Revista de Administración Pública

INAP

Hacia una estrategia nacional de ciberseguridad en México

Edgar Iván Espinosa*

México atraviesa por una crisis de ciberseguridad que se ha ido agudizando ante la falta de una política unificada que coordine los esfuerzos implementados por algunas dependencias gubernamentales y la iniciativa privada. Contar con una estrategia integral resulta indispensable para hacer frente a tres principales amenazas: la ciberdelincuencia, el ciberespionaje y el *hacktivismo*.

La preocupación por las cuestiones de ciberseguridad no es algo nuevo. La reflexión sobre estos temas inició desde mediados de los años 90 en Estados Unidos, ante el temor de que *hackers* o piratas informáticos comprometieran la información gubernamental, y los sistemas de control y supervisión de procesos (SCADA, por sus siglas en inglés) de plantas nucleares, hidroeléctricas, tratamiento de aguas, sistemas de transporte, salud, defensa, y otros servicios de la infraestructura crítica.[1]

A nivel internacional, el interés se incrementó a raíz de tres incidentes. El primero, los ciberataques lanzados en 2007 contra Estonia desde direcciones IP rusas, en represalia por la remoción de un monumento dedicado a los soldados soviéticos caídos durante la Segunda Guerra Mundial.[2] Dicho acontecimiento dejó en claro que el mundo estaba ante una nueva amenaza asimétrica capaz de vulnerar la Seguridad Nacional de cualquier país, derivado de la incapacidad de poder desarrollar una estrategia de disuasión frente al problema de la atribución o identificación

* Egresado del Centro de Estudios Hemisféricos de Defensa (CHDS) de la Universidad Nacional de Defensa (NDU) de Estados Unidos. Licenciado en Ciencia Política y licenciado en Relaciones Internacionales con Mención Especial por el Instituto Tecnológico Autónomo de México (ITAM). Cursó la especialización en Ciberseguridad por el Instituto para la Seguridad Nacional y el Contraterrorismo de la Universidad de Siracusa (INSCT), en Nueva York. Se ha desempeñado como Co-coordinador Académico del Diplomado en Seguridad Nacional del ITAM.

1 Warner, Michael, "Cybersecurity: A Pre-history", *Intelligence and National Security*, 27, 5, 2012, pp. 781-799; y Rudner, Martin, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge", *International Journal of Intelligence and CounterIntelligence*, 26, 3, 2013, pp. 453-481.

2 Martínez De Rituerto, Ricardo, "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE", *El País*, 18 de mayo del 2007.

exacta de la ubicación y/o los autores de un ciberataque.[3] En efecto, aunque los ataques contra Tallin provenían de territorio ruso, técnicamente no era correcto asumir que el Kremlin estuviera involucrado. Aun si se hubiesen detectado computadoras del gobierno, Moscú habría podido alegar que éstas habían sido infectadas y transformadas en *botnets* o redes "zombies" manipuladas a distancia.[4]

Este hecho a su vez detonó la discusión en torno a si un ciberataque puede o debe considerarse *casus belli*, ya que, según algunos, estrictamente no constituiría un ataque físico convencional, como el que proscribe el Artículo 2 de la Carta de Naciones Unidas. Tampoco quedaba claro cómo aplicaría el Derecho Internacional Humanitario en caso de que fuese interpretado como una agresión.[5]

El segundo incidente que incrementó la preocupación global fue el empleo en 2010 de Stuxnet, un virus tipo gusano –considerado la primer ciberarma–, diseñado para destruir los sistemas de la planta nuclear iraní de Bushehr y el complejo de enriquecimiento de uranio en Natanz, utilizando certificados de seguridad robados.[6]

El ataque, atribuido a Estados Unidos e Israel, fue comparado con el lanzamiento de la bomba atómica en Hiroshima y Nagasaki. Este episodio tuvo al menos tres implicaciones: 1) por primera vez un virus informático "confeccionado a la medida" tenía la capacidad de causar daño físico; 2) su complejidad evidenciaba la participación de un Estado, y 3) en cualquier momento una ciberguerra podría estallar.[7]

[3] Kostadinov, Dimitar, *The Attribution Problem in Cyber Attacks*, Infosec Institute, 2013; Wheeler, David A., *et al., Techniques for Cyber Attack Attribution*, Institute for Defense Analyses, 2003; Hunker, Jeffrey, *et al., Role and Challenges for Sufficient Cyber-Attack Attribution*, Institute for Infrastructure Protection (I3P), Dartmouth College, 2008; Rid, Thomas y Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, 38, 1-2, 2015, pp. 4-37; Hare, Forrest, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective", 4th International Conference on Cyber Conflict, Tallin, OTAN, 2012; y Healey, Jason, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, The Atlantic Council's Cyber Statecraft Initiative, 2012.

[4] Plohmann, Daniel *et al., Botnets: Detection, Measurement, Disinfection & Defence*, European Network and Information Security Agency (ENISA), 2011, y Zheng Bu, *et al., The New Era of Botnets*, McAfee, 2010.

[5] Meulenbelt, Stephanie, "The 'Worm' as a Weapon of Mass Destruction: How to respond legally to Cyber-warfare?", *The RUSI Journal*, 157, 2, 2012, pp. 62-67; Lucas, Jr., George R., "Postmodern War", *Journal of Military Ethics*, 9, 4, 2010, pp. 289-298; y Eneken Tikk, *et al., International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.

[6] Collins, Sean y Stephen McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications", *Journal of Policing, Intelligence and Counter Terrorism*, 7, 1, 2012, pp. 80-91; Langner, Ralph, *To Kill a Centrifuge*, The Langner Group; y Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2014.

[7] Clarke, Richard A., *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, 2012; Rid, Thomas, *Cyber War Will Not Take Place*, Oxford University Press, 2013; Stone, John, "Cyber War Will Take Place!", *Journal of Strategic Studies*, 36, 1, 2013, pp. 101-108; McGraw, Gary, "Cyber War is Inevitable (Unless We Build Security In)", *Journal of Strategic Studies*, 36, 1, 2013, pp. 109-119; Carr, Jeffery, *Inside Cyber Warfare: Mapping the Cyber Underworld*, California, O'Reilly Media, 2011; y Caplan, Nathalie, "Cyber War: the Challenge to National Security", *Global Security Studies*, 4, 1, 2013.

El tercer evento, las revelaciones en 2013 del ex analista de seguridad informática, Edward Snowden, sobre los programas de ciberespionaje o vigilancia electrónica de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), alertó a la comunidad internacional sobre las capacidades desarrolladas por Estados Unidos para intervenir masivamente los correos electrónicos, servicios de voz, video, chat, fotos, direcciones IP, notificaciones de inicio de sesión, transferencia de archivos y perfiles en redes sociales de cualquiera, incluidos la Canciller alemana Angela Merkel, la mandataria brasileña Dilma Rousseff, el ex presidente Felipe Calderón, y el entonces candidato y ahora presidente, Enrique Peña Nieto.[8]

En este contexto, en diferentes momentos el gobierno mexicano ha implementado medidas para tratar de contener las ciberamenazas, reconocidas desde el 2009 como antagonismos a la Seguridad Nacional en la Agenda Nacional de Riesgos.[9] Asimismo, su inclusión en el actual Plan Nacional de Desarrollo (PND) y el Programa para la Seguridad Nacional (PSN) dan cuenta de la relevancia que ha cobrado el tema para las autoridades.

Hasta ahora, las políticas más notables han sido la Estrategia Nacional de Seguridad de la Información (ENSI), enfocada en los aspectos técnico-administrativos, y la Estrategia de Ciberseguridad de la Policía Federal (PF), centrada en la prevención y combate de la ciberdelincuencia.

Sin embargo, estas iniciativas están lejos de ser soluciones integrales como las que han implementado otros países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) o la Unión Europea (UE).[10] En términos reales, se trata de esfuerzos aislados, como los que venían desarrollando cada una de las entidades de la Administración Pública Federal (APF).

En efecto, la ENSI, además de no haber sido publicada ni difundida lo suficiente tras su adopción –a un año de concluir el sexenio pasado–, presenta un importante retraso en su implementación. Asimismo, sus tres fases de operación (APF; gobiernos locales, poderes Legislativo y Judicial; y sector privado y público en general) no son coherentes con las necesidades, entre las que apremia la creación de un marco jurídico y una cultura de ciberseguridad entre la población. La estrategia tampoco define el tipo de ciberamenazas que enfrenta el Estado, y deja de lado elementos

[8] Greenwald, Glenn, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, 2014; y Peinado, Mari Luz, "Snowden afirma que la NSA tuvo acceso al correo electrónico de Felipe Calderón", *El País*, 20 de octubre del 2013.

[9] "National Strategy for Information Security", Gobierno Federal, Ottawa, Canadá, 2012. http://www.oas.org/cyber/presentations/PresentacionIngl%C3%A9sOttawa-Sin%20tiempo.pdf

[10] Para un estudio comparado de ciberestrategias véase: "Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy", *OCDE*, 2012.

clave como el fortalecimiento de la ciberdefensa y la colaboración con el sector privado.[11]

Por su parte, la estrategia de la PF, institución pionera de la ciberseguridad en México, privilegia de forma natural la atención de la ciberdelincuencia a nivel federal, dejando en segundo lugar la protección de la infraestructura crítica y la información sensible del Estado. De igual forma, no delimita los criterios de colaboración con las Fuerzas Armadas, corresponsables en dichas tareas.

Los vacíos e imprecisiones en las políticas, se deben en buena medida a la tardía discusión de las cuestiones estratégico-organizacionales de la ciberseguridad. Y es que los primeros estudios consistían esencialmente en simples traducciones y revisión de conceptos.[12] Años después, la investigación fue tomando dos vertientes: el aspecto técnico de la Seguridad Informática y la Seguridad de la Información; y el marco jurídico.[13] Aunque, recientemente algunos ya han comenzado a plantear ideas novedosas encaminadas al desarrollo y organización de Equipos de Respuesta de Emergencias Informáticas (CERT, por sus siglas en inglés), e incluso se ha empezado a debatir la viabilidad y pertinencia de crear un cibercomando en el seno de las Fuerzas Armadas.[14]

[11] Gobierno Federal, *op. cit.*

[12] Rosas, María Cristina, "Ciberespacio, Crimen Organizado y Seguridad Nacional", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, 2011.

[13] García Cancino, Jorge Luis, "La importancia de los estándares y su certificación en la seguridad de la información", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, abril-junio 2008; Guadarrama Mendoza, Juan Alexander, "¿Por qué seguir las mejores prácticas de seguridad de la información?", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, abril-junio 2008; Cámpoli, G. A, *Delitos informáticos en la legislación mexicana*, México, Instituto Nacional de Ciencias Penales (INACIPE), 2005; Sosa Alquicira, Gabriela, *Análisis de instrumentos jurídicos en México y propuesta de un nuevo marco jurídico para regular los delitos informáticos*, México, ITAM, 2005; Navarro Isla, Jorge, "Delitos informáticos: México en el contexto mundial", *Tecnologías de la información y de las comunicaciones: aspectos legales*, México, Porrúa/ITAM, 2008, 381-462; Muñoz Torres, Ivonne Valeria, *Delitos informáticos: diez años después*, México, Ubijus, 2009.

[14] Medina Pérez, José G., "Recomendaciones para la creación de un equipo de respuesta a incidentes de seguridad informática", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, 2007; Ávila Ponce de León, Juan Carlos, *Conformación de un grupo de guerra electrónica especializado en ciberguerra para el apoyo a las operaciones navales de la Armada de México*, Centro de Estudios Superiores Navales (CESNAV), Secretaría de Marina-Armada de México, Tesis, 2009; Villalobos Antonio, Roberto Andrés, *Establecimiento de un grupo multidisciplinario de operaciones de información en apoyo a las operaciones navales*, Centro de Estudios Superiores Navales (CESNAV), Secretaría de Marina-Armada de México, Tesis, 2012; Mares Mojica, Roberto, *Ciberguerra: una visión estratégica de Defensa Nacional para las Fuerzas Armadas mexicanas*, Colegio de Defensa Nacional (COLDEF), Secretaría de la Defensa Nacional, Tesis, 2015; Castro Reynoso, Sergio, *Principios de Ciberguerra: Una Guía para Oficiales Militares*, México, Mimeo.

Sin abundar en las nociones teórico-conceptuales del término ciberseguridad, ampliamente discutidas en la literatura, el presente artículo se enfoca en exponer algunos lineamientos que podrían servir de referencia para la formulación de una Estrategia Nacional de Ciberseguridad, como la que otros países han desarrollado, con base en la creación de un marco jurídico robusto; la promoción de buenas prácticas; la formación de especialistas; la colaboración con el sector privado; y el fortalecimiento de la ciberdefensa.[15]

El texto está dividido en dos secciones. En la primera se describe la crisis de ciberseguridad por la que México atraviesa, haciendo énfasis en los principales riesgos y amenazas. Asimismo, se exponen las medidas implementadas por los sectores público y privado para intentar reducir las vulnerabilidades. En el segundo apartado se bosquejan los lineamientos considerados por otros países para formular una Estrategia Nacional de Ciberseguridad que coordine y fortalezca los esfuerzos hasta ahora realizados.

I. La crisis de ciberseguridad en México

En los últimos diez años, el número de internautas y el porcentaje de hogares con acceso a Internet en México se ha incrementado rápidamente. La penetración del servicio ha aumentado 300%, pasando de 12.8 millones de usuarios en 2004 a 53.9 millones en 2014. Este año podría lograrse una cobertura del 53% de la población, concentrada principalmente en el centro y noreste del país (Distrito Federal, Baja California, Sonora y Nuevo León).[16] De este modo, México podría ocupar el segundo lugar con el mayor crecimiento de usuarios en términos absolutos, después de Brasil.[17]

Sin embargo, pese a la adopción de una Estrategia Digital Nacional, que entre otras cosas pretendía potenciar la conectividad, aún queda mucho

[15] Para fines de este artículo se entiende por ciberseguridad "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros, tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios en el ciberentorno". *Unión Internacional de Telecomunicaciones (UIT)*. No obstante, existe un extenso debate en torno a la definición de ciberseguridad. Para conocer algunas aproximaciones véanse: Hansen, Lene y Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly*, 53, 4, 2009; Von Solms, Rossouw y Johan van Niekerk, "From information security to cyber security", *Computers & Security*, 38, 2013, pp. 97-102; Giles, Keir, "Russian Cyber Security: Concepts and Current Activity", *Chatham House*, Conflict Studies Research Center, 2012; y Rubio Reinés, Ó, "Ciberseguridad y Administración Pública", *Universidad Politécnica de Valencia*, Tesis, 2014.

[16] "Estudio sobre los hábitos de los usuarios de internet en México 2015", Asociación Mexicana de Internet (Amipci).

[17] Sánchez Onofre, Julio, "México tendrá 65 millones de internautas en 2015", *El Economista*, 29 de marzo del 2012.

por hacer.[18] Mientras en México 30.7% de los hogares tuvo conexión en 2013 y 35.8% tenía una computadora, en Uruguay la cifras fueron 33.3% y 52.8%; en Argentina 34% y 47%; en Brasil 37.8% y 45.4%; en Chile 35% y 46.8%; y en Costa Rica 33.6% y 45.3%. En América Latina, México sólo superó a Colombia (23.4% y 29.9%), Paraguay (19.3% y 22.7%) y Perú (14% y 23%), aunque en comparación con la OCDE, donde más del 70% de los hogares tiene Internet, el país se ubica en el último lugar junto con Turquía y Chile.[19]

Desafortunadamente, el rápido aumento de la conectividad no ha sido acompañado de una política integral que garantice la protección de los usuarios y la información. Así, año con año México se ha afianzado como uno de los países más vulnerables en términos del número de ataques y costos. En 2011, la compañía rusa de seguridad informática *Kaspersky*, lo colocó como el quinto país a nivel mundial en ciberataques, al concentrar 4% de los incidentes, detrás de Rusia (16%); Ucrania (12%); Tailandia (7%) y Malasia (6%).[20] Un año después, un reporte del *think-tank Security & Defence Agenda* y la compañía *McAfee* situó a México entre los peor preparados en ciberseguridad.[21] Al mismo tiempo, la Organización de Estados Americanos (OEA) y Trend Micro identificaron al país como el principal originador de *spam* o correo electrónico basura en la región.[22] De acuerdo con *Symantec*, ese mismo año, México fue el segundo país de América Latina con mayor afectación (superado por Brasil), al registrar costos de 3 mil millones de dólares (50% más que en 2011), lo suficiente para comprar un *Ipad* a todos los habitantes del Distrito Federal.[23] Finalmente, el Índice Global de Ciberseguridad 2014 de la Unión Internacional de Telecomunicaciones (UIT) identifica a México con un nivel bajo de preparación ante ciberamenazas asignándole 32.4 puntos de 100.[24]

---

[18] Sánchez Onofre, Julio, "Es oficial: existe en México una Estrategia Digital Nacional", *El Economista*, 25 de noviembre del 2013; Lucas, Nicolás, "Estrategia Digital Nacional vivió su primer tropiezo", *El Economista*, 11 de diciembre del 2013; y "AHCIET: Estrategia Digital se encamina al retraso", *El Economista*, 16 de enero del 2014.

[19] INEGI, *op. cit.*

[20] Ángel, Arturo, "Vigila Policía Federal red informática del país", *24 Horas*, 12 de marzo del 2012.

[21] "Cyber-security: The vexed question of global rules", Security & Defence Agenda, McAfee, 2012, http://www.mcafee.com/au/resources/reports/rp-sda-cyber-security.pdf

[22] OEA y Trend Micro, "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", 2013, p. 12.

[23] OEA y Symantec, "Tendencias en la seguridad cibernética en América Latina y el Caribe", 2014.

[24] El *Global Cybersecurity Index* (GCI) evalúa cinco aspectos: marco jurídico, soporte técnico, estructura organizacional, capacitación y cooperación internacional. www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Tabla 1.
Número de usuarios y porcentaje de hogares con acceso a Internet en México

Año	2001	2002	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Usuarios (millones)	7.1	10.7	12.8	16.4	20.2	23.9	27.6	30.6	34.9	40.6	45.1	51.2	53.9	65*
% de hogares	6.1	7.4	8.7	9	10.1	12.3	14.5	16.1	22.2	24.4	26	30.7	38.4**	-

Fuente: INEGI, Amipci, UIT.
Notas: *Estimaciones de Intel y del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC). **Estimación del informe de la OEA y Symantec "Tendencias en la Seguridad Cibernética en América Latina y el Caribe".

Los ciberataques, entendidos como accesos no autorizados a sistemas, interrupción o denegación de su servicio (DoS, por sus siglas en inglés), se han incrementado a un ritmo más que proporcional. En 2012, el aumento fue de 40%; en 2013 de 113% y las cifras preliminares de la PF indican que en 2014 el repunte habría sido superior a 300%.[25]

El 98% de los incidentes en México se lleva a cabo mediante *malware* (*software* diseñado para dañar una computadora), y el resto mediante *phishing* o suplantación de identidad.[26] En 2013 los incidentes de acceso lógico no autorizado aumentaron 260%, las infecciones de *malware* 323% y el *phishing* 409%. En contraste, las intrusiones DoS disminuyeron 16%.[27]

Sin incluir los ataques que de diciembre del 2012 a enero del 2015 afectaron a individuos, 53% fue dirigido contra el gobierno, 26% contra organizaciones académicas, y 21% contra el sector privado.[28]

Entre los afectados hay gobiernos municipales (Guadalajara, Chilpancingo, Acapulco, León), estatales (Puebla, Guanajuato, Tabasco, Querétaro, Guerrero, Nayarit, Quintana Roo), así como órganos federales (como el Consejo Nacional para la Cultura y las Artes [CONACULTA], el Consejo Nacional para Prevenir la Discriminación [CONAPRED], el *Diario Oficial de la Federación* [DOF], el Servicio de Administración Tributaria [SAT], la Presidencia de la República y el Senado).

[25] OEA y Trend Micro, *op. cit.*, p. 8; y OEA y Symantec, *op. cit.*, p. 68.

[26] Hernández, Lilian, "Más de 45 millones de mexicanos son víctimas de ciberataque", *Excélsior*, 21 de septiembre del 2014.

[27] OEA y Symantec, ídem.

[28] "Fortalece CNS estrategias para la protección del ciberespacio mexicano", *OEM*, 24 de febrero del 2015.

En particular, resultan alarmantes las intrusiones registradas desde el 2003 en los sistemas de instituciones con información sensible, como la Secretaría de Gobernación (SEGOB), la Secretaría de la Defensa Nacional (SEDENA), la Secretaría de Marina-Armada de México (SEMAR), la Procuraduría General de la República (PGR) y la extinta Secretaría de Seguridad Pública (SSP), sustituida en 2013 por la Comisión Nacional de Seguridad (CNS).

En cuanto al sector privado, en 2012 una de cada 10 empresas sufrió un ataque y en 86% de los casos hubo fraudes, modificación de estados financieros y contables, así como robo de información. Un año después, 72% de las firmas se vieron afectadas, particularmente los sectores financiero, de mayoreo y manufactura.[29] En buena medida, esto pudo haberse debido a que apenas la mitad de las compañías mexicanas (52%) capacitan a sus empleados en ciberseguridad, y menos del 1% de los ingresos son destinados a seguridad y administración de riesgos tecnológicos, pues no se percibe un beneficio inmediato, lo cual contrasta con el 5% que invierten las economías desarrolladas.[30]

Las ciberamenazas

Cada país enfrenta diferentes amenazas. Para algunos el principal temor es el inicio de una ciberofensiva que pueda conducir a una confrontación tradicional entre Estados. Para otros, la gran amenaza es padecer atentados ciberterroristas.[31] A unos simplemente les preocupa que su información económica, financiera y tecnológica caiga en manos de potencias extranjeras. En el caso de México, son tres las principales ciberamenazas: la primera tiene una motivación económica, la segunda es además política, y la tercera es una combinación, más un factor narcisista.

La más preocupante, al igual que en el mundo físico, es la ciberdelincuencia, especialmente el robo, el fraude y la difusión de pornografía infantil, debido a su estrepitoso incremento, su elevado costo, y los limitados recursos con los que cuenta el Estado para combatirle.

[29] Las cifras podrían revertirse, ya que 80% de los directivos comienza a invertir en recursos humanos para vigilar la seguridad cibernética y física (especialmente en el sector financiero y de telecomunicaciones), con lo que buscan evitar un costo mayor derivado de un ataque, que por concepto de reparación y recuperación de información podría oscilar entre 15 y 20 mil dólares en un espacio de dos o tres semanas, pudiendo alcanzar los 6.9 millones de dólares como en el caso de la cadena departamental Liverpool, *hackeada* en diciembre pasado. Véanse: Meré, Dayna, "Sufre ciberataques 72% de empresas", *Reforma*, 13 de mayo del 2014; Ruiz, Carolina, "México, preocupado por la ciberseguridad", *El Financiero*, 23 de octubre del 2014; Chávez, Gabriela, "México, 'en pañales' en ciberseguridad", *CNN Expansión*, 13 de mayo del 2014; y Ruiz, Carolina, "Hackeo a Liverpool podría costarle más de 100 mdp, estiman", *El Financiero*, 13 de enero del 2015.

[30] "Exposing the Cybersecurity Cracks: A Global Perspective. Part 2", Ponemon Institute, 2014; y "Afectadas por ataques cibernéticos una de cada 10 empresas en México", *Notimex*, 31 de marzo del 2014.

[31] Chen, Thomas M., *Cyberterrorism after Stuxnet*, Strategic Studies Institute (SSI), 2014.

El ciberespionaje ocupa la segunda posición, ya que México no cuenta con la tecnología, presupuesto ni experiencia que otros países poseen para evitar el acceso a información sensible que podría vulnerar la soberanía nacional. Concretamente, la amenaza se circunscribe a las operaciones de extracción de información política de Estados Unidos y Rusia; las de China, interesada en obtener ventajas económicas; al igual que las de Irán, dirigidas a posicionarse en el sector energético (aun cuando es un importante país productor), en el marco de las reformas estructurales del 2014 que abrieron la puerta a la inversión extranjera.[32]

En tercer lugar se ubica el desafío de colectivos *hacktivistas* como *Anonymous*, *Safety Last Group*, Resistencia Cibernética, Raza Mexicana, Insurgencia Digital, *Mexican Hackers Mafia*, entre otros, cuyos miembros –en su mayoría menores de edad–, poseen los conocimientos necesarios para sabotear las plataformas tecnológicas del Estado e imponer sus agendas.

Ciberdelincuencia

La UIT describe al cibercrimen como "actividades en las que computadoras o redes informáticas son utilizadas como herramientas, blancos o plataformas para la consecución de fines criminales". Por su parte, el Convenio sobre cibercriminalidad del Consejo de Europa, conocido como Convenio de Budapest, adopta una definición más amplia en cuatro dimensiones: 1) ofensas contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos [*hackeo*, *phishing*, espionaje, intercepción, DoS]; 2) ofensas relativas a los contenidos [pornografía infantil, extremismo, apuestas, *spam*]; 3) ofensas mediante el uso de computadoras [fraude, falsificación, robo de identidad], y 4) ofensas contra los derechos de autor y la propiedad intelectual (piratería). Empero, no existe un concepto único que permita una clasificación exacta de los ciberdelitos, los cuales suelen ser combinaciones de tipos y vectores de ataque.

Hasta ahora el estudio del fenómeno se ha realizado a partir de las definiciones y metodologías de compañías como *Kaspersky*, *Symantec*, *Microsoft* y *McAfee*. Esta última, por ejemplo, estima que el costo global de la ciberdelincuencia oscila entre los 400 y los 575 mil millones de dólares, monto superior al ingreso de muchos países y empresas transnacionales.[33] Por su parte, *Symantec* calcula que el costo de los ciberdelitos perpetrados entre julio del 2012 y julio del 2013, ronda los 113 mil millones de dólares (un aumento de 3 mil millones respecto al año anterior), de los cuales 38% fueron pérdidas por fraudes, 24% por reparaciones, 21% por información

[32] Garduño, Silvia, "Ofrece Irán experiencia petrolera", *Reforma*, 4 de diciembre del 2014.

[33] "Net Losses: Estimating the Global Cost of Cybercrime", McAfee, Center for Strategic and International Studies, 2014.

robada y 17% por otros ataques. Durante ese periodo 378 millones de adultos reportaron haber sido víctimas (178 millones menos).[34]

Para el caso de México, la empresa calcula que 71% de los internautas fueron afectados (4 puntos porcentuales menos), una proporción superior al promedio mundial (61%). Así, México se ubicó como el país más vulnerado de América Latina, y entre los primeros a nivel global, detrás de Rusia, China y Sudáfrica. En tanto, las cifras de la PF señalan que de diciembre del 2012 a enero del 2015 se cometieron 59 mil 236 delitos cibernéticos, de los cuales 68% fueron *phishing*, 17% fraude, y 15% *defacement* o remplazo de contenidos por comunicados, quejas, sátiras o amenazas.[35] La cifra contrasta con los 10 millones de víctimas contabilizados por *Symantec* sólo en 2013.

Los delitos más recurrentes son la estafa, el fraude al comercio electrónico (principalmente en telefonía, autos, ropa y accesorios), robo, extorsión, generación y envío de *spam*, difamación, amenazas, robo de contraseñas, así como difusión de pornografía infantil.[36]

El robo se concentra en el sector financiero. Los bancos han llegado a reportar pérdidas anuales de 93 millones de dólares.[37] En 2014 los intentos de robo sumaron 2 millones; al menos cuatro organizaciones fueron vulneradas por troyanos diseñados para interceptar y redireccionar transacciones de banca en línea. A nivel regional, México, Brasil y Colombia han sido los más afectados. Hace poco fue detectada una nueva modalidad de este delito, a través de la extracción directa de cajeros automáticos (ATM), tras infectarlos con el *malware Ploutus*.[38]

El correo electrónico y las redes sociales son la principal vía utilizada para amenazar a los usuarios con publicar material privado, bloquear o suprimir la información del disco duro (a través de *ransomware* como *CryptoLocker*), a cambio del pago de "rescates" que van de los 100 a los 3 mil dólares, una amenaza que sólo en 2012 generó pérdidas por 5 millones de dólares, intensificándose 500% a nivel global en 2013.[39] El *modus operandi* consistía anteriormente en obligar a los usuarios a adquirir un antivirus falso, para eliminar una amenaza inexistente. También estuvo de moda enviar mensajes de parte de una supuesta autoridad (PF,

[34] "Reporte Norton 2013", *Symantec.*

[35] Alvarado, Noel F., "Participa la Policía Federal en la Expo Seguridad 2014", *Notired*, 8 de abril del 2014.

[36] "Comprehensive Study on Cybercrime", United Nations Office on Drugs and Crime (UNODC), 2013; y Organización de Estados Americanos (OEA) y Symantec, *op. cit.*, p. 69.

[37] McAfee, *op. cit.*, p. 15.

[38] *Ibídem.* p. 25.

[39] *Ibídem.* p. 21.

CNS, SAT), "multando" a los usuarios por ingresar a páginas no seguras o con contenido prohibido.

El *ciberbullying* o acoso escolar, el *sexting* o envío de contenidos eróticos, y el *grooming*, hacerse pasar por un menor para atraer a uno y luego causarle un daño, son otros riesgos a los que están expuestos los internautas. Aunque, la principal amenaza es la difusión de pornografía infantil, un delito que genera anualmente ganancias cercanas a los 34 mil millones de dólares, según el Departamento de Seguridad Interior de Estados Unidos (DHS, por sus siglas en inglés).[40]

De acuerdo con el *National Center for Missing and Exploited Children*, México es el principal difusor a nivel internacional. La Asociación *End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes* (ECPAT), coloca el país en la segunda posición como productor y distribuidor.

En 2010 la Fiscalía Especial de la PGR para los Delitos de Violencia contra las Mujeres y Trata de Personas (FEVIMTRA), registró 580 cuentas personales de Internet desde las que se difundían fotografías o videos de explotación sexual a menores, las cuales aumentaron a más de 3 mil en 2011; a 7 mil en 2012, hasta llegar a las más de 12 mil 300 en 2013. La cifra podría incrementarse, pues el Fondo de Naciones Unidas para la Infancia (Unicef), estima que cada mes 100 menores en México son víctimas de redes de pornografía infantil que operan en Internet.[41]

Ciberespionaje

Buenos vecinos

De acuerdo con documentos filtrados a la prensa por Edward Snowden, el ciberespionaje de Estados Unidos contra México y otros países habría sido llevado a cabo por la NSA en el marco del programa de intercepción masiva denominado *Prism*, aprobado en 2007 durante la administración del presidente George W. Bush.[42]

Al menos dos operaciones habrían sido diseñadas para recabar información sobre la lucha contra el narcotráfico, la estabilidad macroeconómica, el comercio internacional, la política exterior, la situación de derechos humanos y las capacidades militares.[43] La primera operación, *Whitetamale*

[40] "México ocupa el primer lugar en difusión de pornografía infantil", *Univision*, 23 de julio del 2014.

[41] Solera, Claudia y Laura Toribio, "Depredador doméstico", *Excélsior*, 11 de agosto del 2013.

[42] Greenwald, Glenn, et al., "Espionagem dos EUA se espalhou pela América Latina", *O Globo*, 9 de julio del 2013.

[43] *Ídem.*

habría penetrado en 2009 los sistemas de la SSP y las comunicaciones de varios funcionarios, llegando a obtener, entre otros datos, diagramas de las estructuras de las agencias de seguridad. La segunda, *Flatliquid*, emprendida en 2010, habría conseguido sustraer más de 260 documentos del correo electrónico del presidente Calderón y sus más cercanos colaboradores.[44]

A unos meses de terminar el sexenio, la NSA incluyó entre sus objetivos al candidato presidencial Enrique Peña Nieto y a nueve de sus asesores. En total, habrían interceptado 85 mil 489 mensajes de texto, así como varias llamadas y correos electrónicos.[45]

La cibervigilancia habría sido llevada a cabo por la unidad TAO (de Operaciones de Acceso "Confeccionadas a la Medida" o *Tailored Access Operations*) –encargada por años de vulnerar los sistemas de China–, desde la Embajada en México y desde las oficinas de la NSA en San Antonio, Texas (donde también se interceptarían datos de Medio Oriente, Cuba y Venezuela).[46]

En febrero pasado, *Kaspersky* reveló la existencia de otro programa de espionaje dirigido contra 42 países, incluido México, iniciado al menos desde el 2001 por un grupo de *hackers* denominado *Equation Group*.[47] Los métodos empleados, que permiten tomar el control de los discos duros de las principales marcas, coinciden con los de los creadores de *Stuxnet* y los de la NSA. Por ello, no se descarta que también se trate de una operación de Estados Unidos.

Osos en el alambre

Con toda certeza Estados Unidos no es el único país que espía a sus aliados. Aunque no existe evidencia de una operación cibernética dirigida por el Kremlin contra "Los Pinos", hay elementos a considerar que vuelven imposible descartar dicha hipótesis.

Históricamente, la Unión Soviética, y luego Rusia, ha buscado afianzar su posición en la puerta trasera de Estados Unidos y el puente hacia América Latina. Las diversas operaciones de inteligencia llevadas a cabo en territorio nacional desde finales de los años 30 dan cuenta de la relevancia

[44] Glüsing, Jens, *et al.,* "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Der Spiegel*, 20 de octubre del 2013.

[45] "Documentos revelam esquema de agência dos EUA para espionar Dilma", *Globo*, 1 de septiembre del 2013.

[46] M. Aid, Mathew, "Inside the NSA's Ultra-Secret China Hacking Group", *Foreign Policy*, 10 de junio del 2013; e "Inside TAO", *Der Spiegel*, 29 de diciembre del 2013.

[47] "Equation Group: Questions and Answers", *Kaspersky*, 2015, https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

para los servicios rusos de tener una representación (резидентура) en México.[48]

Asimismo, en el marco de la recesión por la que atraviesa su petrolizada economía, Rusia podría estar interesada en conseguir información económica, comercial y política que le permitiera ventajas comerciales.[49]

No sería la primera vez que Rusia emprendiera ciberoperaciones, pese a la constante negativa de su *stablishment* de seguridad (силовики) que las atribuye a "patriotas entusiastas" sin vinculación con el gobierno. Los ataques a Estonia no son el único antecedente. La afectación a los sitios gubernamentales de Georgia en 2008, previo al despliegue militar durante el conflicto con el gobierno del presidente Mijaíl Saakashvili es otro ejemplo.[50]

De hecho, los ciberataques siempre han sido parte de la estrategia rusa. En 1998 el coronel Oleg A. Gordievsky, quien desertó en favor de Reino Unido, reveló que la alternativa ofrecida por el gobierno a los cibercriminales condenados era trabajar para el Servicio Federal de Seguridad (FSB, por sus siglas en ruso), agencia a la que el presidente Vladímir Putin recientemente ha encomendado la ciberseguridad nacional.[51]

Las ciberacciones rusas pueden rastrearse incluso hasta 1999 cuando fue descubierta la operación *Moonlight Maze*, en la cual se sustrajo información clasificada del Pentágono, la Administración Nacional de Aeronáutica y del Espacio (NASA, por sus siglas en inglés), centros de investigación, y otras entidades.[52]

Tampoco debe ignorarse el sólido capital humano con el que Rusia cuenta, herencia de los programas de formación soviéticos que enfatizaban la enseñanza de ciencias exactas, dominadas por la mayoría de los miembros de su comunidad *hacker* (хакеры).[53]

---

[48] Cedillo, Juan Alberto, *Eitingon: Las Operaciones secretas de Stalin en México*, Debate, 2014.

[49] "Foreign Spies stealing US Economic Secrets in Cyberspace", Office of The National Counterintelligence Executive, 2011, p. 5.

[50] Markoff, John, "Before the Gunfire, Cyberattacks", *The New York Times*, 12 de agosto del 2008; y "Overview of the Cyber Campaign against Georgia in August 2008", US. Cyber Consequences Unit, 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

[51] "President Putin orders FSB to protect media sites from cyber attack", *RT*, 21 de enero del 2013.

[52] Vistica, Gregory, "We're in the middle of a cyberwar", *Newsweek*, 20 de septiembre de 1999.

[53] Flook, Kara, "Russia and the Cyber Threat", Critical Threats Project, 13 de mayo del 2009.

El ojo del dragón

Los programas chinos de ciberespionaje que por décadas se han enfocado en Estados Unidos, podrían haber puesto también los ojos en México. Para nadie es un secreto que el principal objetivo de Beijíng es conseguir información que le otorgue ventajas económicas, financieras y tecnológicas, especialmente ahora que busca fortalecer su posición en América Latina.[54] Para ello, en los últimos años el gobierno chino no sólo ha recurrido al reclutamiento de expatriados y estudiantes de intercambio, sino, que ha apostado por agresivas campañas de ciberespionaje conducidas por la Sección Tercera (3/EPL) y la Unidad 61398 del Ejército Popular de Liberación (EPL).[55]

Algunos indicadores del interés en México son el intenso cabildeo para la construcción del centro comercial *Dragon Mart* en Cancún, Quintana Roo, y el tren de alta velocidad México-Querétaro, ambos suspendidos por las autoridades.[56] Pero las señales de alerta provienen, sobre todo, de la introducción a las entidades de la APF de toda clase de equipos y servicios tecnológicos de empresas de propiedad estatal, como *China Telecom* y *Huawei*, ésta última vetada en 2012 como proveedor de Estados Unidos, Canadá y Australia por el empleo de *backdoors* o "puertas traseras" a través de las cuales se puede sustraer información.[57]

Igualmente sospechosa resulta la insistencia en formar parte de una asociación público-privada para controlar una red mayorista de telecomunicaciones que el gobierno mexicano desea construir, pese a su ineficiencia. De tener éxito, las empresas chinas podrían captar todo tipo de datos en el espectro de banda de 700 MHz y de otras bandas.[58]

---

[54] Ellis, Evan y Ulises Granados, "La conquista china de Latinoamérica", *Foreign Affairs Latinoamérica*, 2015; y Joseph M. Humire *et al., Iran's Strategic Penetration of Latin America*, Lexington Books, 2014.

[55] Inkster, Nigel, "Chinese Intelligence in the Cyber Age", *Survival: Global Politics and Strategy*, febrero-marzo, 55, 1, 2013, pp. 45-66.
"Exposing One of China's Cyber Espionage Units", Mandiant; y Mark A. Stokes, *et al., The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, 2011.

[56] Vázquez, Jesús, "Suspenden obras del *Dragon Mart* en Cancún", *El Economista*, 24 de junio del 2014; y "Suspenden indefinidamente tren México-Querétaro", *Milenio*, 30 de enero del 2015.

[57] García, Carolina, "El Congreso de EE UU recomienda vetar a Huawei y ZTE", *El País*, 8 de octubre del 2012; Chase, Steven, "Ottawa set to ban Chinese firm from telecommunications bid", *The Globe and Mail*, 10 de octubre del 2012; y "Australia bans China's Huawei from bidding for work on Internet network amid security worries", *The Telegram*, 26 de marzo del 2012.

[58] Tejado Dondé, Javier, "La SCT y la unidad militar 61398", *El Universal*, 10 de febrero del 2015.

La daga persa

De acuerdo con una investigación de la empresa de ciberseguridad *Cylance*, desde el 2012 México habría sido uno de los blancos de *Cleaver*, operación dirigida por Teherán contra la industria militar, energética, aeroportuaria, química, sanitaria, aeroespacial, de telecomunicaciones, manufactura y educativa, de Canadá, Reino Unido, Francia, Alemania, India, Israel, Kuwait, Qatar, Arabia Saudita, Corea del Sur, Turquía, Emiratos Árabes Unidos, China y Estados Unidos.[59]

Aunque no hay registro de la vulneración de sistemas *SCADA*, existe evidencia del robo de información "extremadamente sensible" de muchas infraestructuras críticas, incluida probablemente la paraestatal Petróleos Mexicanos (PEMEX).[60]

Las capacidades ciberofensivas desarrolladas por Irán desde que fue presa de *Stuxnet* no deben ser subestimadas. Las diversas operaciones lanzadas desde o por Irán (*Comodo*, *DigiNotar*, *Shamoon*, *Ababil*, *Saffron Rose* y *Newscaster*) demuestran que se ha convertido en una ciberpotencia a la altura de Rusia y China.[61]

Hacktivismo

Aunque para muchos se trata sólo de jóvenes en busca de publicidad y diversión, el *hacktivismo* se ha convertido en una ciberamenaza para México por lo complejo que resulta su neutralización, debido a su estructura acéfala, su red de apoyo internacional y su capacidad operativa perfeccionada los últimos 15 años. La fuerza acumulada por estos grupos ha sido tal, que en 2011 llegaron a declarar la guerra a "Los Zetas", uno de los cárteles más poderosos en la historia del narcotráfico en México.[62]

El fenómeno *hacktivista* puede ser entendido como un movimiento colectivo, global y emergente que cuestiona el orden social a través de ciberataques dirigidos contra los sistemas de instituciones públicas y privadas, en promoción de diversas causas, orientadas a la construcción de una sociedad más democrática y un Internet libre del control gubernamental.[63]

---

[59] "Operation Cleaver", Cylance, http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

[60] "Petróleo y gas en México, blanco de hackers iraníes", *CNN Expansión*, 2 de diciembre del 2014.

[61] Siboni, Gabi y Sami Kronenfeld, "Developments in Iranian Cyber Warfare 2013-2014", *Military and Strategic Affairs*, 6, 2, 2014, pp. 83-104.

[62] Solís, Víctor, "Anonymous declara la guerra a 'Los Zetas'", *El Universal*, 1 de noviembre del 2011.

[63] Burgos Pino, Edixela Karitza, "El Hacktivismo: entre la participación política y las tácticas de subversión digital", *Razón y Palabra*, 88, 2014.

En su mayoría, los colectivos *hacktivistas* organizan ataques (no siempre coordinados) para ser lanzados en fechas conmemorativas, como celebraciones de independencia (15 de septiembre), días internacionales (de la mujer, del agua, del Internet, etc.) o tomas de protesta de servidores públicos, aunque también actúan en respuesta a situaciones o acontecimientos que consideran atentan contra los valores que promueven, como la aprobación de leyes o la violación de derechos humanos. Los ciberataques suelen ser *DoS* y *defacement*. No obstante, también ha habido robo y filtración de información reservada o confidencial.

De acuerdo con diversos foros y blogs, uno de los primeros grupos en que anidó el *hacktivismo* en México fue "Raza Mexicana", surgido entre estudiantes del Instituto Tecnológico de Puebla en 1996, con la creación de una revista sobre *hacking*, *cracking* y *phreaking*, así como una lista de distribución y el sitio web del grupo. La mayoría de sus miembros eran mexicanos, pero también se incorporaron *hackers* españoles, argentinos y posteriormente de toda América Latina. La consolidación del grupo entre 2000 y 2005, coincidió con una etapa de disputas internas, conflictos de interés, acciones radicales y la dimisión de sus fundadores.[64]

Si bien uno de los miembros de este colectivo, Alejandro Hernández Flores, alias *alt3kx*, se hizo famoso cuando fue detenido por la extinta Agencia Federal de Investigación (AFI), por atacar el sitio de la Presidencia en junio del 2003, Raza Mexicana como agrupación no se vio oficialmente implicada en el *hacktivismo*.[65] Fue el grupo *X-Ploit*, quien protagonizó la mayoría de las demostraciones entre 1998 y 2001, principalmente en defensa del movimiento zapatista.[66]

Actualmente, el colectivo más conocido es *Anonymous*. Surgido en 2003 bajo la máscara de Guy Fawkes y con el lema "Somos legión, no olvidamos, no perdonamos, espéranos", este grupo internacional ha sido responsable de importantes golpes contra empresas y gobiernos de los cinco continentes.[67]

En México sus miembros se han atribuido operaciones contra sitios de instalaciones y servicios públicos (incluido el Aeropuerto Internacional de la Ciudad de México), partidos políticos (PRI, PAN, PRD), autoridades electorales (IFE e institutos locales), gobiernos municipales, estatales y el federal, de los tres poderes de la Unión, así como casas encuestadoras (*Consulta Mitofsky*), medios de comunicación (*Televisa* y *TV Azteca*) e instituciones del sector de Seguridad Nacional como SEGOB, PGR,

[64] "Raza Mexicana", Hack Story, http://hackstory.net/Raza_Mexicana

[65] "Cae hacker que intervenía la página de la Presidencia", *Milenio*, noviembre del 2003.

[66] Hack Story, *ídem.*

[67] Olson, Parmy, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, Little, Brown, 2012.

SEDENA y SEMAR. En estos últimos, la estrategia gubernamental ha sido negar o bien subestimar los ataques, pese a que algunas veces se ha comprometido información sensible, como nombres del personal activo y en situación de retiro.[68]

Entre los motivos de sus ataques destacan el repudio a la violencia e inseguridad en algunas partes del país; la corrupción; la coartación de la libertad de expresión y la aprobación en 2014 de las reformas estructurales en materia hacendaria, laboral, energética, educativa y financiera.

Medidas de contención

Para hacer frente a estas amenazas el gobierno ha implementado en diferentes momentos medidas como la creación de una división especializada en ciberdelincuencia al interior de la PF, la creación de un CERT, la capacitación y equipamiento tecnológico de las Fuerzas Armadas y la creación de un Comité Especializado en Seguridad de la Información (CESI) al interior de la SEGOB.

Patrullaje cibernético

Dependiente de la CNS, la PF es la principal autoridad en materia de combate y prevención del ciberdelito. La primera Unidad de Delitos Cibernéticos surgió en el año 2000 dentro del Sector de Inteligencia de la Policía Federal Preventiva (PFP), con la misión de perseguir los ilícitos cometidos en o a través de Internet, especialmente la pornografía infantil.[69] Tras la reestructuración de la PFP y su transformación en 2009 en PF, y debido al incremento en el número de ciberataques, fue creada una Coordinación para la Prevención de Delitos Electrónicos, responsable del manejo de la respuesta a incidentes, el análisis de pruebas digitales, y la protección de la infraestructura crítica.[70]

Bajo dicha Coordinación en la División Científica de la PF, en mayo del 2010 entró en operación el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), que monitorea 24 horas, los 365 días del año, los dominios públicos y privados con fines de seguridad, prevención e investigación.[71]

---

[68] "Anonymous asegura poseer datos de más de 25 mil militares mexicanos", *Animal Político*, 21 de enero del 2013.

[69] "Unidad de Policía Cibernética y Delitos Contra Menores", PFP, http://www.disc.unam.mx/2005/presentaciones/delitos_menores.pdf

[70] "Reglamento de la Ley de la Policía Federal", *Diario Oficial de la Federación*, 17 de mayo del 2010.

[71] Para conocer sobre los CERT véase: Moira J. West-Brown, *et al., Handbook for Computer Security Incident Response Teams (CSIRTs)*; Carnegie Mellon, Software Engineering Institute, 2003.

El Centro está integrado por cerca de un centenar de agentes capacitados en Estados Unidos, Canadá, España, Colombia, Francia, Países Bajos, Japón y Singapur.[72] Entre los servicios que ofrece se encuentran el análisis, forensia, respuesta y soporte a incidentes; elaboración de auditorías; difusión de alertas; capacitación e intercambio de información con instituciones de los tres órdenes de gobierno, la academia, el sector privado y con 316 CERT de 69 países, en el marco de su adhesión al Foro de Equipos de Respuesta de Emergencias Informáticas (FIRST, por sus siglas en inglés) desde julio del 2011.[73]

Las principales medidas implementadas por la PF son la Estrategia de Ciberseguridad y la firma de un convenio de colaboración con *Microsoft*, mediante el cual es posible acceder a los activos desarrollados por la firma, entre ellos el Centro de Ciberdelincuencia ubicado en Redmond, Washington.[74]

El modelo desarrollado los últimos 15 años por la PF ha servido como base a otras corporaciones locales, como la Secretaría de Seguridad Pública del Distrito Federal (SSP-DF), que en 2013 creó la Policía de Ciberdelincuencia Preventiva, integrada por 30 agentes, quienes además de emitir alertas y bloquear sitios maliciosos –en coordinación con la Unidad de Investigación Cibernética de la Procuraduría del DF–, también imparten capacitación en escuelas, empresas y dependencias.[75] Desde su creación se han recibido mil 334 denuncias, 499 incidentes sociales en internet, 279 reportes de ventas fraudulentas, 250 de contenido inapropiado, 198 de suplantación de sitios web, y 108 reportes de virus.[76]

Una cuarta dimensión de operaciones

Las Fuerzas Armadas fueron la segunda institución en haber puesto en marcha medidas para fortalecer sus capacidades defensivas en el ciberespacio, mediante la capacitación, actualización, desarrollo tecnológico y colaboración interinstitucional.

Entre septiembre del 2013 y julio del 2014, un representante del Grupo de Coordinación y Ciberdefensa de la SEDENA participó en la Segunda Junta de Trabajo de Oficiales de Alto Rango en C4/Ciberseguridad, en

[72] "Fortalece CNS estrategias para la protección del ciberespacio mexicano", *OEM*, 24 de febrero del 2015.

[73] Ángel, *op. cit.*

[74] "Fortalece CNS estrategias para la protección del ciberespacio mexicano", *OEM*, 24 de febrero del 2015; Gómora, Doris, "Microsoft y Policía Federal firman acuerdo contra ciberdelitos", *El Universal*, 8 de mayo del 2014; y Warnick, Jennifer, *Digital Detectives*, Microsoft, http://news.microsoft.com/stories/cybercrime/index.HTML

[75] Jiménez, Gerardo, "SSPDF crea la policía cibernética, para evitar delitos por Internet", *Excélsior*, 4 de abril del 2013.

[76] "La Policía de Ciberdelincuencia Preventiva", *Efekto Noticias*, http://www.efektotv.com/nacional/la-policia-de-ciberdelincuencia-preventiva-especial#sthash.suNQNsaP.dpuf

Colorado, Springs, Estados Unidos. Otros miembros acudieron a Madrid a las jornadas de ciberdefensa realizadas por el Mando Conjunto de Ciberdefensa español.[77]

Asimismo, algunos oficiales visitaron el Cibercomando de Estados Unidos (USCYBERCOM), en Washington, D.C.; y otros más participaron en el "Tercer Taller de Trabajo Técnico de Ciberseguridad" en San Antonio, Texas. En septiembre, personal especializado acudió al seminario "Cyber Endeavor", organizado por el Comando Norte (USNORTHCOM). En noviembre del 2013 se asistió al Primer Encuentro Internacional sobre el Ciberespacio, en Hamburgo. Incluso se enviaron representantes a la "Exposición y Conferencia Internacional sobre Soluciones de Ciberseguridad", realizadas en Tel Aviv.[78]

Otro paso importante encaminado a preparar al personal que eventualmente podría integrarse al Centro de Operaciones del Ciberespacio (COC) –que la SEDENA busca crear durante la actual administración–, es la inclusión de los temas de ciberseguridad en la currícula de la Maestría en Administración Militar para la Seguridad Interior y Defensa Nacional del Colegio de Defensa Nacional (COLDEF).[79]

Por su parte, la SEMAR ha reestructurado y modernizado su Centro de Monitoreo y Respuesta a Incidentes de Seguridad en el Ciberespacio, el cual es controlado por la Subsección de Protección de Infraestructuras de Información, de la Sección Segunda del Estado Mayor General de la Armada (Inteligencia).[80] Asimismo, la Marina ha reforzado su programa de Maestría en Seguridad de la Información, impartido en el Centro de Estudios Superiores Navales (CESNAV), y ha organizado talleres en coordinación con el USNORTHCOM, así como un seminario dirigido al público, realizado en marzo pasado.[81]

Los planes de la SEMAR son de hecho más ambiciosos, ya que, de acuerdo con su programa sectorial, contemplan elaborar un Diagnóstico Institucional de Seguridad de la Información, Ciberdefensa y Ciberseguridad (DISICC); una Estrategia Institucional de Seguridad de la Información, Ciberdefensa y Ciberseguridad (EISICC); además de modernizar su Sistema Integral de Seguridad de la Información; y constituir un Centro de Control de Ciberdefensa y Ciberseguridad.[82]

[77] Veledíaz, Juan, "En marcha la Ciberdefensa", EstadoMayor.mx, 8 de septiembre del 2014.

[78] "Segundo Informe de Labores", Secretaría de la Defensa Nacional (SEDENA), 2014.

[79] "Programa Sectorial de Defensa Nacional 2013-2018", *Diario Oficial de la Federación*, 13 de diciembre del 2013.

[80] "Segundo Informe de Labores", Secretaría de Marina-Armada de México (SEMAR), 2014.

[81] "Seminario Internacional: Seguridad y Defensa en el Ciberespacio", Centro de Estudios Superiores Navales (CESNAV), http://www.cesnav.edu.mx/pdfs/web_trip.pdf

[82] "Programa Sectorial de Marina 2013-2018", *Diario Oficial de la Federación*, 16 de diciembre del 2013.

Con el propósito de reforzar la estrecha coordinación que por primera vez ha caracterizado a ambas secretarías, se han adoptado también protocolos de intercambio de información, alineados a su vez con acuerdos con las áreas de ciberdefensa de las Fuerzas Armadas de Francia y España.[83]

Investigación universitaria a la vanguardia

Las instituciones académicas también han jugado un papel determinante en el fortalecimiento de la ciberseguridad. Probablemente la Universidad Nacional Autónoma de México (UNAM) ha sido la que más ha contribuido a través del establecimiento del UNAM-CERT en 2001, adscrito actualmente a la Coordinación de Seguridad de la Información (CSI) de la Dirección General de Cómputo y Tecnologías de Información y Comunicación.[84]

Dicho CERT, que colabora de cerca con el CERT-MX, proveedores de servicios, gobiernos estatales y CERT privados (como el inaugurado por Telmex en septiembre del 2014), está encargado de proveer respuesta a incidentes, así como de publicar boletines, alertas sobre vulnerabilidades, y realizar investigaciones para mejorar la seguridad de los sitios. Asimismo, el Centro evalúa soluciones como *antivirus*, *antispam*, *firewalls*; realiza auditorías y pruebas de penetración, entre otras asesorías que le reportan ingresos.[85]

Una más de sus contribuciones ha sido la concientización y formación de personal especializado, a través de la difusión en foros académicos desde el 2011, y su programa de becarios, en el que se ha formado cerca del 60% de su personal.[86]

Hacia una estrategia

Buscando responder a las amenazas en el ciberespacio, en abril del 2010 el Consejo de Seguridad Nacional (CSN) ordenó la conformación de un Grupo Técnico Intersecretarial Especializado en Seguridad de la Información (GTECSI), dividido en un subgrupo técnico y otro legal, para coordinar el desarrollo de la ENSI, aprobada en diciembre del 2011.[87]

Este grupo, transformado un año después en el Comité Especializado en Seguridad de la Información (CESI), tiene entre sus responsabilidades: 1) monitorear y asesorar a las entidades de la APF en la implementación del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad

[83] Veledíaz, *op. cit.*

[84] Aquino Luna, Rubén, "Equipos de Respuesta a Incidentes: Experiencias y Retos", Subdirección de Seguridad de la Información UNAM-CERT, Dirección de Telecomunicaciones.

[85] *Ídem.*

[86] *Ídem.*

[87] Gobierno Federal, *op. cit.*

de la Información (MAAGTICSI), en vigor desde el 2012;[88] 2) proponer reformas al marco jurídico para alcanzar los estándares requeridos por la Convención de Budapest; 3) presentar iniciativas de ley sobre ciberdelincuencia; 4) crear una Unidad Especializada responsable del desarrollo de la política pública en tres fases; 5) impulsar la participación activa en materia de ciberdelincuencia, y 6) concientizar a la sociedad sobre las buenas prácticas de seguridad de la información.[89]

No obstante, el incremento en el número de ciberataques y las pérdidas generadas demuestran que las medidas adoptadas hasta ahora no han sido suficientes. Para potenciar su alcance es necesario alinearlas a una Estrategia Nacional, enfocada no sólo en los procedimientos técnicos de resguardo de la información como la ENSI, sino también en la prevención y respuesta a incidentes, a través de una estrecha coordinación inter e intrainstitucional que evite la duplicación de funciones, la disparidad de presupuestos, y defina responsabilidades en caso de crisis.

II. Una estrategia nacional de ciberseguridad

La elaboración de una Estrategia Nacional de Ciberseguridad, como la que han implementado Estados Unidos (2003), Alemania (2005), Reino Unido (2009), Corea del Sur, Francia, Argentina, Colombia (2011), Bélgica, Suiza, Noruega (2012), Panamá, España, (2013), Kenia (2014) y otros países, debe fundamentarse en al menos cinco ejes: 1) la adopción de un marco jurídico robusto; 2) la promoción de una cultura de ciberseguridad y buenas prácticas; 3) la formación de personal especializado; 4) la colaboración con el sector privado, y 5) el fortalecimiento de la ciberdefensa.[90]

Es importante tener en cuenta que el diseño de la estrategia solamente es un primer paso hacia el desarrollo de una capacidad de pronta recuperación frente a ciberataques (resiliencia). Al mismo tiempo se requiere fijar un responsable de la implementación y monitoreo, el cual enfrente costos políticos reales en caso de retraso o incumplimiento, pues cuando depende de varios actores, no depende de nadie en realidad. Se requiere

[88] El MAAGTICSI define las políticas de seguridad de la información de todas las agencias del gobierno federal, la metodología de identificación de infraestructuras críticas y análisis de riesgos. Asimismo, establece los criterios para la creación del CERT al interior de cada agencia, así como el protocolo de coordinación con el CERT-MX. Véase: Miranda, Horacio, "Nuevo MAAGTIC y Seguridad Pública", *PolíticaDigital.com.mx*, 1 de febrero del 2012.

[89] "APEC Counter Terrorism Action Plan: Mexico", Counter-Terrorism Working Group Meeting, 2012 y 2014. http://mddb.apec.org/Documents/2015/CTWG/CTWG1/15_ctwg1_013.pdf

[90] La UIT propone hasta diez ejes: 1) la rendición de cuentas; 2) un coordinador nacional de ciberseguridad; 3) una Agencia Nacional de Ciberseguridad; 4) un marco jurídico; 5) un marco administrativo de referencia; 6) un CERT; 7) una cultura de ciberseguridad; 8) cooperación pública-privada; 9) capacitación, y 10) cooperación internacional. Véase: Wamala, Frederick, "The ITU National Cybersecurity Strategy Guide", *Unión Internacional de Telecomunicaciones (UIT)*, 2011.

además presupuestar recursos para cada dependencia involucrada. De lo contrario, la estrategia podría convertirse en una lista de buenos deseos, como ha sucedido con la Estrategia Digital Nacional.

Un marco jurídico robusto

Lo más apremiante es crear una ley única que establezca tipos penales para cada conducta delictiva en o a través del ciberespacio, como la que en su momento implementaron Chile (1993), Venezuela (2001), Argentina (2008), Colombia (2009), Costa Rica (2012), Perú, Brasil (2013) y otros países con menor incidencia ciberdelictiva.[91]

Actualmente, sólo algunos ciberdelitos son punibles, aunque no siempre se encuentran explícitamente tipificados y su fundamento está disperso en distintos ordenamientos, en su mayoría del orden federal, lo que complica su procesamiento a las autoridades.

Por ejemplo, el artículo 16 de la Constitución estipula la inviolabilidad de las comunicaciones y la protección de los datos personales. Por su parte, el Código Penal Federal sanciona la interrupción, interferencia e intervención de comunicaciones electrónicas (Arts. 167, Fracc. VI, y 177); el almacenamiento y difusión de pornografía infantil a través de medios electrónicos (Arts. 202 y 202 Bis); el acceso ilícito a equipos y sistemas de informática (Art. 211 Bis 1-7); y la creación de programas para desactivar la protección de otros (Art. 424 Bis).

En tanto, la Ley Federal del Derecho de Autor regula la copia, alteración y reproducción de *software* y bases de datos (Título IV, Capítulo IV). La Ley Federal de Protección al Consumidor (Arts. 18 Bis y 76 Bis), regula el envío de publicidad no deseada (*spam*), y establece los derechos en las transacciones a través de medios electrónicos. La Ley Federal de Instituciones de Crédito tipifica la alteración, copia o reproducción de la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquier instrumento de pago (Art. 112 Bis, Fracc. IV y VI). También sanciona el uso, obtención, transferencia o disposición indebida de fondos (Art. 113 Bis).

El acceso no autorizado a bases de datos con información personal está sancionado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. La Ley Federal de Telecomunicaciones y Radiodifusión (Art. 298, Inciso B, Fracc. I; D, Fracc. III y V), pena el bloqueo del servicio de Internet; la intercepción de la información transmitida en redes públicas; y la no adopción de medidas para garantizar la confidencialidad y privacidad de las comunicaciones.

[91] Glickhouse, Rachel, "Fighting Cybercrime in Latin America", Americas Society / Council of the Americas. http://www.as-coa.org/articles/explainer-fighting-cybercrime-latin-america

Recientemente ha habido otros esfuerzos aislados, como la definición de los conceptos "ciberespacio", "cómputo en la nube" y "ciberseguridad" en el Acuerdo en el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la APF.

Sin embargo, muy pocas legislaciones locales contemplan la sanción de ciberdelitos. El Distrito Federal, Estado de México, Jalisco, Nuevo León, Colima y Quintana Roo son pioneros en la regulación de algunas conductas. Empero, la necesidad de una ley es patente en las diversas iniciativas y propuestas de reforma presentadas desde el 2004 para regular el *hacking*, *cyberbullying*, el envío de *spam*, entre otros cibercrímenes.[92]

Una futura Ley no sólo debe tipificar claramente cada delito y sus vectores de ataque, sino también definir el procedimiento para que la autoridad pueda acceder a la información en posesión de proveedores de servicios en el curso de alguna investigación.

Igualmente, deben fijarse mecanismos para que las compañías reporten a sus clientes y a la autoridad (quizá al CERT-MX) los ataques que comprometan información reservada o confidencial. De esta manera se incentivaría, por una parte, el reforzamiento continuo de la ciberseguridad mediante la libre elección de las empresas que mejor resguarden los datos. Por otra parte, se contribuiría a reducir la dependencia de las estadísticas elaboradas por compañías cuyo único fin es la venta de soluciones de seguridad, a partir de una contabilidad más precisa de los incidentes.

Al mismo tiempo, para evitar la transferencia directa de los costos a las compañías, podrían estipularse obligaciones básicas a los usuarios en caso de querer iniciar algún procedimiento legal, como comprobar el uso de antivirus. Así, todas las partes serían corresponsables: las compañías de resguardar y reportar; el gobierno de contabilizar, analizar y sancionar; y los usuarios de navegar protegidos.

En conformidad con las medidas de austeridad implementadas durante la actual administración, la alternativa más eficiente sería evitar la creación de un ente regulador o supervisor, aprovechando las estructuras existentes al interior de la PF, las Fuerzas Armadas y el CSN, aunque designando

[92] Véanse, por ejemplo: Propuesta de Ley Federal que regula el Correo Electrónico, presentada por el diputado Jorge Legorreta del Partido Verde el 29 de septiembre del 2004, http://gaceta.diputados.gob.mx/Gaceta/59/2004/sep/20040930.html; Propuesta de reformas y adiciones a diversas disposiciones de la Ley Federal de Protección al Consumidor, del Código Penal Federal y de la Ley Federal de Telecomunicaciones en materia de la remisión masiva de mensajes no solicitados (SPAM), presentada por el diputado Julio César Córdova Martínez del PRI el 21 de abril del 2005, http://gaceta.diputados.gob.mx/Gaceta/59/2005/abr/20050421-II.html; y Proyecto de Decreto que reforma y adiciona diversas disposiciones al Código Penal Federal, en materia de delitos en contra de medios o sistemas informáticos, presentada por los diputados Juan José Guerra Abud y Rodrigo Pérez-Alonso González del Partido Verde el 29 de noviembre del 2011, http://gaceta.diputados.gob.mx/Gaceta/61/2012/mar/20120328-III.html

un responsable directo. Esto evitaría además una migración masiva de personal especializado, como sucedió en el año 2000 con personal del Centro de Investigación y Seguridad Nacional (CISEN) tras la creación de la SSP y la AFI.[93]

Una cultura de ciberseguridad

El 57% de los usuarios en México tiene menos de 35 años, y permanece en línea diariamente un promedio de seis horas y 11 minutos, principalmente accediendo a redes sociales, realizando búsquedas o consultando su correo electrónico, ya sea desde su domicilio, trabajo, escuela o algún café Internet, –sobre todo a través de conexiones *Wi-Fi*–.[94]

Sin embargo, la mayoría no es consciente de los riesgos y amenazas a los que está expuesto, y tampoco conoce las medidas básicas para protegerse. Según la Asociación Mexicana de Internet (Amipci), 31% de los cibernautas ignora las medidas de seguridad para realizar transacciones en Internet y 14% no sabe cómo utilizarlas. Entre los pocos que toman precauciones, la mayoría recurre a antivirus (66%), aunque no necesariamente los mantiene actualizados; *firewalls* (48%); anti *spam* (35%); programas anti espías (29%); y actualizaciones del sistema operativo (24%).[95]

El problema es mayor si se toma en cuenta que cada vez más personas navegan desde dispositivos móviles, como *smartphone* y *tablet*, sin ningún tipo de protección. El 54% de los usuarios desconoce que existen aplicaciones de seguridad para sus equipos, y sólo dos de cada cinco tienen un *software* básico de seguridad.[96] El año pasado unos 16 millones de dispositivos a nivel mundial fueron infectados, un incremento del 25% respecto a 2013.[97]

Para reducir la exposición a los riesgos, es indispensable llevar a cabo una extensa, coordinada y permanente campaña de difusión de alertas y buenas prácticas (Tabla 2), mediante acciones de bajo costo dirigidas al usuario promedio, como cursos y talleres en centros educativos, y a través de redes sociales *(Facebook, Twitter, YouTube)*. Su diseño podría basarse en la Campaña Nacional de Prevención contra el Delito Cibernético, emprendida desde el 2008 por la SSP, la cual llegó a impactar a entre 90 mil y 143 mil personas, principalmente menores de edad.[98]

[93] Parte de este proceso de transferencia de capital humano es descrito en Borges, Tomás, *Diario de un agente encubierto*, Temas de Hoy, 2013.

[94] Amipci, *ídem.*

[95] "Estudio sobre la Banca en Línea", Asociación Mexicana de Internet (Amipci), 2013, https://www.amipci.org.mx/es/estudios

[96] Symantec, *ídem.*

[97] Posada García, Miriam, "Infectados, unos 16 millones de dispositivos móviles en 2014", *La Jornada*, 23 de febrero del 2015.

[98] "Tercer y Cuarto Informe de Labores", Secretaría de Seguridad Pública (SSP), p. 52 y 53, respectivamente, http://www.ssp.gob.mx/portalWebApp/wlp.c?__c=fbf

Dicha campaña sería coordinada por el responsable de la Estrategia Nacional de Ciberseguridad, y puesta en marcha por la PF en colaboración con la Academia, para la impartición de cursos, conferencias y seminarios a nivel superior; así como el sector privado, que impartiría talleres, financiaría eventos, además de ofrecer descuentos y entrevistas en medios de comunicación. El desempeño de este programa podría ser medido en función del incremento en la proporción de los usuarios que implementan buenas prácticas, a través de una encuesta aplicada en asociación con la Amipci.

Tabla 2.
Buenas prácticas de ciberseguridad para usuarios promedio

• Instalar *firewalls*, sistemas de detección y prevención de intrusos, así como barreras anti *phishing*.	• Evitar descargar información contenida en correos electrónicos de origen dudoso o desconocido.
• Privilegiar el uso de aplicaciones seguras de proveedores certificados.	• Respaldar periódicamente la información en medios físicos alternos (CD, USB, etc.).
• Activar actualizaciones automáticas o actualizar el *software* una vez por semana.	• Instalar filtros parentales, para evitar que menores accedan a contenidos inapropiados, y supervisar su navegación.
• Evitar transacciones que requieran ingresar usuario y contraseña (inicio de sesión) en computadoras públicas.	• No publicar en redes sociales información o imágenes que permitan identificar el estatus socioeconómico o el entorno familiar.
• Utilizar contraseñas con caracteres alfanuméricos, mayúsculas y minúsculas, con símbolos especiales, que no contengan datos personales (fecha de nacimiento, RFC, CURP, etc.), y modificarlas al menos cada tres meses. El grado de seguridad de la contraseña debe estar en función del tipo de información a resguardar.	• Configurar la privacidad de las cuentas de redes sociales para que sólo usuarios conocidos puedan ingresar al perfil.

Fuente: Elaboración propia.

Formación de especialistas

El siguiente elemento necesario es contar con policías, peritos, ministerios públicos, jueces, abogados y administradores públicos especializados en las cuestiones técnicas, legales y estratégicas de la ciberseguridad.

Para ello, sin tener que crear más burocracia, de manera similar a la Iniciativa Nacional para la Educación en Ciberseguridad (NICE, por sus siglas en inglés), establecida en Estados Unidos, el responsable de la implementación de la estrategia nacional, en coordinación con las instituciones académicas del sector de seguridad, COLDEF, CESNAV, la Escuela de Inteligencia para la Seguridad Nacional (ESISEN), el Instituto Nacional de Ciencias Penales (INACIPE) y el Instituto Matías Romero, junto con el Sistema Integral de Desarrollo Policial (Sidepol), la UNAM, empresas y expertos independientes, podrían conformar un grupo de trabajo en el cual se presenten propuestas de planes y programas de formación que capturen las necesidades de cada dependencia y del mercado laboral.

Al mismo tiempo debería buscarse incrementar la formación en el extranjero mediante el apoyo de socios estratégicos, como Estados Unidos, Reino Unido, Francia, España, Estonia, Corea del Sur y Japón, cuyo apoyo abarca casi todos los gastos de los participantes, excepto transportación.[99]

Otra propuesta en materia de formación es la adhesión a los estándares internacionales de certificación en seguridad informática y de la información (pruebas de penetración, *hackeo* ético, etc.), los cuales homologan las habilidades de los expertos, y liberan al gobierno y a las empresas de la necesidad de realizar evaluaciones propias. Esto incentiva la actualización permanente, por cuanto los especialistas buscan obtener credenciales que les garanticen movilidad y permanencia en el mercado laboral. En este sentido, valdría la pena establecer como requisito la obtención de dichos certificados para los responsables de la ciberseguridad en cada dependencia.

Invertir en capital humano es una inversión a mediano plazo, bien sea para su aprovechamiento nacional o incluso para su exportación a países como Estados Unidos donde, en el corto plazo, podrían beneficiarse de la escasez de personal capacitado, pudiendo lograr, dependiendo de las capacidades, una remuneración promedio de entre 200 y 250 mil dólares anuales.[100]

Asociación público-privada

En el ciberespacio tanto el gobierno como las empresas están expuestos a riesgos y amenazas. Ambos actores podrían beneficiarse de sus experiencias, a partir de una estrecha y estructurada colaboración. Por

[99] Hernández, Cristina, "Capacita Corea a SSP en ciberdelitos", *Reforma*, 1 de octubre del 2014.

[100] Evans, Karen y Franklin Reeder, *A Human Capital Crisis in Cybersecurity*, Center for Strategic and International Studies (CSIS), 2010.

ejemplo, una de los sectores de los que más podría aprenderse es del financiero, pues lo sensible de sus transacciones y su reputación siempre en juego, le han obligado a reforzar sus medidas de ciberseguridad. A cambio del conocimiento generado, las empresas podrían recibir información oportuna sobre ataques a sitios gubernamentales y otras industrias, producida en el CERT-MX o por alguno de sus socios internacionales. Incluso podría considerarse la realización de *hackeos* éticos mutuos con el propósito de identificar vulnerabilidades.

Sin duda éste sería el mejor escenario. No obstante, existen pocos incentivos a intercambiar información. Si una empresa reporta al gobierno o anuncia públicamente que posee cierta vulnerabilidad, o que ésta fue explotada, su posición en el mercado podría verse perjudicada. De manera que la mayoría de los incidentes en realidad nunca son reportados.

Algunas alternativas para generar confianza y fomentar el intercambio de información podrían ser la creación de un esquema de incentivos fiscales o de un mercado de compra y venta de información sobre vulnerabilidades y mecanismos de seguridad entre empresas y gobierno.[101]

Ciberdefensa

Las Fuerzas Armadas mexicanas atraviesan por una etapa dual. Por una parte, se promueve la formación y capacitación en ciberseguridad, en el marco de un extenso plan de modernización. Aunque, por otra, se reflexiona con cautela acerca del papel que debe desempeñarse en el ciberespacio, una interrogante a la que en otras latitudes han respondido con el reconocimiento de una cuarta dimensión de operaciones (el ciberespacio), y creando grupos de élite para atacar o defender en una ciberguerra.[102]

Estados Unidos, China, Rusia, Venezuela (2010), Brasil, Colombia (2011) y España son pioneros en la conformación de un cibercomando, unidad rápidamente adoptada por otros países. Así, cuando en la mayoría de los Ejércitos se haya conformado dicha unidad, México no tendrá otra alternativa que hacer lo propio, tal y como sucedió con la incursión en operaciones de paz de Naciones Unidas.

Por ello, el verdadero debate nacional no debe ser si es oportuno crear un cibercomando, sino cuál debería ser su estructura, sus responsabilidades,

[101] Rosenzweig, Paul, *National Security Threats in Cyberspace*. American Bar Association Standing Committee on Law and National Security & National Strategy Forum, 2009, http://www.americanbar.org/content/dam/aba/migrated/natsecurity/threats_in_cyberspace.authcheckdam.pdf

[102] Algunas reflexiones sobre la creación de un cibercomando en México pueden hallarse en: Ávila Ponce de León, *op. cit.*; Villalobos Antonio, *op. cit.*; y Mares Mojica, *op. cit*.

bajo qué circunstancias sería operativo, qué respuesta se daría a cada tipo de ataque (*rules of engagement*), el perfil de sus integrantes y el presupuesto que se requeriría.

Una forma en que esta unidad podría constituirse sería modificando el artículo 56 de Ley Orgánica del Ejército y Fuerza Aérea para crear una nueva arma, lo cual requeriría la intervención del Congreso, casi siempre enfocado en temas coyunturales. Otra manera sería adicionando al artículo 103 un "cuerpo especial" de ciberseguridad. En el caso de la Marina no habría necesidad de reformas a la Ley, pues su artículo 43, fracción IV, contempla otros cuerpos "que sean necesarios a juicio del alto mando".

Empero, la forma más sencilla de constituir un cibercomando es creando un grupo de coordinación intersecretarial (SEDENA-SEMAR), integrado por ingenieros en sistemas y/o comunicaciones, con un mando rotativo, el cual refuerce la cooperación interagencial y distribuya equitativamente los costos políticos y económicos.

Las responsabilidades del cibercomando deben apegarse a la misión esencial de las Fuerzas Armadas, por ello, el cibercomando debería ser empleado sólo para proteger los sistemas SCADA de la infraestructura crítica nacional, y las bases de datos con información reservada.

Por otra parte, sin necesidad de profundas reflexiones, y manteniendo la vocación pacifista de México, las reglas de operación podrían adoptarse de las sugeridas por el Centro de Excelencia de Ciberdefensa (CCDCOE, por sus siglas en inglés), de la Organización del Tratado del Atlántico Norte (OTAN), las cuales han sido bien acogidas por buena parte de la comunidad internacional.[103]

Es importante tener presente que un futuro cibercomando debe ser plenamente operacional, es decir, debe poseer capacidades ciber-ofensivas. De otro modo, no sería más que un CERT constituido por ingenieros militares, para dar respuesta, básicamente, a incidentes domésticos contra los sistemas sólo de la SEDENA y SEMAR.

III. Conclusiones

Durante la última década el número de cibernautas en México se ha incrementado sustancialmente. Sin embargo, a la par no ha sido desarrollada una política integral que garantice la protección de los usuarios y la información. Así, año con año el país se ha colocado como uno de los más vulnerables a nivel internacional en términos del número de ataques y los costos asociados.

[103] "Tallinn Manual on the International Law Applicable to Cyber Warfare", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2013. https://ccdcoe.org/tallinn-manual.html

De manera particular, México enfrenta tres ciberamenazas. La más preocupante es la ciberdelincuencia, especialmente el robo, el fraude y la difusión de pornografía infantil. La segunda es el ciberespionaje de Estados Unidos, Rusia, China e Irán, quienes buscan extraer información política, económica y comercial, sobre todo en materia energética. En tercer lugar está el desafío de colectivos *hacktivistas* como *Anonymous*, los cuales poseen las capacidades necesarias para irrumpir en los sistemas del Estado e imponer sus agendas.

Las medidas diseñadas para mitigar los riesgos no han sido suficientes. Por ejemplo, la ENSI ha estado centrada en los aspectos técnico-administrativos de la seguridad de la información. Por su parte, la Estrategia de la PF, ha dado mayor peso a la prevención y persecución de ciberdelitos. Sin embargo, ninguna de ellas ha tomado en cuenta los ámbitos de la ciberdefensa y la colaboración con el sector privado.

Por ello, resulta indispensable diseñar una Estrategia Nacional de Ciberseguridad bajo un enfoque integral, como la que otros países han implementado desde el 2003, a partir de cinco ejes.

El primero, la creación de una ley que tipifique todo tipo de conductas lesivas en el ciberespacio. El segundo, la difusión entre la población de buenas prácticas que reduzcan su exposición al riesgo, como el uso de antivirus, *firewalls* y contraseñas robustas, a través de una campaña nacional en centros educativos y redes sociales. En tercer lugar, la formación de personal especializado en los aspectos técnicos, jurídicos y estratégicos de la ciberseguridad, a partir de planes y programas diseñados por instituciones académicas del sector de Seguridad Nacional, como el COLDEF, CESNAV, ESISEN y el INACIPE. El cuarto eje consiste en la construcción de acuerdos de cooperación con el sector privado para el intercambio de información sobre vulnerabilidades, incidentes y mecanismos de seguridad, con base en incentivos fiscales o económicos. El último eje es el fortalecimiento de la ciberdefensa, a partir de la creación de un cibercomando conjunto con plenas capacidades ofensivas y defensivas.

La efectividad de ésta o cualquier otra estrategia dependerá esencialmente de la asignación de recursos y el nombramiento de un funcionario responsable, expuesto a costos políticos reales derivados del retraso o incumplimiento. Asimismo, es importante tomar en cuenta los tiempos políticos antes de presentar una iniciativa de ley o propuesta de reforma, ya que justo ahora el gobierno tiene otras prioridades.

Además, habría que considerar que para llevar a buen puerto cualquier política en la materia, en primera instancia debe contarse con el apoyo del titular del Ejecutivo, el cual actualmente apuesta por la Estrategia

Nacional Digital, y en tanto no resulte exitosa, tendrá muy poco interés en emprender cualquier ciberodisea.

Bibliografía

Asociación Mexicana de Internet (AMIPCI), "Estudio sobre los hábitos de los usuarios de Internet en México 2014", https://www.amipci.org.mx/es/estudios

Ávila Ponce de León, Juan Carlos, *Conformación de un grupo de guerra electrónica especializado en ciberguerra para el apoyo a las operaciones navales de la Armada de México*, Centro de Estudios Superiores Navales (CESNAV), Secretaría de Marina-Armada de México, 2009.

Burgos Pino, Edixela Karitza, "El Hacktivismo: Entre la participación política y las tácticas de subversión digital", *Razón y Palabra*, 88, diciembre 2014-enero 2015.

Cámpoli, G. A, *Delitos informáticos en la legislación mexicana*, México, Instituto Nacional de Ciencias Penales (INACIPE), 2005.

Caplan, Nathalie, "Cyber War: the Challenge to National Security", *Global Security Studies*, 4, 1, 2013.

Carr, Jeffery, *Inside Cyber Warfare: Mapping the Cyber Underworld*, California, O'Reilly Media, 2011.

Castro Reynoso, Sergio, *Principios de Ciberguerra: Una Guía para Oficiales Militares*, México, Mimeo.

Clarke, Richard A., *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, 2012.

Collins, Sean y Stephen McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications", *Journal of Policing, Intelligence and Counter Terrorism*, 7, 1, 2012, pp. 80-91.

García Cancino, Jorge Luis, "La importancia de los estándares y su certificación en la seguridad de la información", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, abril-junio 2008. http://www.cesnav.edu.mx/pdfs/revista/revistas_completas/2008-2.pdf

Guadarrama Mendoza, Juan Alexander, "¿Por qué seguir las mejores prácticas de seguridad de la información?", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, abril-junio 2008. http://www.cesnav.edu.mx/pdfs/revista/revistas_completas/2008-2.pdf

Guitton, Clement, "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?", *European Security* 22, 1, 2013, pp. 21-35.

Hare, Forrest, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective", 4th International Conference on Cyber Conflict, Tallin, OTAN, 2012. https://ccdcoe.org/publications/2012proceedings/2_5_Hare_TheSignificanceOfAttribution.pdf

Healey, Jason, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, The Atlantic Council's Cyber Statecraft Initiative, 2012, http://www.atlanticcouncil.org/en/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace

Hunker, Jeffrey, *et al., Role and Challenges for Sufficient Cyber-Attack Attribution*, Institute for Infrastructure Protection (I3P), Dartmouth College, 2008, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf

Instituto Nacional de Estadística Geografía e Informática (Inegi), "Estadísticas a propósito del día mundial de Internet", 2013, http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/contenidos/estadisticas/2014/Internet0.pdf

Kostadinov, Dimitar, *The Attribution Problem in Cyber Attacks*, Infosec Institute, 2013, http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/

Langner, Ralph, *To Kill a Centrifuge*, The Langner Group. http://www.langner.com/en/resources/papers/

Mares Mojica, Roberto, *Ciberguerra: Una visión estratégica de Defensa Nacional para las Fuerzas Armadas mexicanas*, Colegio de Defensa Nacional (COLDEF), Secretaría de la Defensa Nacional, 2015.

Martínez López, Mario, "Marco teórico para la formulación de una Estrategia Nacional de Seguridad de la Información". *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, 3 y 4, 2009, p. 46.

McGraw, Gary, "Cyber War is Inevitable (Unless We Build Security In), *Journal of Strategic Studies*, 36, 1, 2013, pp. 109-119.

Medina Pérez, José G., "Recomendaciones para la creación de un equipo de respuesta a incidentes de seguridad informática", *Revista del Centro de Estudios Superiores Navales (CESNAV)*, Secretaría de Marina-Armada de México, 2007. http://www.cesnav.edu.mx/pdfs/revista/revistas_completas/2007-4.pdf

Meulenbelt, Stephanie, "The 'Worm' as a Weapon of Mass Destruction: How to respond legally to Cyberwarfare?" *The RUSI Journal*, 157, 2, 2012, pp. 62-67.

Muñoz Torres, Ivonne Valeria, *Delitos informáticos: diez años después*, México, Editorial Ubijus, 2009.

Navarro Isla, Jorge, "Delitos informáticos: México en el contexto mundial.", *Tecnologías de la información y de las comunicaciones: aspectos legales*, México, Porrúa/ITAM, 2008, pp. 381-462.

Organización de Estados Americanos (OEA) y Symantec, "Tendencias en la seguridad cibernética en América Latina y el Caribe", 2014. http://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends

——— y Trend Micro, "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", 2013. http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf

Rid, Thomas, *Cyber War Will Not Take Place*, Oxford University Press, 2013.

——— y Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, 38, 1-2, 2015, pp. 4-37. http://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.977382

Rosenzweig, Paul, *National Security Threats in Cyberspace*. American Bar Association Standing Committee on Law and National Security & National Strategy Forum, 2009, http://www.americanbar.org/content/dam/aba/migrated/natsecurity/threats_in_cyberspace.authcheckdam.pdf

Rudner, Martin, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge", *International Journal of Intelligence and CounterIntelligence*, 26, 3, 2013, pp. 453-481.

Sosa Alquicira, Gabriela, *Análisis de instrumentos jurídicos en México y propuesta de un nuevo marco jurídico para regular los delitos informáticos*, México, ITAM, 2005.

Stone, John, "Cyber War Will Take Place!" *Journal of Strategic Studies*, 36, 1, 2013, pp. 101-108.

United Nations Office on Drugs and Crime (UNODC), "Comprehensive Study on Cybercrime", 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Villalobos Antonio, Roberto Andrés, *Establecimiento de un grupo multidisciplinario de operaciones de información en apoyo a las operaciones navales*, Centro de Estudios Superiores Navales (CESNAV), Secretaría de Marina-Armada de México, 2012.

Warner, Michael, "Cybersecurity: A Pre-history", *Intelligence and National Security*, 27, 5, 2012, pp. 781-799.

Wheeler, David A., *et al., Techniques for Cyber Attack Attribution*, Institute for Defense Analyses, 2003.

Zetter, Kim*, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2014.