# PANORAMA GENERAL DE LA CIBERSEGURIDAD INTERNACIONAL Y NACIONAL

Antonio Berdeja Rivas

Ignacio Olivares Linares

## INTRODUCCIÓN

Hoy hablar sobre temas referentes a la Ciberseguridad en México nos obliga a realizar una revisión de los casos y los probables autores de estos sucesos, no sólo para conocer y adoptar los muy sofisticados sistemas de seguridad, sino también para estar preparados ante ataques que cada vez serán más poderosos y con consecuencias graves. Particularmente porque México se encuentra en una posición débil tanto en materia tecnológica como legal.

De ser verdad que, muchos de los poderosos hackers del ciberespacio están obedeciendo a intereses políticos que en el fondo son una guerra silenciosa contra las grandes corporaciones no sólo del ámbito tecnológico, sino también financieras y principalmente, contra las grandes potencias del mundo occidental. Si bien es cierto que a finales de los años 80s terminó la denominada guerra fría, surgieron nuevos esquemas de lucha por el poder global, en este sentido las nuevas tecnologías de la información, junto con las redes sociales, han jugado un papel fundamental. La información sigue siendo un elemento clave de poder, los datos intangibles se han convertido en grandes tesoros mundiales, y la idea de apoderarse de ellos o destruirlos es la nueva guerra fría o soft (suave) de estos últimos años.

Tan sólo hace una semana los medios de información daban cuenta del ciberataque más grande ocurrido en los últimos 10 años. Pablo David Livsit calificó así este episodio: “Un ataque cibernético golpeó a algunos de los gigantes de internet y afectó las operaciones de varios sitios como Twitter, Netflix, Spotify, The New York Times y The Guardian.

“El ciberataque contra el proveedor de infraestructura de internet Dyn interrumpió el servicio en importantes firmas afectando sobre todo a usuarios en la Costa Este de Estados Unidos.

“No quedó claro quién es el responsable. Funcionarios dijeron que el Departamento de Seguridad Nacional y la Oficina Federal de Investigaciones (FBI) están investigando “todas las posibles causas” del ataque.

“Los sitios de Airbnb, Spotify, Soundcloud, The New York Times, The Guardian y Vox Media también se vieron perturbados en sus servicios.

“Por otro lado, aunque los investigadores expertos en seguridad se apresuraron a ponerlo en duda, seguidores de WikiLeaks también se atribuyeron el ataque: el grupo Anonymus dijo que estaba detrás del ‘apagón’, indicando que lo hacía en respuesta a la decisión del gobierno de Ecuador de cortar el acceso a internet a Jualian Assange, fundador de WikiLeaks.” [3]

Sin embargo, días después se publicó la siguiente información en otros medios de información digital: “La empresa china Hangzhou Xiongmai, fabricante de webcams y reproductores DVD, se ha responsabilizado de la caída masiva de internet ocurrida el pasado viernes (21 de octubre).

“A través de un comunicado, los representantes de la compañía explicaron que sus productos habían sido infectados con el malware Mirai, el causante del ciberataque, para ser utilizados en el ataque contra los servidores DNS de Dyn.

“Con el ataque a los servidores, se generó la caída de sitios como Twitter, Amazon, Spotify y Netflix, entre otros. El problema fue ocasionado debido a que los usuarios de las cámaras web no hicieron el cambio de la contraseña preestablecida.

“Buscando evitar un ataque similar, Hangzhou Xiongmai pedirá a los usuarios devolver los primeros productos que estaban disponibles en Estados Unidos, mientras que para los productos hechos antes de abril de 2015 se liberará un parche que solucionará el problema de seguridad.

[3] Pablo David Livsit, periodista con un posgrado en Periodismo Digital, su portal informativo se denomina “Tecnología sin Fronteras”.

“Aunque la solución propuesta por Hangzhou pretende solucionar una parte del problema, esto no evitaría que se vuelva a repetir un escenario similar a futuro. Días antes del ataque, fue publicado en la red el código de hackeo Mirai, desde ese entonces, expertos en seguridad informática han rastreado varios intentos de reactivarlo. El proveedor de servidores Dyn aseguró que al menos 10 millones de direcciones IP estuvieron relacionadas con el ataque.”

Aunque el pasado 23 de octubre, el diario digital paraguayo La Nación, publicó que “El grupo de hackers ‘New World Hackers´, distribuidos en China y Rusia, se adjudicó la responsabilidad por el ataque al proveedor de internet Dyn. Mediante un mensaje de Twitter, ´New World Hackers’ explicó que el ciberataque se hizo a través de las redes de computadoras ‘zombies’ (como refrigeradores y lavadoras inteligentes, y otros enseres hoy dotados de sistemas de cómputo) que lanzaron en simultáneo 1,2 terabits de datos por segundo a los servidores gestionados por Dyn, firma que ofrece servicio en EEUU a compañías como Twitter, Spotify y medios de comunicación como CNN y The New York Times.

Al respecto los atacantes, de acuerdo a dicha nota informativa, dijeron: “No hicimos esto para atraer a los agentes federales, sólo para probar nuestro poder”, así lo declararon dos miembros del grupo de piratas informáticos, identificados como “Profeta” y “Zain”.

Así este ataque fue tan sólo hace unos días y aunque no ha habido mayor información que permita ratificar o acusar a dichos personajes y confirmar si la empresa china fabricante de cámaras web fue la responsable de este grave “descuido”, lo cierto es hoy estar cada vez más atentos a estos sucesos para que a partir de ellos podamos encontrar una posición de equilibrio para nuestro país. Es decir, se debe crear mayor conciencia en los usuarios de estas tecnologías en nuestro país, puesto que los atacantes sólo están esperando un descuido o una provocación para que de inmediato inicie un ataque.

Javier Arreola, hace unos meses escribía para Red Forbes “¿qué es la ciberseguridad y qué tan importante es? La seguridad cibernética (o ciberseguridad) se refiere a la protección de las computadoras, redes, programas y datos contra el acceso o modificación no deseada o no autorizada. Para ello se

utilizan herramientas, políticas, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, conceptos de seguridad, mejores prácticas e incorporación de tecnologías (Danilak & Thomas, 2016).

Areola informaba que el valor en juego de la información es cada vez más grande. De acuerdo con Brand Financer, de los 71.0 billones de dólares (trillions, en inglés) que concentran las 58 mil compañías más valiosas del mundo, 37.5 billones –más de la mitad– son activos intangibles como propiedad intelectual o información que están almacenados en computadoras. Más aún, el Foro Económico Mundial espera que robustecer la protección en contra de los riesgos cibernéticos podría añadir hasta 22 billones de dólares (trillions, en inglés) a la economía antes del 2020. (Jessop & Kerber, 2015)."

Coincidimos con Arreola cuando indica que desafortunadamente, como consecuencia del siempre cambiante y complejo entorno tecnológico, de los inevitables descuidos humanos, y de la continua sofisticación de los ciberataques, no existe alguna protección infalible para estar 100% seguros en la internet. Ni las compañías más grandes del mundo, ni los gobiernos de las economías más grandes podrán evitar ser víctimas de ataques cibernéticos.

Ya en el año 2015 algunos expertos en la materia visualizaban que conforme las organizaciones y los países engrosan sus defensas digitales, los cibercriminales siguen desarrollando maneras más sofisticadas y elaboradas de poder penetrar hasta las infraestructuras tecnológicas más robustas. Además hoy se está generalizando la idea de que algunos de los ciberatacantes son parte de programas del gobierno, es un hecho que a cualquier compañía le va a resultar imposible prevenir un ataque cibernético desarrollado con los casi ilimitados recursos del gobierno. Esta idea de Arreola, nos hace recordar lo que en los años 70 y 80s cuando era creciente los ataques terroristas, que se trataba de un Terrorismo de Estado, es decir se sospecha de la abierta participación de gobiernos en estos operativos, cuyo efecto era doblemente magnificado al tener como cámara de resonancia a los medios de comunicación.

Para el caso de los ciberataques, la razón puede ser porque criminales, terroristas y países que quieren dañar a otros individuos, organizaciones y naciones han

comprobado que es más sencillo hacer daño al adversario atacando vía cibernética que de manera presencial. Es decir, como sosteníamos al inicio, los tesoros intangibles son el blanco favoritos de ellos.

Tan sólo el año pasado, refiere el propio Arreola, 594 millones de personas en el mundo fueron víctimas de la ciberdelincuencia, lo cual ha orillado a varios gobiernos a tomarse en serio el asunto. Pero el continuo cruce de fronteras tecnológicas y los dilemas éticos que este tema presenta hacen que los gobiernos participen igualmente en la protección de ataques cibernéticos a sus ciudadanos e instituciones, que desarrollen programas de hackers cuya función es romper encriptaciones de países adversarios o espiar la actividad en línea de ciudadanos considerados sospechosos.

Por ejemplo, el presidente estadounidense ha creado la posición de "Jefe de Seguridad Informática de la Casa Blanca", quien se encargará de endurecer la seguridad informática interna de las agencias federales, así como de modernizar los sistemas de tecnologías de la información del gobierno federal. También ha establecido la Comisión Nacional para la Mejora de la Ciberseguridad, que hará recomendaciones de acciones que se puedan tomar la próxima década para proteger la privacidad y mantener la seguridad pública, así como otros datos de seguridad nacional. Todas estas acciones son parte del Plan Nacional de Ciberseguridad, que en caso de que lo apruebe el Congreso, expandiría el presupuesto del rubro a 19 mil millones de dólares. (Calmes, 2016)

Por otro lado, el mismo Congreso estadounidense acaba de aprobar la controvertida Ley de Seguridad Cibernética e Intercambio de Información (CISA, por sus siglas en inglés), bajo la cual se compartiría información privada de ciudadanos con compañías contratistas, agencias de investigación, espionaje y criminalidad, y se seguiría a ciudadanos sospechosos de cometer delitos. Esta ley fue combatida fuertemente por los cabilderos de Amazon, Apple, Dropbox, Google, entre otras empresas tecnológicas. (Caldwell, 2016)

En años recientes, el Ejército Popular de Liberación (PLA, por sus siglas en inglés) de China ha invertido grandes recursos en su departamento especial de ciberinteligencia, que no solamente realiza vigilancia y espionaje avanzado, sino

que posee malware capaz de destruir infraestructura de interés nacional como redes de distribución eléctrica e hidráulica en el extranjero. (Stone, 2013).

Con respecto a Rusia, se sospecha que tiene ciberarmas aún más avanzadas que las del gobierno chino. La milicia rusa también cuenta con unidades especiales dedicadas al ciberespionaje, que además de hacer espionaje para robar secretos de otros países, complementan a su ejército en ataques de guerra. En el 2014, Rusia utilizó ataques de denegación de servicio distribuido (DDoS, en inglés) para apagar las comunicaciones móviles de Ucrania, previo a comenzar un ataque tradicional de campo de batalla (Weedon & Galante, 2014).

Cabe destacar que el Servicio Federal de Protección ruso compró en 2013 cientos de máquinas de escribir que se usan para salvaguardar las comunicaciones entre el Kremlin y el presidente. El objetivo es evitar la fuga de documentos, ya sea por parte de su personal o por parte de hackers. Cada máquina de escribir ha sido modificada para que tenga un patrón único que permite identificar rápidamente los documentos que produce. Eso sí, este sistema no está exento del robo o fotografía de papeles, ni de incendios. (Irvine, 2013)

Al ser un país emergente con una amplia población, México ha incrementado significativamente su acceso a banda ancha e internet. Es preocupante que los cibercrímenes han crecido aún más rápido, y un factor clave es la pobre educación cibernética de la población y sus organizaciones. De acuerdo con estimaciones de Symantec, el 40% de los internautas mexicanos, unas 54.9 millones de personas, ha sufrido al menos un crimen.

De ellos, el 58% de los delitos son suplantación y robo de identidad, seguidos por el 17% por fraudes y el 15% por hackeo. Todo esto convierte a México en el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica. De acuerdo con la Comisión Nacional de Seguridad, en los últimos 5 años, el 53% de los ataques fueron contra dependencias gubernamentales, 26% contra recintos académicos y 21% contra el sector privado. (López, 2016)

**¿Qué es el robo de identidad?**

Cuando alguien roba tu información personal y financiera, con la finalidad de suplantar tu identidad para obtener beneficios de forma fraudulenta, se dice que comete robo de identidad.

Tus datos pueden ser utilizados para solicitar créditos o usar los que ya tienes de forma exagerada, crear cheques falsos con tu número de cuenta e incluso obtener a tu nombre algún documento oficial. Cuando esto sucede, no sólo pierdes dinero, también se daña tu reputación financiera. Si solicitan un crédito a tu nombre sin que te des cuenta y por consiguiente nunca se paga, esto dañará tu historial crediticio y es probable que en el futuro las instituciones financieras te nieguen algún crédito. En casos más graves puedes tener problemas con las autoridades, derivados de algún fraude o infracción que el ladrón cometa a tu nombre.

Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada y cuando se percatan del fraude, el ladrón ya ha hecho estragos.

En México, el delito de robo de identidad va en aumento día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria.

Comúnmente, el delito de robo de identidad se usa de manera ilegal para abrir cuentas de crédito, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos, para el cobro de seguros de salud, vida y pensiones. Al respecto se debe escuchar las diversas recomendaciones que sobre este tema en su oportunidad ha emitido la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

México también es el segundo lugar mundial con más ataques tipo phishing, que es el intento de adquirir información sensible mediante comunicaciones electrónicas. Esto no es de extrañar debido a que apenas el 35% de los mexicanos usan contraseñas seguras y además comparten datos sensibles con

mucha facilidad. Muchas veces nos causa una terrible pereza modificar desde nuestro NIP en los cajeros electrónicos o elaborar contraseñas más complejas para asegurar nuestros datos personales.

La Policía Cibernética, perteneciente al área de seguridad del gobierno, es la principal unidad de combate al cibercrimen. Además, el Instituto Politécnico Nacional cuenta con el único equipo de especialistas digitales forenses en México, así como con el Centro de Investigación en Computación, que desarrolla sistemas para proteger la transmisión de la información digital. (Notimex, 2015)

Dependencias como Gobernación, Seguridad Pública y la Procuraduría General de la República informaron haber sido blanco de ataques orquestados por delincuentes cibernéticos que intentaron y a veces lograron penetrar sus defensas, pese a que hay secretos de Estado en sus redes.

Incluso la Presidencia de la República aceptó no ser inmune y advirtió que el gobierno federal se encuentra en riesgo frente a un “arsenal de armas” virtuales en manos de bromistas así como la delincuencia común y organizada.

Gobernación admitió que los ataques cibernéticos que se han presentado se limitan a peticiones múltiples a los sistemas informáticos, aunque insistió en que este tipo de agresión “no representa un riesgo” para la seguridad informática de Bucareli.

Un total de 106 equipos en la dependencia, que tiene conexiones con áreas tan sensibles como el Centro de Investigaciones sobre Seguridad Nacional (CISEN) y el Instituto Nacional de Migración, han sido infectados con programas dañinos.

En tanto, la Secretaría de Seguridad Pública repuso que en mayo de 2009, registró un récord de 509 ataques a sus servidores, mientras que la Procuraduría General de la República admitió haber detectado una infección con el virus klif, un spyware capaz de retransmitir información de una computadora a otro usuario.

La PGR sostuvo que su información es altamente protegida porque, de ser penetrada por terceros, “la delincuencia puede tener acceso directamente a los bancos de información, a fin de manipular, destruir total o parcialmente y descargar los datos reservados y confidenciales”.

La Presidencia de la República clasificó como reservada por 12 años toda la información referente a ataques a sus servidores, los más visitados dentro de todo el gobierno federal.

En los Pinos argumentaron que dar a conocer información sobre el número de ataques a sistemas informáticos, terminales de cómputo, servidores y redes, así como cuántas computadoras han sido infectadas "comprometería la seguridad y la defensa nacional".

"Esta información se encuentra clasificada como reservada", expuso la Presidencia, que se amparó en los artículos 15, 16 y 17 de la Ley Federal de Transparencia para negar los datos, bajo el argumento de que revelarlos "proporcionaría información respecto de las vulnerabilidades de la red institucional".

Sobre la situación de la Ciberseguridad en México, Daniel Kapellmann y Benjamín Reyes, difundían recientemente que según el reporte "Tendencias de Seguridad en América Latina y el Caribe" de la Organización de los Estados Americanos (OEA), tan sólo en México los costos anuales generados por ciberdelitos en 2014 ascendieron a $3,000 millones de dólares, afectando al sector público, privado y civil. Los riesgos en materia de seguridad cibernética que fueron denunciados incluyen desde malware, phishing y hackeos, hasta incidentes de fraude y extorsión, difamación, amenazas, robo de contraseñas, suplantación de identidad y acoso.

Si bien ya existen esfuerzos a nivel nacional para impulsar este tipo de seguridad, como la creación del CERT-MX (Equipo de Respuesta a Incidentes de Seguridad Cibernética) o la operación de la División Científica de la Policía Federal, entre otras cosas, México aún sigue rezagado en este tema con un creciente impacto negativo. De acuerdo con el "Índice Global de Seguridad 2014" liberado a inicios del año en curso por la Unión Internacional de Telecomunicaciones (UIT), el país cuenta con un bajo nivel de preparación ante ciberamenazas.

Este reporte evalúa la respuesta general de más de 100 países ante la inseguridad cibernética, utilizando una escala de evaluación entre 0 y 100 puntos. De este modo, cada país cuenta con una calificación que puede repetirse,

derivando en un ranking con 29 posiciones, entre las cuales México ocupa la 18, a la par de Perú, Vietnam y Burkina Faso.

México cuenta con una calificación global de 32.4 sobre 100, lo cual implica que se encuentra 12.3 puntos por debajo del promedio global. A nivel Latinoamérica, esto implica que México se encuentra por encima de países como Paraguay y Venezuela, pero muy por debajo de otros como Brasil, Uruguay, Argentina, Costa Rica, Chile y Colombia.

En específico, el Índice Global de Ciberseguridad se centra en cinco principales indicadores o áreas, que son las medidas legales, técnicas, orgánicas, capacitación y cooperación tanto nacional como internacional.

Daniel Kapellmann y Benjamín Reyes, aseveran: “Las principales fortalezas de México se encuentran en las medidas técnicas, mientras que su principal debilidad son las orgánicas. Esto indica que se cuenta con algunas instituciones y marcos técnicos de ciberseguridad, incluyendo equipos contra incidentes cibernéticos, pero se no cuenta con una planificación y estructuras orgánicas que promuevan la implementación de medidas de este tipo de seguridad entre distintos sectores e instituciones.”

Aunado a lo anterior México registra bajos niveles en materia de marcos legales e instituciones encargados de tratar la seguridad en línea, así como en programas de capacitación, certificación, desarrollo de profesionales y certificación de organizaciones de carácter público en esta materia. Este patrón se refleja nuevamente en una falta de mayor desarrollo en materia de marcos para cooperación nacional e internacional y redes de divulgación de información.

Ante esta situación México debe trabajar más en la búsqueda de estrategias articuladas, donde haya una planeación a fondo para hacer de las redes sociales y demás tecnologías digitales, espacios de crecimiento y desarrollo que tanto necesita nuestro país.

Asimismo, debemos alejarnos de blanco concéntrico que buscan los hackers y nuevos luchadores sociales internacionales que buscan la menor provocación para lanzar sus ataques planeados y destructivos. Las razones o sin razones de estos atacantes también es porque buscan decirnos algo que posiblemente no

está bien según la óptica de ellos, debemos agradecer que al menos en lo que va de este Congreso Internacional de Ciberseguridad, no hayamos tenido, ni lo deseamos, al menos un apagón.

Trabajos citados

— Arreola, J. (26 de abril de 2016). Padrón electoral en la nube: ¿ciberproblemas a la mexicana? Obtenido de Forbes México.

— Caldwell, G. (07 de febrero de 2016). Why You Should Be Concerned About The . Obtenido de TechCrunch.

— Calmes, J. (09 de febrero de 2016). Obama's Last Budget, and Last Budget Battle With Congress. Obtenido de The New York Times.

— López, J. (07 de febrero de 2016). Cibercrimen ataca a 40% de internautas mexicanos. Obtenido de El Financiero.

— Danilak, M., & Thomas, D. (23 de marzo de 2016). What is Cybersecurity? Obtenido de Quora.

— Jessop, S., & Kerber, R. (28 de agosto de 2015). Investors still in the dark as cyber threat grows. Obtenido de Reuters UK.

Kapellmann, Daniel & Benjamín Reyes, Retos de Ciberseguridad en México. Obtenido en http://the-ciu.net/nwsltr/381_1Distro.html

— Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum: Technology, Engineering, and Science News. N.p., 26 Feb. 2013. Web. 16 May 2016.

— Notimex. (28 de diciembre de 2015). México, tercer lugar mundial en ataques cibernéticos; equipo de IPN los combate. Obtenido de Aristegui Noticias.

— Office of the National Counterintelligence Executive. "Foreign Spies Stealing US Economic Secrets in Cyberspace." Counterintelligence (n.d.): n. pág., Oct. 2011. Web.

— Stone, Richard. "A Call to Arms." Science Mag 339.6123 (2000): n. pag. 1 Mar. 2013. Web.

— The White House. (09 de febrero de 2016). Fact Sheet: Cybersecurity National Action Plan. Obtenido de The White House Office of the Press Secretary.

— Weedon, Jen, and Laura Galante. "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast. « Executive Perspective." Atom. N.p., 12 Mar. 2014. Web. 17 May 2016.

— Wikipedia. (07 de mayo de 2016). List of cyber-attacks. Obtenido de Wikipedia.

-- www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/Benjamín Reyes