Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Revista de Administración Pública

INAP

Atlas de riesgos para la Seguridad Nacional Cibernética en México

Carlos Estrada Nava

Resumen: La Seguridad Nacional Cibernética es una "zona híbrida" entre conocimientos de ingeniería de programación, así como de actualidad de los temas de geopolítica mundial. Adicionalmente, existe una simbiosis entre Seguridad Cibernética y el Cómputo Forense, el cual se encarga de obtener y procesar evidencias digitales sobre incidentes informáticos. En México para abordar el campo de la "Seguridad Nacional Cibernética", la Secretaría de la Defensa Nacional recientemente creó el primer Comando Cibernético. Nuestro aporte consiste en la elaboración del primer Atlas Nacional de Riesgos Cibernéticos, los cuales pueden ser mitigados por ISO 2700, así como medidas concretas de este documento.

Palabras clave: Seguridad Nacional Cibernética, Infraestructuras Críticas, BlockChain.

Atlas of risks for National Cyber Security in Mexico

Abstract: National Cyber Security is a "hybrid zone" among programming engineering knowledge, as well as topical issues of global geopolitics. Additionally, there is a symbiosis between Cyber Security and Forensic Computing, which is responsible for obtaining and processing digital

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

evidence on computer incidents. In Mexico to address the field of "National Cyber Security", the Ministry of National Defense recently created the first Cyber Command. Our contribution consists in the elaboration of the first National Atlas of Cyber Risks, which can be mitigated by ISO 2700, as well as concrete measures of this document.

Keywords: National Cyber Security, Critical Infrastructures, BlockChain.

Fecha de recepción: 22 de mayo de 2019
Fecha de aceptación: 7 de junio de 2019

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Revista de Administración Pública

INAP

Atlas de riesgos para la Seguridad Nacional Cibernética en México

Carlos Estrada Nava*

Introducción

Si bien el año de 2018 ha sido el peor en ataques cibernéticos en México, con pérdidas en gobierno y empresas por más de 1,200 millones de pesos, en 2019 y el porvenir de la tendencia prevista incluye más riesgos, debido a que no se han corregido ninguno de los 5 principales problemas estructurales del país.

Aunado a ello, el tema de la Seguridad Nacional Cibernética en México se encuentra en estado embrionario debido a que se trata de un campo híbrido, y el mayor riesgo actualmente lo constituyen posibles ataques a las Infraestructuras Críticas del país, como lo es la red eléctrica nacional, misma que ya ha tenido fallas masivas durante 2019.

* Licenciatura en Ciencias Políticas y Administración Pública por la Facultad de Ciencias Políticas y Sociales de la UNAM. Master in Business Administration (MBA) por University of Phoenix, Arizona, USA. Estudios de Ingeniería en Desarrollo de Software. Técnico en Computación profesional, y perito privado ante Ministerio Público de la Procuraduría General de Justicia de la Ciudad de México. Consultor de análisis de datos, cómputo forense y seguridad cibernética en corporaciones mexicanas y americanas de seguridad e inteligencia como: Kroll Inc., Ernst & Young (EY), así como FTI Consulting. Actualmente socio de firma privada Vestiga Consultores, al servicio de Gobierno, Bancos, Minería, Construcción y otras industrias. Ha impartido conferencias de tecnología en los congresos internacionales de la Asociación Mexicana de Ciencias Políticas (AMECIP), y participado en la materia de Seguridad Nacional en Universidad Anáhuac.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Primeramente, resulta indispensable comprender los desarrollos tecnológicos que, día a día, crean nuevas amenazas digitales, más porque en los últimos 5 años existe una explosión en el desarrollo de códigos de programación, debido al crecimiento exponencial del *Open Source* (programas de código abierto), ya que las plataformas de *Big Data* y *Machine Learning* se basan fundamentalmente en código abierto.

Además, se requiere una comprensión de la lógica geopolítica, así como de relaciones internacionales, bajo la cual operan muchos de estos desarrollos, ya sea para atacar o defender la infraestructura de los países y sus empresas.

En nuestro caso en particular, tenemos el objetivo de desarrollar un primer "Atlas Nacional de Riesgos Cibernéticos" de la República Mexicana, lo cual implica analizar riesgos potenciales en contra de las instalaciones estratégicas públicas y privadas, como pueden ser: plantas eléctricas, gasoductos, transporte público, hospitales, escuelas, entre otras.

Asimismo, para poder analizar, diagnosticar y anticipar eventos de Seguridad Cibernética, resulta indispensable emplear elementos técnicos básicos de su disciplina hermana, el Cómputo Forense.

Sobre la actualidad de la Seguridad Cibernética

Junto con la democratización de las tecnologías de la información, debido a la posibilidad de su acceso para cada vez mayores sectores de la población mundial, también se generalizó el acceso global a Internet, convirtiéndose esta red en una plataforma donde por primera vez pueden interactuar por igual Gobiernos, Organizaciones públicas y privadas, así como los individuos en lo particular.

Esta apertura y universalización de las tecnologías multiplicó a su vez los riesgos y vulnerabilidades de los usuarios de las mismas, al tratarse muchas veces de entornos no regulados. Si bien los errores de programación o de hardware, así como los virus informáticos han existido desde el origen de la computación, en el inicio del siglo XXI, a nivel empresas se ha consolidado una industria conocida como "Crimeware", pero a nivel gobierno los ataques

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

cibernéticos se enmarcan en las llamadas "guerras de cuarta generación", caracterizadas por usar herramientas no convencionales y ocultas, para atacar por sorpresa al enemigo, siendo que se le desestabiliza al grado de poder derrotarlo.

Primeramente, la Seguridad de la Información se encuentra enfocada hacia los procesos y prácticas organizacionales para proteger el entorno de una empresa; este concepto se consolidó en octubre de 2005 por la *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*, quienes aprobaron y publicaron como estándar internacional de seguridad de la información la serie ISO 27000, siguiendo el modelo de la serie ISO 9000, comenzando con el ISO/IEC 27001:2005 (Calder, 2009, p. 29).

A diferencia de esta noción de "Seguridad de la Información", la "Seguridad Cibernética" engloba todos aquellos elementos que pudieran representar un riesgo para la integridad digital de alguna entidad en específico, como pueden ser: ataques de fuerza bruta contra claves de correos electrónicos, ingeniería social con *phishing*, distribución de malware que solicita el pago de un rescate por archivos encriptados, intervención de dispositivos móviles o líneas telefónicas, así como hackeo en general de equipos de cómputo.

En cuanto al desarrollo conceptual del término "Seguridad Cibernética", Tim Stevens (2015, p. 11) desarrolla 3 diferentes planos: a nivel ontológico, su definición posee una connotación de buscar una condición de liberación ante la "inseguridad cibernética", esto es, evitar los riesgos y amenazas propias de la proliferación de las tecnologías de la información, de las cuales dependen nuestras sociedades actuales; en su lado procedimental, la Seguridad Cibernética implica abarcar un rango de prácticas tecnológicas y políticas, desde lo defensivo y proteccionista, hasta lo ofensivo y subversivo; finalmente, la Seguridad Cibernética constituye un medio no sólo de protección y defensa de la sociedad y sus infraestructuras de información, sino también un medio para perseguir políticas nacionales e internacionales mediante instrumentos informáticos-tecnológicos.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Debe ponerse especial atención en que a partir de los recientes 5 años se han disparado los ataques cibernéticos en todo el mundo, impulsados por diferentes procesos paralelos:

1. La explosión y consolidación del *Open Source* frente a Software por licencia, orillando a empresas tradicionales a abrir sus códigos, como Microsoft con Azure o Apple con Swift; debido a que los desarrolladores prefieren programas libres (gratuitos), con la consecuencia de que se descuidan las vulnerabilidades del código (por ejemplo, hay más *hackeos* en celulares con código abierto de Android, pero muy pocos en el código privado de iOS del iPhone)
2. El auge del *Big Data* y el nuevo *Machine Learning* (basados fundamentalmente en Open Source), aumentando el poder analítico y de procesamiento, lo cual también eleva la sofisticación de los ataques digitales
3. Irrupción de las *Crypto Currencies*, basadas en la tecnología *BlockChain*, las cuales impiden rastrear el destino final de las transacciones, promoviendo con ello los delitos cibernéticos

Ante esta nueva actualidad de la Seguridad Cibernética en el mundo, han surgido nuevos enfoques que ayudan a organizaciones públicas y privadas a lograr la ahora llamada "Resiliencia Cibernética", esto es, la capacidad de una entidad para prevenir, anticipar, responder, recuperarse e incluso contraatacar ante un incidente cibernético, y así evitar con ello que se ponga en riesgo la continuidad de su operación.

De las opciones para evaluar la Resiliencia Cibernética de una organización, se encuentran las pruebas de penetración (*pentesting*), mismas que pueden incluir: *denial of Service* (DoS), *out-of-band attacks*, *applications security testing*, *wireless networks analysis*, *mapping* and OS *fingerprinting*, *vulnerability scanning/analysis* (*Spoofing*, *Network sniffing*, *Trojan*, *Brute force attack*, etcétera), entre otros.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Cómputo forense como complemento de la seguridad cibernética en general

En la última década del siglo XX, a nivel global, la industria de la computación vivió un periodo de consumo masivo de equipos de cómputo personales y para nivel corporativo, esto debido fundamentalmente al empaquetamiento de diferentes ambientes de trabajo, como lo han sido los sistemas operativos de Windows, Apple o de código abierto como Linux.

El uso cada vez más generalizado de estas tecnologías, derivó en la necesidad de obtener evidencias informáticas para poder apoyar procesos legales, todo ello en la disciplina de las ingenierías de sistemas, bajo el paraguas del llamado Cómputo Forense. Bajo este campo teórico y práctico, es posible obtener, documentar, procesar y presentar, de manera científica, toda aquella evidencia obtenida de equipos de cómputo, susceptible para usarse en peritajes y dictámenes informáticos.

La rama del Cómputo Forense tiene una naturaleza intrínsecamente científica, debido a que las evidencias recabadas son susceptibles de replicarse, obteniendo en todos y cada uno de los casos los mismos resultados, debido al carácter digital de sus elementos. Adicionalmente, este proceso puede auditarse por un tercer actor interesado, aplicando los métodos de comprobación necesarios, tras lo cual obtendría los mismos resultados del reporte forense original. De esta manera, es posible documentar con Cadenas de Custodia, evidencias forenses de equipos de cómputo en general (escritorio, laptops, servidores), así como realizar análisis forense de redes, datos y dispositivos móviles.

Entre las capacidades básicas de Cómputo Forense podemos encontrar la recuperación profunda de información borrada, análisis del código de archivos, registros de sistema operativo, historiales de navegación por Internet, contenido y encabezados de correos electrónicos, dispositivos móviles, redes de trabajo, entornos de *Cloud*, bases de datos, así como expresiones regulares en el universo de datos en particular, entre otras.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Infraestructuras críticas como nuevo teatro de operaciones de la Seguridad Nacional

Desde nuestra práctica profesional, actualmente nos encontramos en el desarrollo de un primer "Atlas Nacional de Riesgos Cibernéticos" de México. A nivel mundial, países líderes de estas iniciativas han sido Singapur, China, India, Inglaterra, Israel y Estados Unidos. En los países referidos, se definen legislaciones y políticas públicas nacionales sobre seguridad cibernética, las cuales incluyen un análisis generalizado sobre los riesgos potenciales que enfrentan sus instalaciones estratégicas públicas y privadas, como lo son: plantas eléctricas, gasoductos, transporte, hospitales, escuelas, etcétera.

Siendo el Departamento Militar de Innovación Tecnológica de Estados Unidos (DARPA o Defense Advanced Research Projects Agency), el creador del Internet, en aquel país desde hace cuando menos 3 décadas, se ha considerado a la Seguridad Cibernética como uno de los más urgentes problemas que deben enfrentar los gobiernos y las organizaciones públicas y privadas. Como parte del debate legislativo estadounidense, a la "Seguridad Nacional Cibernética" se le considera como el grupo de actividades estratégicas relacionadas con los "sistemas de información electrónicos", conocidos también como "infraestructuras de información", sobre todo aquellas que implican una amplia gama de activos económicos y de seguridad para los sectores públicos y privados (John Rollins, 2009).

Debe mencionarse que dentro del "teatro de operaciones cibernético", para el Pentágono americano, un ataque digital equivale a un ataque físico, por lo cual todo ciberataque requiere una respuesta, ya sea digital o física.

En este documento, se considera el término "teatro de operaciones" o "teatro de guerra", bajo el concepto de "área de operaciones", usado en el diccionario militar del Departamento de la Defensa americano y la OTAN (Organización del Tratado del Atlántico Norte), entendido como "la porción de un área de guerra necesaria para las operaciones militares y para la administraciones de tales operaciones" (Departamento de la Defensa, 1987, p.34).

De esta manera, como fue expuesto anteriormente, los ataques cibernéticos se enmarcan en las llamadas

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

"guerras de cuarta generación", caracterizadas por usar herramientas no convencionales y ocultas, para atacar por sorpresa al enemigo, siendo que se le desestabiliza al grado de poder derrotarlo. La diferencia a comparación de las guerras anteriores, consiste en que el nuevo "teatro de operaciones cibernético" se lleva a toda la extensión del Internet.

El mayor ejemplo de ello a la fecha, y que se considera la primer arma cibernética, fue el desarrollo del malware "Stuxnet", por parte de Estados Unidos, con el apoyo de la Unidad 8200 de Israel, símil de la NSA (National Security Agency) americana, con el objetivo de atacar los procesadores Siemens de las centrales nucleares de Irán, logrando detener por más de 10 años que alcanzaran la capacidad de enriquecer uranio.

No obstante, esta caja de Pandora se ha extendido hasta la aparición de "filtradores" (*leakers*) que obtienen estas herramientas cibernéticas y las publican o venden abiertamente, como ha sido el caso de "ShadowBrokers" y el grupo "Lazarus", quienes han estado detrás del ataque de bancos y organizaciones mexicanas, incluyendo a la Bolsa Mexicana de Valores. A nivel global, también desarrollaron el *ransomware* famoso llamado "WannaCry", que infectó cientos de miles de computadoras de más de 100 países; este malware usaba sólo 2 herramientas "zero-day" (desconocidas para el público al momento de su ataque) por parte de la NSA, pero desarrollos más recientes como "EternalRocks", usan hasta 7 zero-days.

El impacto de los ataques cibernéticos no ha sido sólo contra la infraestructura o sistemas financieros de los países, porque a partir de 2016 se han documentado estrategias globales para atacar a gobiernos democráticos. El caso político más conocido es el de Rusia, quien habría estado atacando procesos electorales en Estados Unidos, Francia, Alemania e Italia, cuando menos. Esta operación global incluye: *hackeo* directo de políticos, organizaciones, universidades y *think tanks*; campañas digitales de propaganda empleando información obtenida de los *hackeos*; y la creación de "fake news" dirigidas específicamente al núcleo de apoyo electoral de candidatos opuestos a las políticas de Moscú.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Para enfrentarse a los incidentes de los ciberdelincuentes, desde 2004 se estableció a nivel internacional el Convenio de Budapest, bajo el cual a la fecha existen 62 países firmantes, siendo México un país observador. En este Convenio también concurre un comité integrado por representantes de la Unión Europea, G7, Interpol, OCDE, OEA, ONU y Unión Africana. Aunque este instrumento de relaciones internacionales busca ser el marco para resolver litigios y extradiciones, en los hechos resulta inoperante, debido a que están ausentes los países de donde provienen la mayor cantidad de ataques en contra de occidente: Norcorea, China, Rusia, India, Irán, Indonesia, Nigeria y Brasil.

A pesar de sus limitaciones, la Convención de Budapest establece el precedente para prevenir y establecer litigios en contra de delitos cibernéticos como son: robo de identidad, ataque a infraestructuras críticas, *spam*, *malware*, *botnets*, terrorismo y ataques DDOS.

En el caso de México, en el año de 2017 el Gobierno Federal publicó el documento rector a la fecha llamado "Estrategia Nacional de Ciberseguridad" (Presidencia de la República, 2017), el cual fue el resultado de mesas de trabajo con el apoyo de la Organización de Estados Americanos, mediante su Comité Antiterrorismo, debido a que se sabe que un 80% de países no cuentan con estrategias de ciberseguridad o planes de protección de infraestructura crítica. Este documento, como sucede con muchas iniciativas de gobierno o privadas, también confunde los esquemas de "seguridad informática" (programas e infraestructura), con respecto a "seguridad de la información" (organización y actividades humanas).

El más reciente esfuerzo a nivel internacional por regular el "teatro de operaciones" de las ciberguerras actuales, ocurrió en noviembre de 2018, en el Foro de Gobernanza de Internet de la UNESCO, donde el presidente de Francia Emmanuel Macron lanzó el "Llamado de París" para la confianza y la seguridad en el ciberespacio. Esta declaración de alto nivel a favor del desarrollo de principios comunes para asegurar el ciberespacio ya ha recibido el respaldo de 552 partidarios oficiales: 66 países, 139 organizaciones internacionales y de la sociedad civil y 347 entidades del sector privado. Entre los objetivos del "Llamado de París" se enlistan:

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

- aumentar la prevención y la resistencia a la actividad maliciosa en línea;
- proteger la accesibilidad e integridad de Internet;
- cooperar para prevenir la interferencia en los procesos electorales;
- trabajar juntos para combatir las violaciones de propiedad intelectual;
- mejorar la seguridad de los productos y servicios digitales, así como la "higiene cibernética" de todos los usuarios;
- reprimir las actividades mercenarias en línea y las acciones ofensivas de actores no estatales; entre otras.

Si bien se requiere un tratado internacional para regular las actividades de las guerras cibernéticas actuales, el "Llamado de París" fue rechazado de inmediato por Rusia, China y Estados Unidos, los 3 principales países involucrados en los conflictos cibernéticos a la fecha (Archer, 2018).

Para comprender la utilidad de los tratados entre países, es necesaria una distinción entre el tipo de ataques, para determinar si se trata de una motivación política o no (Kim Andreasson, 2012, capítulo 13). A detalle, en el caso de los ataques sin motivación política, los acuerdos internacionales y la cooperación con el sector privado ayudan a mitigar las amenazas, como son: aquellas de motivación financiera, como las cometidas por ciberdelincuentes, el robo de propiedad intelectual, el fraude digital, así como el hackeo por retribución, diversión o por empleados molestos.

En cambio, será mucho más difícil poder lidiar con amenazas de motivación política, aquellas realizadas por gobiernos o con su apoyo, como son: la ciberguerra, el ciberterrorismo, espionaje y "hacktivismo" (hackeo con fines políticos). Un caso reciente de este tipo ocurrió contra la embajada de México en Guatemala, en este año de 2019, la cual fue víctima de un "hackeo", donde más de 4,800 documentos fueron comprometidos, incluyendo copias de pasaportes, visas y cartas confidenciales de ciudadanos y diplomáticos mexicanos que viven en la capital guatemalteca (Ruiz, 2019).

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

De la unipolaridad a un mundo de cuatro potencias

Cuando se analiza la cantidad de Infraestructuras Críticas de Información y Telecomunicaciones de los diferentes países en el mundo, puede observarse una correlación directamente proporcional con respecto a aquellas naciones protagonistas en el "teatro de operaciones" cibernético.

Uno de los principales elementos de soberanía en telecomunicaciones consiste en la operación de satélites para uso militar o de gobierno. Al momento de la elaboración del presente documento, existe un aproximado de 2,062 satélites en operación en la órbita terrestre, de los cuales 992 corresponden a satélites activos de uso militar, de gobierno o compartido entre ambos, con uso civil o comercial, cuyos países encargados de su operación son los siguientes:

Cuadro 1
Satélites activos de uso militar, de gobierno o compartido

RANK	PAÍS	SATÉLITES	PORCENTAJE
1	EUA	333	34%
2	China	218	22%
3	Rusia	123	12%
4	India	51	5%
5	Japón	35	4%
6	Multinacional	23	2%
7	Agencia Europea	22	2%
8	Alemania	14	1%
9	Francia	12	1%
10	Reino Unido	11	1%
11	Corea del Sur	9	1%
12	España	9	1%
13	Israel	9	1%
14	Italia	8	1%
15	Arabia Saudita	6	1%
	TOTAL	**992**	**100%**

Elaboración propia, Vestiga Consultores, mayo 2019. Con base en datos de satélites de la Union of Concerned Scientists (UCS), marzo 2019.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

En caso de que continuáramos el listado, México aparece hasta el lugar 28, con sólo 2 satélites de uso militar o de gobierno: Mexsat-3 (Mexsat Bicentenario, desarrollado por Orbital Sciences Corp, número Norad 39035) y Mexsat3 (Morelos-3, desarrollado por Boeing Satellite Systems, número Norad 40946). Dadas las características y necesidades de telecomunicaciones en el país, como ha sido el llamado de la nueva administración federal para proveer de Internet a todo el territorio nacional, México requeriría cuando menos de 4 satélites adicionales, independientemente de las redes de fibra óptica y las antenas instaladas por parte de las compañías de telefonía e Internet en el país.

Como puede observarse en la tabla anterior de infraestructura de satélites en operación, los cuatro países con mayor presencia también son las 4 potencias que disputan actualmente las principales estrategias geopolíticas en el mundo: Estados Unidos, China, Rusia e India.

Estas cuatro naciones también tienen un papel destacado en el gasto militar mundial en 2018, el cual ha sido el año de mayor inversión militar en la historia:

Cuadro 2
Gasto militar mundial en 2018

RANK	PAÍSES	GASTO (USD BN)	% PIB
1	Estados Unidos	649	3.2
2	China	250	1.9
3	Arabia Saudita	68	8.8
4	India	67	2.4
5	Francia	64	2.3
6	Rusia	61	3.9
7	Reino Unido	50	1.8
8	Alemania	49	1.2
9	Japón	47	0.9
10	Corea del Sur	43	2.6
11	Italia	28	1.3
12	Brasil	28	1.5
13	Australia	27	1.9

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

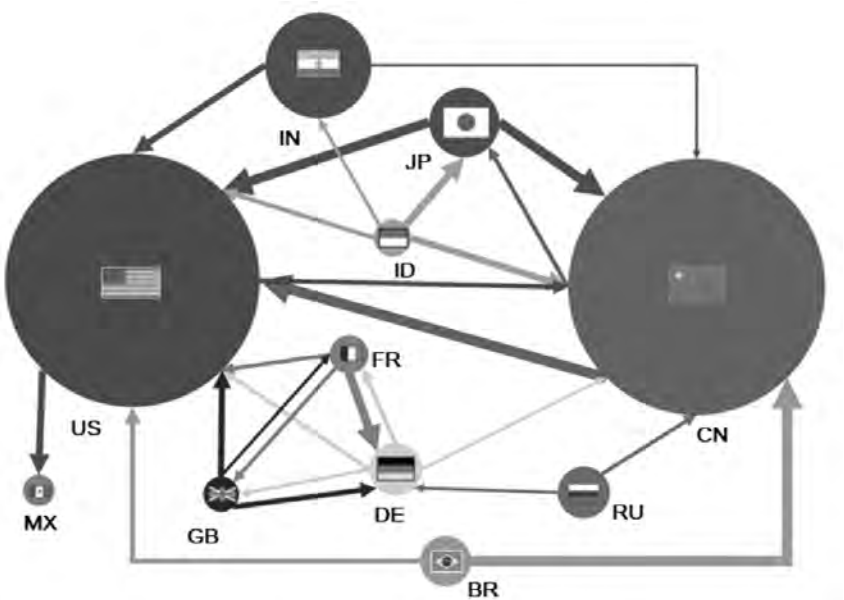
Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

RANK	PAÍSES	GASTO (USD BN)	% PIB
14	Canadá	22	1.3
15	Turquía	19	2.5
	Total mundial	**1,822**	**2.1**

SIPRI (Stockholm International Peace Research Institute), en: Nan Tian, *et. al.*, *Trends in World Military Expenditure.*

Para comprender la dinámica e interdependencia actual entre las potencias mencionadas, hemos elaborado un diagrama con las principales relaciones comerciales entre estos países. En este diagrama, mientras el tamaño de los círculos representa la dimensión de cada economía (por paridad de poder adquisitivo), el tamaño de las fLechas indica el tipo de relación comercial (importaciones o exportaciones), así como el valor de las mismas.

Figura 1
Relación comercial de 11
principales economías exportadoras



Elaboración propia, Vestiga Consultores. Con base en datos del *Factbook 2012* de la Agencia Central de Inteligencia, Estados Unidos.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Esta correlación de fuerzas cambiará poco en las próximas décadas. De acuerdo a la firma PriceWaterhouseCoopers (PwC, febrero 2015), junto con Indonesia y Nigeria, México es una de las 3 economías emergentes que integrarán el listado de las 10 principales economías entre 2030 y 2050:

Figura 2
Proyección de 10 principales economías 2050

	2014		2030		2050	
PPP rank	Country	GDP at PPP (2014 US$bn)	Country	Projected GDP at PPP (2014 US$bn)	Country	Projected GDP at PPP (2014 US$bn)
1	China	17,632	China	36,112	China	61,079
2	United States	17,416	United States	25,451	India	42,205
3	India	7,277	India	17,138	United States	41,384
4	Japan	4,788	Japan	6,006	Indonesia	12,210
5	Germany	3,621	Indonesia	5,486	Brazil	9,164
6	Russia	3,559	Brazil	4,996	Mexico	8,014
7	Brazil	3,073	Russia	4,854	Japan	7,914
8	France	2,587	Germany	4,590	Russia	7,575
9	Indonesia	2,554	Mexico	3,985	Nigeria	7,345
10	United Kingdom	2,435	United Kingdom	3,586	Germany	6,338
11	Mexico	2,143	France	3,418	United Kingdom	5,744

PwC, febrero 2015. PIB proyectado en PPP.

Debido a estas proyecciones, se sabe que aumentará el valor geopolítico de México ante el mundo, y por tanto, podrían aumentar los ataques cibernéticos en contra del país y sus intereses comerciales.

Estado del arte en México y problemas estructurales

Bajo el contexto mundial que aborda el presente documento, el 1 de junio de 2016 en México se crea el Centro de Operaciones del Ciberespacio de la Secretaría de la Defensa Nacional. Parte de las capacidades ampliadas del gobierno mexicano se ha reflejado recientemente, por ejemplo, en operativos de la Secretaría de Marina, para el arresto de líderes de cárteles del narcotráfico, los cuales se habrían logrado mediante la intercepción de comunicaciones de aplicaciones de mensajería, tales como Whatsapp y Telegram, apoyados por tecnología americana e israelí,

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

como puede ser aquella que se basa en explotar las vulnerabilidades del código SS7, técnica reciente que usan los hackers de élite mundial para romper la "doble autentificación" de los usuarios.

Un esquema básico del sistema de ciberseguridad nacional, fue presentado recientemente para el Instituto de Investigaciones Estratégicas de la Armada de México[1], como puede verse a continuación:

Figura 3
Posible organigrama de la Seguridad Nacional Cibernética en México

Adolfo Arreola (2018), Secretaría de Marina.

A nivel mundial el esquema de defensa cibernética que se sigue es el establecido por los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), los cuales surgen como respuesta de DARPA ante el primer

1 Adolfo Arreola García, Ciberseguridad Nacional en México y sus desafíos. Instituto de Investigaciones Estratégicas de la Armada de México, Secretaría de Marina. Septiembre 2018, pp. 28

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

malware de la historia en 1988 ("Morris worm", el cual infectó casi 10% de las 66 mil computadoras que en aquel entonces conformaban Internet).

> En un trabajo reciente de Rodrigo Riquelme (2018), se explica que:
> en el mundo sólo existen dos CERT como tal: uno es el CERT/CC (CERT Coordination Center), que forma parte del Instituto de Ingeniería en Software de la Universidad de Carnegie Mellon, en Pennsylvania, Estados Unidos, y el otro es el US-CERT, el equipo de respuesta del Departamento de Seguridad Nacional estadounidense.
>
> En todos los demás países del mundo, a los equipos de ciberseguridad se les denomina Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por su sigla en inglés), los cuales al obtener la certificación que ofrece la Universidad de Carnegie Mellon pueden incluir en su nombre la sigla CERT. Además, es necesario distinguir entre los CSIRT que pertenecen a instituciones públicas, como es el caso del CERT - UNAM, y aquellos que forman parte de la oferta de empresas privadas, como puede ser el CERT - IQSec.

De esta manera, tenemos la siguiente lista de defensas cibernéticas de México:

CSIRTs públicos (Equipo de Respuesta ante Incidentes de Seguridad Informática):

1. CSIRT de la Universidad Nacional Autónoma de México (CERT UNAM)
2. CSIRT de la Policía Federal (CERT MX)
3. CSIRT de la Universidad Autónoma de Chihuahua (CERT UACH)
4. CSIRT del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (CERT Infotec)

CERTs privados (Equipos de Respuesta ante Emergencias Informáticas):

1. CSIRT de Scitum (Scitum CERT)
2. CSIRT de IQSec (IQSec CERT)

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

3. CSIRT de Total Sec (CERTDSI Totalsec)
4. CSIRT de Netrix (CERT Ntx)
5. CSIRT de Global CyberSec (GCS CERT)
6. CSIRT de Mnemo (Mnemo CERT)
7. CSIRT de TIC Defense (TIC CERT)

A pesar de la existencia de los once centros de monitoreo cibernético mencionados, con base en diez años de experiencia con participación personal directa en investigaciones o análisis post-mortem de incidentes cibernéticos, podemos considerar que México se enfrenta cuando menos a los siguientes problemas estructurales particulares.

A. Ausencia de capital humano

A nivel de todas las ingenierías, se sabe que México tiene un déficit de 2 millones de profesionistas, el cual sería cubierto hasta dentro de 14 años. Por esta razón, el país es el principal importador de mano de obra calificada de toda Iberoamérica.

En la industria de seguridad cibernética, esta carencia de personal calificado deja expuestas a las organizaciones públicas y privadas. Este factor se agrava cuando en algunas industrias no se comparte la información suficiente sobre nuevos riesgos. El caso más reciente fue el hackeo a Bancomext, con un monto defraudado por 30 millones de dólares. Este ataque fue realizado por el colectivo Lazarus, y dado a conocer hasta enero de 2018. De acuerdo a las autoridades mexicanas, al menos durante 500 días más de 30 equipos de cómputo habrían sido infectados por el mismo malware que usó este colectivo para atacar a la empresa Sony, así como a otros bancos en el sudeste asiático. En México, de acuerdo a contactos de la industria, dos años antes del ataque a Bancomext, cuando menos 2 bancos privados ya tenían conocimiento de los intentos de ataque en el país, pero los detalles técnicos no fueron compartidos a tiempo.

B. Cárteles de crimen organizado

Debido a la proliferación de actividades de los grupos de crimen organizado en México, desde hace más de una década se sabe que varias células de los mismos están dedicadas al secuestro o reclutamiento de grupos de ingenieros o empleados de empresas de sectores clave,

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

como son las entidades financieras del país. El mayor caso al respecto ha sido el hackeo al sistema de SPEI (Sistema de Pagos Electrónicos Interbancarios) en el primer semestre de 2018. De acuerdo a información interna de algunas de las empresas afectadas, sabemos que cuando menos 3 mil cuentas de cada banco fueron empleadas en toda la República Mexicana, las cuales en promedio tenían más de 4 años de existencia, para poder distribuir el dinero que se fue extrayendo de la alteración a la operación del SPEI. En muchos de estos casos, más que un hackeo externo, existe complicidad por parte de empleados que son contratados o extorsionados por los cárteles del narcotráfico. Fue ahora en mayo de 2019 que habría sido capturado el líder de la célula que organizó esta operación, con cuentas y activos físicos por 250 millones de pesos.

C. Robo de identidad

Un problema recurrente en el país es el robo de identidad, e incluso las entidades financieras se enfrentan al reto de poder comprobar la documentación que presentan los clientes para "aperturar" nuevas cuentas. Este tema afecta en particular a las empresas dedicadas a otorgar préstamos o créditos, ya sea financieros o para adquirir algún inmueble o bien mueble. Hasta donde tenemos entendido, las compañías reciben documentación que incluso es oficial, pero no corresponde a la identidad real de la persona. Al respecto, al interior del INE (Instituto Nacional Electoral), instancia que otorga el principal documento de identificación en México, existe una deliberación con respecto a cómo mejorar los procesos de comprobación de identidad, así como del almacenamiento de la misma. En años recientes, una de las principales tecnologías que ayudarían al respecto es el BlockChain (Cadena de bloques): existen programas de Naciones Unidas, como el de entrega de alimentos, donde se apoyan en registros biométricos, para asignar un BlockChain infalsificable, por ejemplo, a desplazados de zonas de guerra que ya no poseen documentación oficial alguna.

D. Carencia de estándares ISO 27000 (ISO/IEC 27001:2005)

De un enfoque heurístico, el elemento de mayor riesgo en la seguridad cibernética lo representa el factor humano,

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

y para el caso de México las organizaciones se enfrentan a la baja educación tecnológica. A ello debe añadirse el desconocimiento de las mejores prácticas de seguridad de la información del ISO 27000 (ISO/IEC 27001:2005). Prueba de ello lo representan los casos de ataque tipo "spear-phishing", los cuales son los mayores tipo de defraudación en el país, donde el atacante envía un correo apócrifo haciéndose pasar por una persona u organización legítima, con tal de solicitar un pago o transferencia bancaria. Técnicamente, para evitar este engaño, basta con analizar el código fuente del correo electrónico recibido, para determinar si se trata de un servidor legítimo; no obstante, es muy reducido el número de usuarios con la capacidad para realizar dicho análisis.

Actual monitoreo sobre México desde el Pentágono

A nivel de industria, la clasificación del nivel de severidad de un ataque cibernético es parecida a los 5 niveles con que se clasifica la fuerza de un huracán, siendo el nivel 5 el de mayor afectación a la infraestructura crítica de un país, donde puede quedar sin energía eléctrica en regiones del mismo o en todo su territorio, como ha sucedido en Ucrania.

El ataque que sufrió Bancomext recientemente se califica entre los niveles 2 y 3. México no ha recibido un ataque de mayor potencia debido a que las infraestructuras críticas del país son protegidas por el Comando Norte de Estados Unidos (United States Northern Command), el cual incluye a toda la Unión Americana y Canadá. El anterior encargado de esta zona militar fue el general John Kelly, anterior jefe de gabinete del Presidente Donald Trump.

A nivel digital, Estados Unidos cuenta con el Comando Cibernético (US Cyber Command), el cual fue creado en 2009 para funcionar bajo el cobijo de la NSA. El Cibercomando americano centraliza las operaciones del gobierno en el ciberespacio, ya sea para organizar recursos cibernéticos o coordinar la defensa y ataque de redes militares.

A partir de la llegada de la actual administración de Estados Unidos, existen 3 cambios radicales en la política de Seguridad Nacional Cibernética de este país:

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

1. Comando Cibernético (US Cyber Command)
   - El Cibercomando es elevado de rango, al nivel de una Secretaría, con lo cual sale de la esfera de la NSA.
   - Este Comando ya cuenta con autorización para realizar ataques preventivos y no sólo de monitoreo o reacción.
2. Departamento de Seguridad Nacional (Department of Homeland Security)
   - Se crea una Unidad especial dedicada a la protección de las Infraestructuras Críticas del país.
   - Se presta especial interés a las instalaciones eléctricas.
3. Fuerza Espacial (Space Force)
   - Se destina un presupuesto y personal para la defensa satelital, frente a los posibles ataques fuera de órbita de Rusia, China o India.
   - Se enfoca el calendario de la NASA para tener misiones tripuladas tanto a la Luna como a Marte en la presente década.

Estas estrategias de Seguridad Cibernética Nacional de Estados Unidos están apoyadas con una red de empresas líderes de la industria de armamento y seguridad, como son: Lockheed Martin, Raytheon, Boeing, Northrop Grumman, General Dynamics, BAE Systems, etcétera. Asimismo, en capital humano, la planeación y ejecución de las estrategias se llevan a cabo por consultoras privadas tales como Booz Allen Hamilton, Leidos, McKinsey, entre otras.

Además, dichas estrategias de Seguridad Cibernética Nacional, están acompañadas por la guerra comercial de Estados Unidos en contra de China. Debe mencionarse que las medidas en contra de empresas chinas no comenzaron con el gobierno de Donald Trump: desde 2016 el Pentágono prohibió el uso de laptops Lenovo, por contener microcomponentes de espionaje; en 2017 se restringió la venta del antivirus Kaspersky incluso en tiendas como BestBuy, porque su creador reconoció el robo de secretos

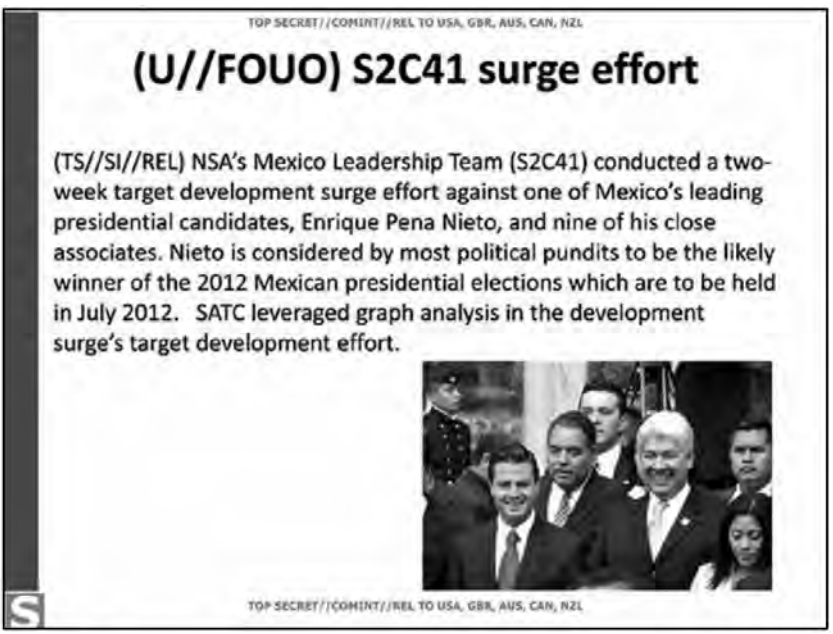
DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

militares americanos; y han sido más difundidos desde 2018 las medidas en contra de Huawei, desde la captura de su CFO e hija del fundador, así como el reciente bloqueo de suministros a esta empresa por parte de tecnológicas americanas como Google o Intel.

Para el caso de México, tanto los ex presidentes Felipe Calderón así como Enrique Peña, junto con otros 35 líderes mundiales, fueron intervenidos en sus comunicaciones por parte de la NSA (mediante su unidad SATC), lo cual fue revelado en una serie de documentos filtrados por el ex ingeniero de esta agencia, Edward Snowden.

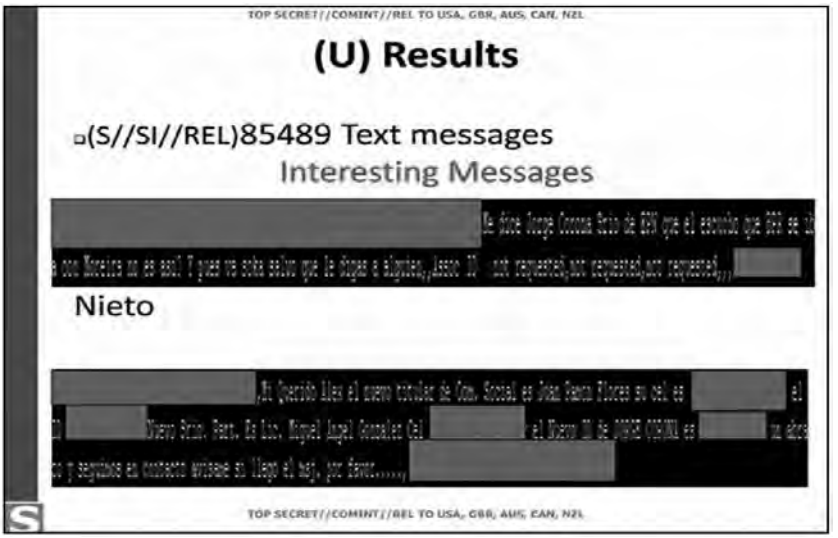
Figura 4
Documento filtrado por Edward Snowden
Publicado por Electronic Frontier Foundation, 2013



DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Figura 5
Documento filtrado por Edward Snowden
Publicado por Electronic Frontier Foundation, 2013



Como puede verse en la evidencia anterior, diversos mensajes de México fueron interceptados, en este caso sobre un encuentro con el entonces Gobernador de Coahuila, Humberto Moreira, con respecto al señor Jorge Corona, en su momento secretario auxiliar del entonces Gobernador Enrique Peña, y actualmente diputado federal.

Esta información de inteligencia obtenida por la NSA es compartida con los "FiveEyes": Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda, con quienes el gobierno americano comparte más información.

En el mismo documento publicado por la Electronic Frontier Foundation (2013, p.19), puede leerse un apartado llamado "Geopolitical Trends: Key Challenges", en donde se describe el objetivo del monitoreo sobre México:

> Algo que une a todos estos países es su importancia para intereses económicos, de comercio y defensa de Estados Unidos (...) (esta división) se enfoca

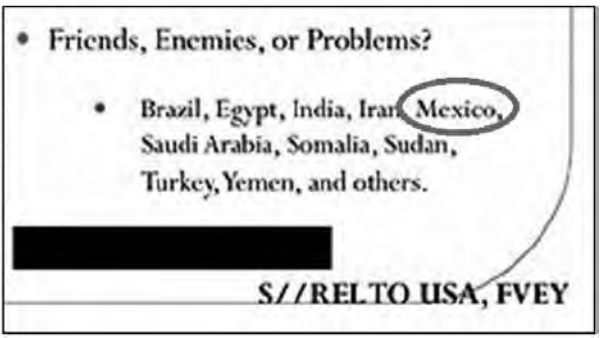
DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

principalmente en la política exterior y actividades comerciales de Bélgica, Francia, Alemania, Italia y España, así como Brasil, Japon y Mexico. Los reportes de esta División también proveen información clave sobre actividades militares y de inteligencia en algunos de estos países.

Además, en el apartado "Factores de estrés sobre la estabilidad regional/Ascenso de nuevos actores", al país se describe de la siguiente manera: "Mexico está estresado, e impacta en nuestra frontera". Debido a este contexto, en la proyección que maneja la NSA, a nuestra nación se le ubica en un bloque entre posibles "amigos, enemigos o problemas":

Figura 6
Documento filtrado por Edward Snowden
Electronic Frontier Foundation, 2013



Finalmente, debe señalarse que la función de la NSA no ha sido sólo de monitoreo: de acuerdo a la información obtenida por Edward Snowden, y revelada en diferentes entrevistas (como lo ha sido la producción de Oliver Stone, y una serie de 4 horas de entrevistas de Stone con el Presidente de Rusia), parte de la información obtenida por la NSA ha sido usada por Estados Unidos no sólo por temas de seguridad nacional, sino para negociaciones de tratados comerciales; adicionalmente, la NSA contaría con dispositivos y códigos al interior de las infraestructuras críticas de varios de sus "aliados" (como son Alemania, Japón y México), para sabotear la energía o telecomunicaciones de estos países en caso de una disputa con Estados Unidos.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Propuestas de Reformas periodo 2018-2024

En México han existido cuatro relevantes momentos en el desarrollo de una estructura de seguridad cibernética, con la creación de diferentes dependencias en los siguientes años:

- 2001: PFP, «Policía Cibernética Federal»
- 2013: CDMX, «Policía Cibernética»
- 2016: Ejército, «Centro de Operaciones del Ciberespacio»
- 2017: PGR, «Unidad de Investigaciones Cibernéticas»

No obstante, estas iniciativas siguen rezagadas, al menos con respecto a los años de creación de los principales referentes en Estados Unidos:

1952: National Security Agency (criptografía)
1978: FISA (Foreign Intelligence Surveillance Act)
2009: United States Cyber Command

Parte de los retos en México parten desde el Poder Legislativo, debido a la ausencia de una Ley federal de delitos cibernéticos, frente al debate actual que existe en Inglaterra y China, en donde están aprobando nuevas leyes sobre ámbito de seguridad cibernética (con respecto a exigir "back doors" a las empresas tecnológicas, o ampliar la recolección de "meta data" de los habitantes).

Recién en marzo de 2019 en el Senado de la República, la fracción del partido Morena hizo pública una propuesta de "Ley de Seguridad Informática" (Senadora Lucía Trasviña, 2019). En esta iniciativa se plantea la creación de una Agencia Nacional de Seguridad Informática (ANSI), la cual proteja la "Infraestructura Información (sic) Esencial", ante posibles actos de: espionaje, sabotaje, terrorismo, rebelión o "traición a la patria". En este sentido, se incluyen como agravantes aquellos ataques en contra del "Estado", así como en contra de entidades financieras, con multas de hasta 136 mil pesos. En un primer análisis de esta iniciativa, y a reserva de que el debate parlamentario modifique su esencia y alcances, de nueva cuenta se parte de una concepción que confunde la "seguridad informática" con respecto de la "seguridad de la información", y no se

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

detallan cuáles serían aquellas infraestructuras críticas a proteger.

Una de las leyes más avanzadas en la materia se aprobó este año en India, donde se obliga a las empresas extranjeras de tecnología (como Amazon, Google, Facebook, etc.), a procesar los datos de los usuarios locales en servidores ubicados físicamente en territorio de la India. De esta manera, la nueva Ley de la India aumenta su "soberanía cibernética", al permitir la realización de procesos legales en contra de las empresas de tecnología ante alguna disputa comercial, de protección de datos, etc. Esta situación no ocurre actualmente en México, debido a que la "extra territorialidad" bajo la que operan estas empresas, obliga a que los usuarios mexicanos presentaran las demandas pero en Estados Unidos.

Elementos para primer atlas de riesgos cibernéticos

Las dependencias potencialmente involucradas en una nueva estrategia de seguridad nacional cibernética requieren mejorar su nivel de tecnología y recursos humanos, para salir de un momento de desmantelamiento que han padecido cuando menos en las recientes 3 administraciones federales.

Existen casos dramáticos que documentan esta situación: en 2015 se filtraron los archivos de una empresa de ciberseguridad italiana "HackerTeam", en cuyos correos internos hicieron mofa de que los servidores del CISEN (Centro de Investigación y Seguridad Nacional) ni siquiera contaban con un FireWall instalado; para la tercera captura del narcotraficante Joaquín "Chapo" Guzmán en 2016, el operativo de la Marina tuvo en todo momento el apoyo de la DEA (Drug Enforcement Administration), pero con intercepción de mensajes y llamadas desde Estados Unidos; desde 2016 se hicieron públicas filtraciones de contratos de dependencias como PGR (Procuraduría General de la República), PFP (Policía Federal Preventiva) o el propio CISEN, para usar software de espionaje de la empresa de Israel NSO (famosa por el malware "Pegasus"), cuyos resultados en México fueron limitados, pero costosos.

Para establecer una primera línea de fuego ante los riesgos de seguridad nacional cibernética en México, se

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

requiere instrumentar el esquema C4ISR, por sus siglas en inglés, que implica: Comando, control, comunicaciones, computadoras e inteligencia, vigilancia y reconocimiento. En el documento más reciente de Estrategia de Defensa Nacional de Estados Unidos (Departamento de la Defensa, 2018), se establece como prioridad el fortalecimiento del C4ISR, entendida esta estrategia como el desarrollo de redes y ecosistemas de información resilientes, constantes, a nivel federal, desde el nivel táctico hasta la planificación estratégica. Esta estrategia también da prioridad a las capacidades para obtener y explotar información, negarles a los competidores las mismas ventajas, y permitan proporcionar atribuciones para responsabilizar a los actores estatales o no estatales culpables durante los ataques cibernéticos.

Adaptándose a la nueva realidad internacional, México necesita establecer un mapa de los siguientes sectores que son definidos como críticos:

Sectores de Infraestructuras Críticas

1. Entidades financieras
2. Instalaciones de comercio y logística
3. Parques críticos de manufacturas
4. Dependencias de gobierno
5. Hospitales y centros de salud
6. Universidades y escuelas
7. Defensa y seguridad nacional
8. Instalaciones eléctricas
9. Abasto energético y gasoductos
10. Sistemas de telecomunicaciones
11. Sistemas de transporte
12. Cobertura de red satelital
13. Plantas de químicos y petroquímica
14. Servicios de emergencias
15. Centrales de represas e hidroeléctricas
16. Sistemas de aguas y tratamiento
17. Producción de alimentos
18. Centros nucleares y de materiales peligrosos

Debe observarse que cuando menos el 85% de estas Infraestructuras Críticas se encuentran en empresas del sector privado, por lo cual resulta indispensable la sinergia de esfuerzos. Algunas tendencias que incrementan los

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

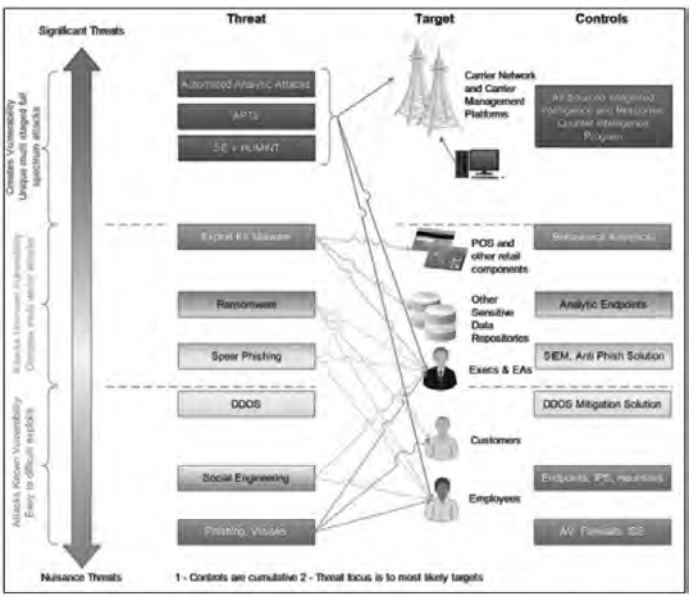
Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

riesgos en estos sectores son: interdependencia entre los mismos sectores, proliferación de puntos expuestos, y concentración de activos.

Como ejemplo de algunos de los elementos del Atlas Nacional de Riesgos Cibernéticos, hemos integrado un listado de las organizaciones, escuelas, empresas y gobiernos estatales más atacados por *hackers* en México. Para ello, parte de nuestra metodología se apoya en el análisis de Cómputo Forense de diferentes campañas de *phishing* y *malware* que han atacado a usuarios nacionales, así como la revisión de directorios con muestras de ataques cibernéticos a servidores mexicanos en los últimos 5 años.

El Atlas de riesgos cibernéticos resulta indispensable para poder mapear las amenazas a todas las Infraestructuras Críticas del país. Los ataques pueden venir desde la parte más alta del sistema, directamente en contra de la infraestructura física, o con ataques sobre los usuarios de la misma, como puede apreciarse en el siguiente diagrama:

Figura 7
Controles según cada tipo de amenaza cibernética



Greg Reith, *Recorded Future,* 2017.

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Para poder proteger a las infraestructuras críticas del país, se requiere instrumentar en todas las dependencias de gobierno directamente relacionadas las siguientes capas de seguridad cibernética:

Capas de seguridad cibernética

1. Dispositivos (seguridad Endpoint, cifrados)
2. Aplicativos (BMS, bases de datos, web)
3. Datos (control de acceso, autenticación, administración de claves)
4. Red (firewalls, DMZs, VPNs, segmentaciones)
5. Perimetral (filtros de Internet, monitoreo de amenazas)
6. Física (guardias, candados)

Conclusiones

Como se ha expuesto en el presente documento, el papel geopolítico de México seguirá creciendo en valor en las próximas décadas, debido a su relación comercial con las principales potencias del mundo. Debido a ello, resulta previsible un aumento en los ataques en contra de las Infraestructuras Críticas del país. Si bien actualmente muchos de estos activos se encuentran bajo monitoreo de diferentes dependencias de Estados Unidos, existen problemas estructurales específicos que aumentan el nivel de riesgo en México, como lo es la presencia de grupos de crimen organizado y la falta de personal altamente capacitado.

Adicionalmente, existen elementos indispensables para la elaboración de un primer Atlas de riesgos para la Seguridad Nacional Cibernética:

- Taxonomía de incidentes cibernéticos frecuentes en México
- Medidas para prevenir y combatir incidentes cibernéticos
- Prácticas de ISO 27000 (desde ISO/IEC 27001:2005) para resiliencia e higiene cibernéticas
- Documentación y protocolos para protección legal
- Nueva Protección de Datos de Unión Europea (GDPR)

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

- Nueva iniciativa nacional para la educación en Ciberseguridad (NICE, por sus siglas en inglés), del National Institute of Standards and Technology (NIST), del Departamento de Comercio de los Estados Unidos

La cooperación entre sectores será una de las principales vías en la cual México pueda aumentar su resiliencia cibernética, como lo es: a nivel Gobierno, fortalecer sus capacidades de reacción, defensa y contraataque, para proteger las Infraestructuras Críticas; a nivel de Universidades, se requiere mayor investigación y capacitación de profesionistas; a nivel de Empresas, se necesita ampliar la cantidad de programas de monitoreo e innovación, así como promover la autoeducación como primera línea de defensa de la nación.

BIBLIOGRAFÍA

Agencia Central de Inteligencia. *The CIA World Factbook*. Virginia, Estados Unidos [Consultado en https://www.cia.gov/library/publications/the-world-factbook/].

Agencia de Seguridad Nacional (unidad SATC). *Intelligently filtering your data: Brazil and Mexico case studies*. Maryland, Estados Unidos. Difundido en el sitio de *Electronic Frontier Foundation* [Consultado en https://www.eff.org/files/2013/11/15/20130903-globo-satc.pdf].

Andreasson, Kim. *Cybersecurity: Public Sector Threats and Responses*. Florida, Estados Unidos. CRC Press. 2012, pp. 392.

Archer, Joseph. "US, Russia and China refuse to back French cybersecurity initiative". *The Telegraph*. Noviembre, 2018 [Consultado en https://www.telegraph.co.uk/technology/2018/11/12/us-russia-china-refuse-back-french-cybersecurity-initiative/].

Arreola García, Adolfo. "Ciberseguridad Nacional en México y sus desafíos". México. Instituto de Investigaciones Estratégicas de la Armada de México, Secretaría de Marina. Septiembre 2018, pp. 28 [Consultado en https://www.researchgate.net/publication/329253059].

Budapest Convention, *The Convention on Cybercrime of the Council of Europe*. Consejo de Europa. 2004 [Consultado en https://www.coe.int/en/web/cybercrime/the-budapest-convention].

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Calder, Alan. *Information Security based on ISO 27001/ISO 27002*, Londres, Reino Unido. Van Haren Publishing. 2009, pp. 102.

Departamento de la Defensa. *2018 National Defense Strategy*. Estados Unidos, Virginia. 2018 [Consultado en: https://dod.defense.gov/Portals/1/ Documents/ pubs/2018-National-Defense-Strategy-Summary.pdf].

Departamento de la Defensa. *The Military Dictionary (Dictionary of Military and Associated Terms)*. Virginia, Estados Unidos. DIANE Publishing. 1987, pp. 399.

France Diplomatie. *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Paris, 2018 [Consultado en: https://www.diplomatie.gouv.fr/en/ french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in].

Presidencia de la República. *Estrategia Nacional de Ciberseguridad*. México, 2017 [Consultado en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf].

PriceWaterhouseCoopers. *The World in 2050. Will the shift in global economic power continue?*, febrero 2015, pp. 46 [Consultado en https://www.pwc.com/gx/en/issues/ the-economy/assets/world-in-2050-february-2015.pdf].

Reith, Greg. "Prioritizing Cyber Threats With Real-Time Threat Intelligence". Recorded Future. Agosto, 2017 [Consultado en https://www.recordedfuture.com/ prioritizing-cyber-threats/].

Riquelme, Rodrigo. "¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?". *El Economista*. Enero, 2018 [Consultado en https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html]

Rollins, John. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. Washington DC, Estados Unidos. DIANE Publishing. Marzo 2009, pp. 18.

Ruiz, Claudia. "Embajada de México en Guatemala es víctima de un hackeo". *CNET*. Abril 2019 [Consultado en https://www.cnet.com/es/noticias/embajada-de-mexico-en-guatemala-es-victima-de-un-hackeo-reporte/].

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge, Reino Unido. Cambridge University Press. 2015, pp. 269.

Tian, Nan, et. al., *Trends in World Military Expenditure*. SIPRI (Stockholm International Peace Research Institute). Abril, 2019.

Trasviña, Lucía. *Propuesta de Ley de Seguridad Informática.* México, Senado de la República, 2019, pp. 17 [Consultado en http://blog.derecho-informatico.org/wp-content/uploads/2019/03/20190319_PropuestaMorena_LSI.pdf].

Union of Concerned Scientists (UCS), *UCS Satellite Database*, marzo 2019 [Consultada desde https://s3.amazonaws.com/ucs-documents/nuclear-weapons/sat-database/5-9-19-update/UCS_Satellite_Database_4-1-2019.xlsx].

DR © 2019. Instituto Nacional de Administración Pública, A.C.
http://www.inap.mx/portal/index.php?option=com_content&view=article&id=90&Itemid=483