equipos de respuesta a incidentes de ciberseguridad; Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes; y, Exigencia de estándares diferenciados en materia de ciberseguridad.

2. Garantizar los derechos de los ciudadanos en el ciberespacio. Que se complementa con los siguientes objetivos específicos: Prevención de ilícitos y generación de confianza en el ciberespacio; Establecimiento de prioridades en la implementación de medidas sancionatorias; Prevención multisectorial; y, Respeto y promoción de derechos fundamentales.
3. Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación. Indica los siguientes objetivos específicos: Una cultura de ciberseguridad; Sensibilización e información a la comunidad; y Formación para la ciberseguridad.
4. Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales. Son cuatro sus objetivos específicos. Principios de política exterior chilena; Cooperación y asistencia; Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas; y Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio.
5. Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país. Contiene cinco objetivos específicos: Importancia de la innovación y desarrollo en materia de ciberseguridad; Ciberseguridad como medio para contribuir al desarrollo digital de Chile; Desarrollo de la industria de ciberseguridad en Chile; Contribuir a la generación de oferta por parte de la industria local; y Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado.

En lo que respecta a la organización del sistema de ciberseguridad la PNC prevé que una ley contemple la estructura y la gobernanza que debe ser preparada por las instituciones responsables. De manera temporal, el CSIRT Gob es la instancia encargada de gestionar los incidentes generados en la Red de Conectividad del Estado, mientras que a nivel político propone postergar y ampliar el mandato del Comité Interministerial cuyas funciones se circunscriben a los ámbitos de la comunicación, coordinación y seguimiento de las medidas contenidas en la PNC. En general, representa una estructura de la PNC muy similar a las adoptadas por el resto de los Estados de la región.

Panamá

Panamá elaboró en 2013 la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, título en donde sobresale la protección de las infraestructuras críticas del Estado. La Estrategia Nacional para la Innovación Gubernamental de Panamá busca el fortalecimiento de todas las instituciones del país. Aunque esta carente de profundidad en su propuesta, existe una legislación sustanciosa en ciberseguridad. El objetivo del Estado panameño, mediante el desarrollo de la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, es el de:

> aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para redundar en un incremento de la seguridad cibernética que

> permita el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, todo esto salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado. (Consejo Nacional para la Innovación Gubernamental, 2013: 3).

Para lograr dicho objetivo las acciones se alinean en los ejes organizativo, legal, tecnológico y cultural. Al mismo tiempo, busca proteger los sistemas y redes informáticas y sensibilizar a las partes implicadas sobre los riesgos que enfrentan durante el uso de las TIC. No presenta de manera explícita los principios, pero se puede asumir que busca la protección de los derechos humanos y las libertades fundamentales, la no discriminación, la corresponsabilidad en el uso de las TIC y la colaboración entre las partes interesadas. Por otro lado, la Estrategia panameña indica seis pilares que son: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio, Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos, Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales, Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región, Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares y, Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.

Para lograr la implementación de la Estrategia y el objetivo general propuesto el gobierno panameño creará programas para mejorar la clasificación de información, adopción de las mejores prácticas y las capacidades de respuesta. Por ello, la Estrategia identifica y clasifica los riesgos que enfrenta la nación como un todo. Finalmente, indica que las instituciones encargadas de la ciberseguridad serán la Autoridad de Innovación Gubernamental, el Consejo Nacional para la Innovación Gubernamental y el Computer Security Incident Response Team (CSIRT) Panamá.

Paraguay

Paraguay presentó en 2017 el Plan Nacional de Ciberseguridad que es un documento estratégico fundamental para las políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptadas para fortalecer la seguridad de sus activos críticos y proteger el ciberespacio. Dicho como plan en su diagnóstico afirma que Paraguay es el país con la población de usuarios que ha crecido con mayor velocidad entre 2010-2014, y en consecuencia es prioritario el fortalecimiento de la ciberseguridad en su territorio. Lo anterior se hará sin dejar de fomentar un entorno económico innovador y respetar los derechos fundamentales.

A diferencia de las otras estrategias de la región, el Plan Nacional de Ciberseguridad presenta una serie de objetivos generales bajo el nombre de ejes, 20 objetivos específicos para su lograrlos y 60 líneas de acción. El Plan Nacional de Ciberseguridad se concentra en los siguientes seis ejes de acción: (i) Sensibilización y Cultura; (ii) Investigación, Desarrollo e Innovación; (iii) Protección de Infraestructuras Críticas;

(iv) Capacidad de Respuesta ante Incidentes Cibernéticos; (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia; y (vi) Administración Pública y (vii) Sistema Nacional de Ciberseguridad.

Sobresale que en este documento se mencionen los siguientes principios orientadores para la formulación e implementación de cualquier política pública de ciberseguridad: proporcionalidad, coordinación de esfuerzos y uso eficiente de recursos escasos, responsabilidad compartida, desarrollo e innovación, cooperación internacional y, monitoreo y evaluación. En cuestión de atribuciones, el Sistema Nacional de Ciberseguridad constituye la estructura institucional que aplica el Plan, cuyos componentes son el Coordinador Nacional de Ciberseguridad y la Comisión Nacional de Ciberseguridad. Este Plan y la Política Nacional de Ciberseguridad deben ser revisado cada tres años.

Región del Caribe

Jamaica

En el caso de Jamaica la ciberseguridad contó con un documento rector desde 2015 bajo el nombre de Estrategia Nacional de Seguridad Cibernética. Dicho documento reconoce que las TICs son una herramienta necesaria para el desarrollo nacional que conlleva riesgos que deben ser mitigados. La Estrategia identifica las siguientes áreas clave para lograr su objetivo: Medidas Técnicas; recursos humanos y desarrollo de capacidades; legal y regulatorio; y Educación y conciencia pública; que se desarrollan a través de 13 objetivos particulares. Además, la Estrategia agrega que busca generar confianza en el ciberespacio para que los jamaiquinos alcancen su máximo potencial. Busca ofrecer garantía de que se puede confiar en las tecnologías en las que depende diariamente, combatiendo los actos del cibercrimen contra las instituciones financieras, gubernamentales e infraestructura crítica.

De hecho, la Estrategia menciona que los costos por los delitos cibernéticos sobrepasan la suma del costo del tráfico de marihuana, cocaína y heroína. Lo anterior pone a la ciberseguridad como un tema prioritario dentro de la agenda de seguridad no sólo publica, sino nacional. Por ello, reconoce que el gobierno no puede solo con el desafío y acepta que la comunidad académica y el sector privado son actores fundamentales en la protección del ciberespacio. La Estrategia tiene los siguientes principios rectores: Liderazgo; Responsabilidades Compartidas; Protección de la Libertad y Derechos Fundamentales; la Gestión de Riesgos; Innovación y Desarrollo Empresarial; y Recursos Sostenibles.

Para cumplir los objetivos, cuenta con la Ley de Delitos Cibernéticos de 2010 que será actualizada y mejorada. En aspectos funcionales, la Estrategia complementa otras políticas y programas del gobierno jamaiquino como: La Estrategia Nacional de Tecnologías de la Información y Comunicaciones 2007-2012; Plan Nacional de Desarrollo 2030; La Política de Tecnologías de la Información y las Comunicaciones de 2011; y la Política de Seguridad Nacional de 2014.

En cuestión de organización y desempeño de las funciones de ciberseguridad han iniciado, con la asistencia de la Unión Internacional de Telecomunicaciones, los trabajos para la creación de un CSIRT nacional, así como la construcción y el despliegue de las capacidades técnicas necesarias. Ha establecido un Grupo de Trabajo Nacional de Seguridad Cibernética (NCSTF) que comprende una amplia transversalidad de partes interesadas de los sectores público, privado y academia. Además, cuenta con La Unidad de Comunicación Forense y Cibernética (CFCU) dentro de la Fuerza Policial de Jamaica (JCF) desde diciembre de 2010 y la Unidad de Delitos Cibernéticos y Evidencia Digital desde 2009. Queda claro que Jamaica cuenta con una organización incipiente pero numerosa de agencias de ciberseguridad. Establece tiempos de implementación de las primeras acciones y una revisión obligatoria de la Estrategia cada 3 años o cuando sea necesario.

Trinidad y Tobago

En el caso de Trinidad y Tobago, la ciberseguridad ha tenido un documento rector desde 2013. La Estrategia Nacional de Seguridad Cibernética reconoce que las actividades cotidianas son dependientes de las TICs., menciona que la realidad de este entorno trae consigo oportunidades, pero también riesgos a la seguridad. La estrategia se basa en el Marco de Política de Mediano Plazo 2011-2014 del Gobierno, en el que se destaca el papel de las TIC en la promoción del desarrollo; y tiene los objetivos:

1. Crear un entorno digital seguro que permita a todos los usuarios gozar plenamente de los beneficios que ofrece la Internet.
2. Proporcionar un marco de gobernanza en relación con todos los asuntos de seguridad cibernética mediante la identificación de las estructuras institucionales y administrativas necesarias, incluidas las de recursos humanos, capacitación y desarrollo de capacidades, y las relativas a las necesidades presupuestarias.
3. Proteger los activos físicos, virtuales e intelectuales de los ciudadanos, las instituciones y el Estado a través de la creación de un mecanismo eficaz para responder a las amenazas cibernéticas, sea cual fuere su origen.
4. Facilitar la seguridad de todos los ciudadanos promoviendo la sensibilización frente a los riesgos cibernéticos y elaborando medidas de protección eficaces y apropiadas para mitigar riesgos y ataques.

Y para lograr dichos objetivos se identificaron las cinco áreas de interés que se enlistan a continuación: Gobernanza; Gestión de Incidentes; Colaboración; Cultura; y Legislación. Que se verán sustentadas por treinta actividades. Todo con el objeto de crear un ciberentorno seguro y sólido, basado en la colaboración incondicional de todos los involucrados. A través de esta estrategia se pretende orientar todas las operaciones e iniciativas relacionadas con la ciberseguridad en el país. En ella se reconoce la necesidad prioritaria de un marco global de gobernanza, una apropiada legislación sobre delitos cibernéticos y el establecimiento de un equipo CSIRT. A lo anterior habría que sumarle la importancia de sensibilizar a todos los interesados generando una cultura de la ciberseguridad.

La Estrategia busca proteger el sistema financiero, servicios gubernamentales, los sistemas de control industrial tipo SCADA, la infraestructura de petróleo, gas y petroquímica, así como los servicios de transporte aéreo y terrestre. En la aplicación de la Estrategia se utilizará la Agencia de Seguridad Cibernética de Trinidad y Tobago (TTCSA, por sus siglas en inglés) como la principal responsable de la coordinación, la aplicación, el seguimiento, la mejora continua y la adecuada gestión de las iniciativas de seguridad cibernética. Además, el gobierno establecerá un CIRST como medio de protección de la infraestructura crítica. De manera complementaria, se promulgarán y aplicarán leyes generales de alcance nacional sobre delitos cibernéticos que sean aplicables y puedan armonizarse en el ámbito nacional e internacional.

Tabla 1. Resumen comparativo Estrategias Nacionales de Ciberseguridad

	Objetivo General	Objetivos Particulares	Estructura Orgánica	Recursos tecnológicos	Marco legal	Observaciones
Canadá 2018	√	√	√	√	√	Remasterizada y actualizada; es la más reciente.
EE.UU. Pendiente	√ Pendiente tener nueva ENCS	√ Pendiente tener nueva ENCS	√	√	√	No cuenta con una Estrategia Nacional de Ciberseguridad única. En el trabajo se utiliza la Ciberestrategia del DoD 2005. Bush presentó en 2003 la Estrategia Nacional para asegurar el Ciberespacio.
México 2017	√	√	√	√	√	Falta profundizar en los detalles de implementación, organización y funciones.
Colombia 2016	√	√	√	√	√	Incluye cronograma y detalles de financiamiento.
Costa Rica 2017	√	√	√	√	√	Incorpora medidas de educación, prevención y mitigación de riesgos. Se revisa cada 2 años.

Chile 2017	√	√	√	√	√	Detalla tareas de corto y mediano plazo, así como responsabilidades.
Panamá 2013	√	√	√	√	+ / -	No presenta de forma implícita los principios.
Paraguay 2017	√ Tiene varios	√	√	√	√	Presenta los principios orientadores.
Jamaica 2015	√	√	√	√	√	Señala que los costos de los delitos cibernéticos sobrepasan los del tráfico de drogas. Se revisa cada 3 años.
Trinidad y Tobago 2013	√	√	Por realizar	Por realizar	Por realizar	Reconoce medidas de marco global de gobernanza, la necesidad de un marco legal y la instalación de un CSIRT.

Elaboración propia. Con base en información publicada por los propios Estados.

Desafíos de las estrategias de ciberseguridad nacional

Si se parte de la definición de estrategia propuesta por Dolman (2005: 18) que dice que la estrategia es «plan para obtener la ventaja continua» entonces las Estrategias, planes o políticas de ciberseguridad que fueron enunciadas deberían estar orientadas a lograr, mantener o aumentar el poder (en este caso ciberpoder). Objetivo político que de acuerdo con Moisés Naím (2013: 47-49) se busca por medio de una mezcla de las cuatro formas distintas para ejercer el poder, también conocidas como tipos ideales o canales, que son: la fuerza, el código, el mensaje y la recompensa. Por lo tanto, bajo el supuesto de incrementar el poder en el ciberespacio solamente la Estrategia estadounidense parece cumplir con el cometido ya que expone que el ciberpoder es el elemento esencial para lograr la ventaja estratégica (DoD, 2005: vii). En contraste, la gran mayoría de las Estrategias Nacionales de Ciberseguridad lo que busca es fortalecer los instrumentos y las instituciones, aunque sin detallar de donde obtener los recursos ni definir funciones.

De la lectura de los documentos guía de las actividades de ciberseguridad se puede inferir que los desafíos que enfrentan las estrategias son diversos. Entre los problemas identificados se tienen aquellos referentes a la falta de una definición universal, la coordinación entre la iniciativa privada y el gobierno, la falta de un sistema educativo que cubra las necesidades de profesionales de la ciberseguridad, la adaptación de las fuerzas armadas y sus operaciones a los nuevos requisitos del

campo de batalla tecnológico, el incremento del impacto y frecuencia de los ciberataques, el desarrollo de tecnología endógena, el diseño de un sistema jurídico eficiente y alineado con los objetivos nacionales, las capacidades para ejercer influencia por medio del ciberpoder, el número de dispositivos conectados a la red, y la falta de tratados internacionales que regulen el cibercrimen, la ciberguerra y sus asuntos relacionados. Entre los desafíos destaca la construcción de confianza entre Estados al mismo tiempo que se contrarrestan amenazas provenientes de actores antagónicos; es decir, como confiar en quien busca dominar a través del ciberpoder.

Simplificando, los desafíos a las diversas estrategias de ciberseguridad pueden ser catalogados como técnicos, administrativos, organizacionales y de recursos humanos. Por lo tanto, en este trabajo solamente se mencionarán algunos de los muchos desafíos que se deslindan de estas categorías. Dentro de los desafíos técnicos se mencionará la dependencia tecnológica, en el plano organizacional la necesidad de contar con un organigrama vertical que centralice las misiones de ciberseguridad para mejorar la cooperación y reacción interinstitucional e internacional, y en cuestión de recursos humanos la falta de profesionales tanto técnicos como estratégicos que asuman las riendas del sistema de ciberseguridad con flexibilidad, conocimiento, ética y una estrategia. Los riesgos o desafíos que enfrentan los Estados en materia de ciberseguridad surgen de las características del ciberespacio que permiten mayor rentabilidad, facilidad de acceso e impunidad.

Primero, el principal desafío tecnológico de la mayoría de las estrategias de ciberseguridad es que los Estados no generan la totalidad de los componentes de los sistemas de cómputo y comunicaciones con los que construyen sus sistemas cibernéticos. Por ejemplo, de acuerdo con Adee (2008) existe una centralización de la producción de componentes esenciales como son los procesadores, ya que Taiwán produce 80 por ciento de los arreglos de compuertas de campo programable (FPGA por sus siglas en inglés) que son circuitos integrados genéricos que pueden ser personalizados por medio de programas de computadora abaratando los costos de manera importante cuando se compara con los circuitos integrados de aplicación especifica (ASIC). El costo baja desde un máximo de entre $4 a $50 millones a tan sólo $500 dólares.

Lo anterior pone en riesgo la seguridad nacional de EE.UU., y de todos aquellos que compren dichos dispositivos, debido a que muchos de sus contratistas de defensa son dependientes de dichos circuitos. Sin embargo, aunque el precio no se relaciona generalmente con la seguridad, en este caso no existe garantía de que estos circuitos integrados de bajo precio no hayan sido modificados para contar con un circuito de apagado o una «puerta trasera» que permita la manipulación remota del sistema en el que se monten dichos circuitos. Para generar este tipo de vulnerabilidades basta con agregar 1000 transistores adicionales en una configuración especial que permitirá su acción cuando le sea instruido por un agente externo (Adee, 2008).

El desafío es contar con una cadena de suministro de dispositivos y componentes de las TIC confiable y eficiente. Al respecto el Deparment of Defense (DoD) estadounidense en 2004 «creó el Programa de Fundiciones de Confianza para tratar de garantizar un suministro ininterrumpido de circuitos integrados seguros para el gobierno. Los inspectores del DoD ahora han certificado ciertas plantas de circuitos

comerciales como fundiciones confiables, tal es el caso de las instalaciones de IBM Burlingtony Vt.» (Adee, 2008). De igual manera, Libicki (2009: 22) ha denunciado que «A muchos en la comunidad de defensa les preocupa la creciente presencia de China en la fabricación de componentes situación que le brinda muchas oportunidades para hacer travesuras, y puede que no sea tímida a la hora de tomar ventaja de dichas oportunidades». Esto sin olvidar que «Ni los agentes ni los componentes modificados/corruptos violan los principios básicos discutidos anteriormente. Ninguno representa un acceso forzado. Ambas son formas de engaño y del tipo que una vez engañado no permite que caiga tan fácilmente otra vez» (Libicki, 2009: 21) Esto lleva al problema de la atribución que evita identificar positivamente a los atacantes y organizar una respuesta proporcional al ataque.

Aunado a lo anterior habría que sumar la complejidad, cantidad y efectividad de los ciberataques, que han convertido las operaciones militares en acciones tipo guerrilla o guerra asimétrica. Cada año se tiene noticia de ciberataques de gran impacto a las áreas estratégicas de los Estados, quienes debido a la diversidad, atomización y automatización de los actores se ha visto imposibilitado para dar respuesta efectiva. En este caso la mejor defensa es la prevención y mitigación de riesgos, pero sin la tecnología adecuada y eficiente esto es una misión casi imposible.

En breve, el mayor desafío tecnológico consiste en generar tecnología endógena con dispositivos seguros y confiables. No depender de tecnologías extranjeras brinda un alto grado de libertad de acción. El pensamiento estratégico dicta que se deben tomar las medidas necesarias para evitar la coerción de cualquier índole y reducir los riesgos de un ataque por sorpresa.

Segundo, en lo relativo a los problemas y desafíos tanto administrativos como organizacionales se puede ver que la falta de recursos y estrategias detalladas entorpece la buena voluntad de algunos gobiernos y actores de la sociedad civil. Particularmente los desafíos surgen de la no consideración de la ciberseguridad como un tema prioritario dentro de la agenda nacional de riesgos u otro documento similar y a la falta de un organismo central que organice y controle las actividades en materia de ciberseguridad nacional. Bajo el contexto actual en primer término se debe convencer a los dirigentes políticos sobre la seriedad y el alcance de los eventos cibernéticos adversos que podrían poner en jaque las actividades económicas, políticas, sociales y militares.

Todo lo cual sería un atentado contra la estabilidad, integridad y permanencia del Estado. Es decir, la ciberseguridad nacional debe ser considerada como una parte complementaria de la seguridad nacional dentro de la legislación vigente para que se asignen los recursos necesarios para fortalecer tanto la infraestructura digital como la educación/cultura en ciberseguridad. Los fondos asignados a la ciberseguridad nacional deben ser vistos como una inversión que garantiza la continuidad de las actividades diarias en el ciberespacio.

Una vez que la administración en turno comprenda la importancia de contar con un ciberespacio seguro y resiliente, identifique los sectores estratégicos de su infraestructura digital o ciberentorno, reconozca las amenazas que enfrenta y cuente con un diagnóstico situacional, podrá estructurar un sistema de ciberseguridad centralizado y vertical. Tendrá la obligación de estructurar un sistema de ciberseguridad

nacional compuesto por: 1) un sistema de ciberseguridad pública y 2) las fuerzas de ciberdefensa con atribuciones, obligaciones y prerrogativas estipuladas de manera clara y detallada.

Diagrama 1. Propuesta de un Sistema de Ciberseguridad Nacional

Elaboración propia. Propuesta de la orgánica de ciberseguridad y ciberdefensa. Aclarando que esta estructura no exime la participación de los diversos componentes en apoyo del resto o en operaciones conjuntas.

Sistema en el cual se define a la policía como el elemento bisagra o de enlace entre la ciberseguridad y la ciberdefensa. No se puede permitir que exista confusión en el papel que cada uno de los órganos que integren dicho sistema de ciberseguridad nacional deben cumplir, la política que deben seguir, los objetivos que deben alcanzar, la estrategia que deben adoptar, los instrumentos legales que puede requerir, las acciones que deben iniciar ni en el perfil de profesionistas que requieren. Todo lo cual representa una revolución en asuntos de ciberseguridad y un desafío a los gobiernos de algunos Estados de América Latina y el Caribe.

Tercero, al mismo tiempo que diseña la estructura orgánica que adoptará el sistema de ciberseguridad nacional, debe iniciar con un plan emergente de formación de cuadros profesionales en ciberseguridad. Particularmente porque la falta de una fuerza de trabajo profesional con especialización en temas de ciberseguridad atenta contra la seguridad de los sistemas informáticos, de la infraestructura crítica y de la información el «oro digital» de la sociedad de la información. De acuerdo con Arreola (2015: 160-163) la experiencia en la selección y reclutamiento de personal para el sistema de inteligencia ha dado como resultado requisitos morales, psicológicos, físicos e intelectuales que deben ser satisfechos para tener acceso a información estratégica o conocimiento privilegiado. Este tipo de reclutamiento puede ser emulado por el sistema de ciberseguridad. Por desgracia, a pesar de todas las medidas de selección de personal, las instituciones de ciberseguridad no pueden garantizar que los profesionales de la ciberseguridad no se vean tentados a cometer actos que pongan en riesgo la ciberseguridad nacional, las actividades de los organismos o la privacidad de los individuos.

Por ello, es recomendable contar con un sistema educativo que brinde una formación integral, que incluya aspectos de desarrollo físico, mental y ético entremezclados con los temas de uso seguro de las TIC. De manera ideal, la formación de cuadros para la ciberseguridad debería ser en instituciones creadas exprofeso para el caso, en donde se haga hincapié en los beneficios de servir por convicción en aras del bienestar público. A lo anterior, habría que sumar un sistema de evaluación y seguimiento del desempeño de cada uno de los elementos para detectar anomalías en su conducta, vida personal y desarrollo profesional que pudieran convertirse en una amenaza para la seguridad del sistema de ciberseguridad.

Sin embargo, se sabe que las necesidades de cuadros profesionales se cubren por medio de la subcontratación de servicios, lo que se vuelve una fuente de potencial riesgo para el sistema. Por lo tanto, se deben establecer lineamientos estrictos para la contratación de terceros dentro del sistema de ciberseguridad con el fin de garantizar la seguridad de las operaciones y la ciberseguridad nacional. Según Arreola (2015: 160-163) el dilema de este tipo de contratación es que el proceso de selección lo realizan las propias compañías subcontratadas y no se puede garantizar que hay sido tan riguroso como las actividades de ciberseguridad lo requieren, al menos en cuestiones de valores morales como son: discreción, honestidad y lealtad. En consecuencia, no solamente se deben firmar acuerdos de confidencialidad, sino que es prioritario fortalecer el sistema legal para regular eficientemente la actuación de los prestadores de servicio en materia de ciberseguridad. De no hacerlo así se corre el riesgo de que áreas estratégicas para la seguridad nacional queden expuestas desde dentro a los embates de potenciales enemigos.

En resumen, de manera general los desafíos de las Estrategias Nacionales de Ciberseguridad son aquellos que se refieren: al fortalecimiento de la infraestructura y medios técnicos de manera personalizada y autónoma; a la creación, mantenimiento y fortalecimiento de un aparato estatal que garantice la ciberseguridad nacional al mismo tiempo que respeta los derechos humanos, privacidad e intimidad de sus ciudadanos; a la implementación de una cultura de la ciberseguridad que permee todos los niveles y sectores enfocándose en el fortalecimiento del eslabón más débil (el ser humano); y finalmente, a la conformación de un sistema educativo que genere los recursos humanos profesionales necesarios para organizar una fuerza de reacción capaz de tomar la iniciativa cuando sea necesario. Todo lo anterior sin olvidar que el internet se ha convertido en un bien común que por el momento aparenta estar bajo el control de nadie y de todos, convirtiendo la gobernanza del internet en un tema de cooperación y seguridad internacional.

En lo que respecta a ciberespacio este por sí mismo conlleva una serie de desafíos que están implícitos en su esencia y estructura. Estos desafíos se refieren a cuestiones de alcance (global), la velocidad para realizar un ataque o contraataque (nanosegundos), la dificultad para identificar de manera precisa al atacante (atribución), hace patente el ciberpoder y la posibilidad de realizar tanto operaciones ofensivas como defensivas (se dice que la ofensiva es dominante). Garantizar el ciberespacio global requerirá la cooperación internacional para crear conciencia, compartir información, promover estándares de seguridad e investigar y enjuiciar los delitos cibernéticos. Por ello, quién domine el ciberespacio, dominará al mundo.

Siguiendo el pensamiento estratégico de Sun Tzu (2008: 21), una estrategia nacional de ciberseguridad o ciberestrategia no garantiza que todos los ataques puedan ser contrarrestados, pero sin un documento guía puede asegurarse que los ataques contra su integridad serán exitosos y lo dañarán seriamente. Se debe recordar que la invencibilidad radica en uno mismo, por lo que la fortaleza propia radica en una defensa efectiva; y las posibilidades de vencer se encuentran en el ataque que explota las debilidades del oponente.

Conclusiones

La mayoría de las estrategias revisadas requieren de mayor trabajo para detallar las acciones concretas que realizarán para alcanzar los objetivos, conocer las necesidades de presupuesto y designar las instituciones que serán las encargadas de implementarlas. Se debe reconocer que la Estrategia de EE.UU., Canadá, Colombia, Paraguay y Chile son las que presentan un mayor grado de detalle. Por ejemplo, la Estrategia estadounidense describe la ciberestrategia militar de su gran estrategia, la Estrategia colombiana fue revisada para adoptar una segunda versión que incluye un cronograma para la consecución de los objetivos y la Estrategia Chilena plasma objetivos a mediano plazo que debe obtenerse para el 2022.

En contraste, la Estrategia de Panamá queda por debajo del promedio y aparenta ser más un compromiso político que un documento rector de la ciberseguridad nacional. A pesar de ello, se debe reconocer que Panamá fue el segundo Estado en adoptar una Estrategia Nacional de Ciberseguridad (2013), solamente detrás de Colombia que fue el primer Estado latinoamericano en contar con un documento rector de la ciberseguridad.

Es previsible que el diseño de estrategias nacionales de ciberseguridad traerá consigo un sentimiento de inseguridad para quienes no cuenten con ella; en consecuencia, el dilema de la seguridad seguirá predominando en el continente americano y en el mundo. De manera clara, la seguridad de uno es la inseguridad del resto. Esto será cierto particularmente para aquellos Estados en donde la tecnología se ha convertido en elemento esencial de las actividades cotidianas de la sociedad, organizaciones y gobierno.

No se puede pasar por alto que las estrategias nacionales de ciberseguridad están orientadas a proteger el ciberespacio que según Arreola (2016) se ha convertido en el campo de batalla de la era tecnológica. Sin lugar a dudas, la superioridad en el ciberespacio brindará la libertad de acción a las fuerzas amigas y la negará al enemigo. Lo que se busca a través de las estrategias de ciberseguridad nacional es la obtención, manutención e incremento del ciberpoder.

Una de las preocupaciones principales de las estrategias de ciberseguridad nacional debe ser la creación de centros educativos de excelencia en cuestiones ciencia y tecnología con un enfoque en todas las aristas de la ciberseguridad. Es decir, la formación de los nuevos profesionales de todas las áreas debe incluir conocimientos de ciberseguridad, esto facilitaría que las empresas y gobierno desempeñen sus funciones utilizando tanto el ciberespacio como las tecnologías de la información y comunicación de manera segura, innovadora y eficaz.

La ciberseguridad del conjunto es igual a la seguridad de su eslabón más débil. Ya que todos los elementos de la sociedad están expuestos y pueden convertirse en la principal vulnerabilidad, los gobiernos deben corregir las asimetrías que existen en el trato prioritario que se da a la ciberseguridad. Lo anterior se puede lograr por medio del asesoramiento, liderazgo, y ampliación del acceso a herramientas de ciberseguridad/seguridad de la información, así como del desarrollo de habilidades especializadas. El gobierno se convierte en el líder de la empresa llamada ciberseguridad nacional que requiere de un enfoque conjunto, multidisciplinario, multifactorial y multinivel para lograrse. La ciberseguridad nacional es un asunto de todos.

Como dicen Clarke y Knake (2014: 21) «la ciberguerra es real, la ciberguerra se desarrolla a la velocidad de la luz, la ciberguerra es global, la ciberguerra evita el campo de batalla y, la ciberguerra ha iniciado». Por ello, un buen inicio es contar con una Estrategia Nacional de Ciberseguridad que atienda de manera integral los pormenores del ciberespacio. No hay debe perder de vista que los ciberataques dependen del engaño para persuadir a los sistemas para hacer lo que los diseñadores originales no quieren que hagan.

La esencia de la ciberseguridad nacional radica en la protección de los equipos e infraestructura. Es prioritario para la estrategia que se garantice un diseño seguro de los componentes internos y accesorios de los diversos sistemas digitales. Para ello, tendría que crearse un área especialmente dedicada a la prueba funcional de los diversos dispositivos y componentes electrónicos con que cuentan las áreas estratégicas para la seguridad y el desarrollo. Remarcando que cualquier daño o pequeña modificación maliciosa puede ser devastadora para el sistema en su totalidad. Garantizar el ciberespacio global requerirá la cooperación internacional para crear conciencia, compartir información, promover estándares de seguridad e investigar y enjuiciar el delito cibernético. No se puede olvidar lo que John Boyd, coronel de la Fuerza Aérea de Estados Unidos, argumentó que «las máquinas no combaten guerras ... los humanos pelean guerras». (Coram, 2002: 341), porque es algo que esta en proceso de cambio.

Para hacer frente a los desafíos de la era de la información el hombre tendrá que diseñar e implementar estrategias integrales que tengan como epicentro la seguridad humana.

Bibliografía

- Adee, S. (2008). The hunt for the kill switch. *iEEE SpECtrum*, *45*(5), 32.
- Arreola, G.A. (2015). *Ciberespionaje, la puerta al mundo virtual de Estados e individuos*. Siglo XXI.
- Arreola, G. A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa*, *11*(22), 109-138.
- Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia*, (149), 165-214.
- Banco Interamericanos de Desarrollo (BID) y Organización de los Estados Americanos (OEA) (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/
- Betz, D. J. and Stevens, T. (2011). *Cyberspace and the State: Towards a Strategy for Cyber-power.* Routledge.
- Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *SI*STEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS), 119, 4-7.
- Carter, A. (2015). The DOD cyber strategy. April, 17, 2015.
- Clarke, R. A., & Knake, R. K. (2014). Cyber war. Tantor Media, Incorporated.
- Clausewitz, C. (1976). On War, Edited and translated by Michael Howard and Peter Paret, Princeton: Princeton University Press.
- Consejo Nacional para la Innovación Gubernamental (12 de marzo de 2013). Gaceta Oficial Digital. Nº 21. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Recuperado el 11 de agosto de 2018, de https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf
- Coram, R. (2002). Boyd: The fighter pilot who changed the art of war. Hachette UK. pp. 341.
- Department of Defense (DoD). (11 de diciembre de 2005). The National Military Strategy for Cyber Operations. www.hsdl.org [Edición digital]. Recuperado el 06 de Agosto de 2018 de, https://www.hsdl.org/?abstract&did=35693
- Department of Defense (DoD). (2015). The DoD Cyber Strategy. EUA: DoD. www.defense.gov [Edición digital]. Recuperado el 06 de Agosto de 2018 de, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- Department of Public Safety and Emergency Preparadness. (2018). National Cybersecurity Strategy. www.publicsafety.gc.ca [Edición digital]. Recuperado el 12 de agosto de 2018 de, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- Documento CONPES 3854 (Consejo Nacional de Política Social y Económica). (2016). Política Nacional de Seguridad Digital. Recuperado el 10 de agosto de 2018, de http://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%C2%A1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y
- Dolman, E. (2005). Pure Strategy: Power and Principle in the Space and Information Age. Routledge.
- Gobierno de Chile (2017). Política Nacional de Ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf
- Gobierno de Jamaica. (2015). Estrategia Nacional de Seguridad Cibernética. www.sites.oas.org

[Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.sites.oas.org/cyber/Documents/Jamaica%20National%20Cyber%20Security%20Strategy%20(Spanish).pdf

- Gobierno de la República de Trinidad y Tobago. (2013). Estrategia Nacional de Seguridad Cibernética. www.sites.oas.org [Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(Spanish).pdf
- Gobierno de México. (2018). Por un internet más seguro en México: impulsa Gobierno de la República Estrategia Nacional de Ciberseguridad. www.gob.mx [Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.gob.mx/mexicodigital/articulos/por-un-internet-mas-seguro-en-mexico-impulsa-gobierno-de-la-republica-estrategia-nacional-de-ciberseguridad
- Gobierno de México. (2018). Por un internet más seguro en México: impulsa Gobierno de la República Estrategia Nacional de Ciberseguridad. www.gob.mx [Edición digital]. Recuperado el 15 de agosto de 2018, de https://www.gob.mx/mexicodigital/articulos/por-un-internet-mas-seguro-en-mexico-impulsa-gobierno-de-la-republica-estrategia-nacional-de-ciberseguridad
- House, W. (2003). The national strategy to secure cyberspace. Washington, DC: White House.
- Johnson, D. D., & Tierney, D. (2011). The Rubicon theory of war: how the path to conflict reaches the point of no return. International Security, 36(1), 7-40.
- Kuehl, T. D. (2009). Cyberspace and Cyberpower, in Cyberpower and National Security, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009).
- Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.
- Libicki, M. C. (2007). Conquest in cyberspace: national security and information warfare. Cambridge University Press.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. Rand Corporation.
- Lynn, W. J. (2010). Defending a new domain: the Pentagon's cyberstrategy. Foreign Affairs, 89(5), 97-108.
- Max Weber, 'Class, Status, Party', in Hans Gerth and C. Wright Mills (eds). (1948). From Max Weber: Essays in Sociology. London: Routledge and Kegan Paul, p. 180.
- MICITT (2017). Estrategia Nacional de Ciberseguridad de Costa Rica. Recuperado el 15 de agosto de 2018, de https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf
- Naím, M. (2013). El fin del poder: Empresas que se hunden, militares derrotados, papas que renuncian, y gobiernos impotentes: cómo el poder ya no es lo que era. Debate.
- Observatorio CISDE (2017). Pronóstico de ciberseguridad para América Latina en 2018. Recuperado de https://observatorio.cisde.es/sin-categoria/pronostico-ciberseguridad-america-latina-2018/
- Organización de Estados Americanos (OEA). (2017). México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA. www.oas.org [Edición digital]. Recuperado el 15 de agosto de 2018, de http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17
- Russell, B. (2004). Power: A new social analysis. Routledge. p. 23.
- Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional

de Ciberseguridad. Retos, roles y compromisos. Recuperado el 12 de agosto de 2018, de http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

- Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional de Ciberseguridad. Retos, roles y compromisos. Recuperado de: http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg
- Sheldon, J. B. (2011). Deciphering cyberpower: Strategic purpose in peace and war. Strategic Studies Quarterly, 5(2), 95-112.
- Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. American Foreign Policy Interests, 36(5), 286-293.
- Starks, T. (12 de abril de 2018). A national cyber strategy may finally be on the way. www.politico.com [Edición digital]. Recuperado el 14 de agosto de 2018 de, https://www.politico.com/newsletters/morning-cybersecurity/2018/04/12/a-national-cyber-strategy-may-finally-be-on-the-way-167541
- Stephens, P. (16 de diciembre de 2010). On the way to a new global balance. Financial Times (Londres).
- Torres, M. (2013). Ciberguerra. En Jordán, J. (coord.), Manual de Estudios Estratégicos y Seguridad Internacional. pp. 329-348. Madrid: Plaza & Valdés.
- U.S. Department of Defense (DoD). The Department of Defense Cyberstrategy. www.defense.gov [Edición digital]. Recuperado el 14 de agosto de 2018 de, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/
- 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). (2017). Índice Global de Ciberseguridad 2017. www.itu.int [Edición digital]. Recuperado el 15 de agosto de 2017 de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf