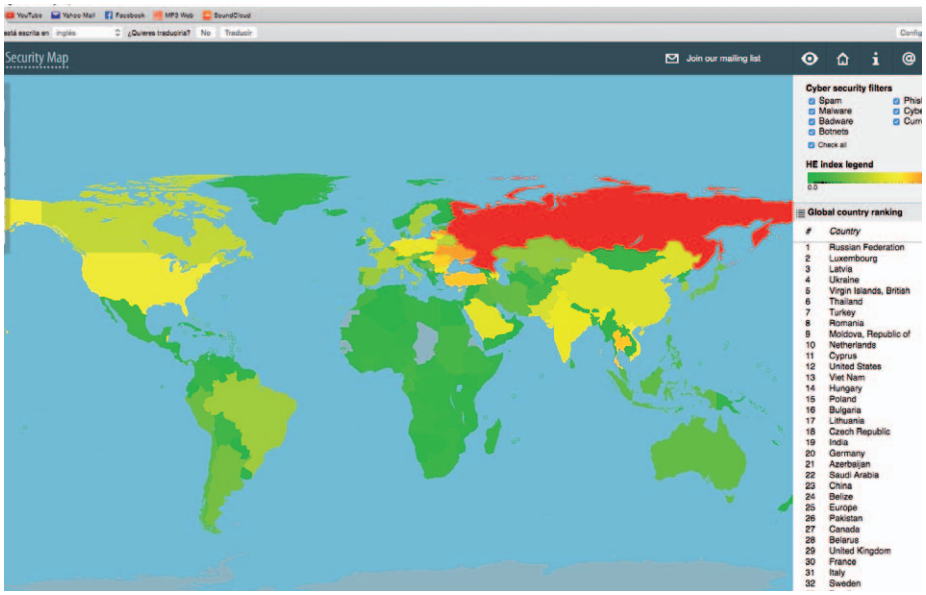
¿Cómo alcanzar la seguridad en **la era del yottabyte?**

Grandes retos técnicos, humanos y legales esperan a los gobiernos, a las empresas y a la comunidad para contrarrestar la ofensiva del crimen organizado, que sigue a la vanguardia de la tecnología, y que va tras un botín de 130.000 millones de dólares.



http://globalsecuritymap.com/

Global Security Map **proporciona un método para visualizar los países con más actividades maliciosas como *malware*, *phishing* y *spam*.**

El *big data* será uno de los mayores desafíos para la ciberdefensa en los próximos decenios, pues aún no existe el software adecuado para procesar zettabytes (10^{21}) o yottabytes (10^{24}) de información. Habrá que desarrollar herramientas para análisis automático de las amenazas, para identificar anomalías y patrones de ataques y preparar a la gente que lidiará con el ciberdelito. Para combatirlo se necesitará inteligencia predictiva y generar instrumentos de apoyo a la decisión para situaciones que mutan a gran velocidad.

Ya se están dando algunos pasos, como las plataformas que funcionan como laboratorios de experimentación real con códigos maliciosos y otras formas de agresión. En España, por ejemplo, se creó un centro de investigación en este tema, donde se estudia con detalle el *malware* y, entre otras operaciones, es posible activar miles de nodos en un polígono y simular el efecto de este tipo de armas en redes públicas. Pero esto implica grandes inversiones en esas infraestructuras —planteadas bajo la idea de investigación, desarrollo y experimentación— y en la buena formación del talento, además de estrategias para evitar la alta rotación del recurso humano. Solo así será posible sincronizarse en una vanguardia tecnológica que permita contrarrestar los riesgos de un enemigo que se ha mostrado muy fuerte y organizado y que, hasta ahora, siempre ha ido a la delantera.

Esto lo dijo el español Samuel Álvarez, director general del Grupo In-Nova, en el 2.° Foro de Ciberdefensa y Ciberseguridad, "Nuevos retos y perspectivas en Latinoamérica". El evento tuvo lugar en la Universidad de los Andes los días 3, 4 y 5 de agosto del 2015, y fue una iniciativa de la Cámara Colombiana de Informática y Telecomunicaciones con la participación del Departamento de Ingeniería de Sistemas y Computación (DISC).

La Interpol también está sintonizada en esta dirección. "Hemos montado un laboratorio forense digital en Singapur —comentó Adrián Eduardo Acosta, oficial de Crimen Digital de la Interpol—. El Centro de Ciberfunción que da soporte operacional es de última generación y dará acceso a bases de datos de inteligencia, suministradas por empresas privadas, para soportar algunas decisiones de Interpol. También permite emitir alertas de notificaciones sobre nuevos modus operandi del cibercrimen e investigar y operar a nivel internacional".

Foto: Viktor Hanacek, picjumbo.com

Se necesitan nuevas herramientas para que la web de la era del *big data* sea segura.

Lo expresado por estos panelistas da cuenta de una realidad distinta a la de los territorios conocidos del crimen y la guerra. "Nos encontramos en un escenario llamado criptodominio, caracterizado por el anonimato, sin certezas ni fronteras definidas —¿cómo puede un Estado actuar contra un indicio para defender su soberanía?—. En estos conflictos asimétricos, con marcados intereses económicos y políticos, se puede hacer mucho daño con pocos recursos. Es un escenario al que cualquiera tiene acceso y está construido sobre una base insegura".

En el contexto empresarial y en tiempos de calma, Wilmer Antonio Prieto, de Intel Security, plantea alinear las estrategias de seguridad con las de tecnología, riesgo, continuidad de negocio y propósitos organizacionales. Y cumplir con unos objetivos de Nación, donde deben actuar la ciberdiplomacia, la ciberdefensa y la cibercomunidad. Y aunque la tendencia del mundo es evolucionar hacia la seguridad virtual, propone, como primer paso, transformar el concepto de seguridad informática en seguridad de la información, ya que hoy se debe velar por la protección de los datos almacenados, transmitidos o procesados.

Esto porque, cada vez se vuelve más corriente que la delincuencia organizada ofrezca en la *deep web* ciertos "servicios": por 200 dólares un *hacker* viola una cuenta de Facebook; por 500 se consigue un ataque de denegación de servicio a una pyme y por 1500 se suplanta la identidad de alguien en Skype. Los dispositivos móviles son el blanco más apetecido. En este crecimiento exponencial de las amenazas, también serán víctimas los objetos conectados en el internet de las cosas: una pulsera o sensor deportivo será susceptible de ser *hackeado*, así como la televisión o cualquier otro aparato.

Para enfrentar a las transnacionales del cibercrimen, conviene que los países se alíen, ya que sus actos pueden involucrar a varias naciones al mismo tiempo. Es decir, aunque el hecho se cometa en Colombia es factible que se origine en otro lugar del planeta. Por ello, actualizar y armonizar las legislaciones (ver Actualizar leyes, clave en la lucha contra un crimen mutante, pág. 41) servirá para castigar a los delincuentes sin que encuentren refugio allí donde haya vacíos en la ley. Para protegernos mejor, también se podrá compartir información sobre riesgos, vulnerabilidades y experiencias de quienes han sido víctimas, pues es una realidad, ya que no hablamos de amenazas locales y las conductas delictivas son reincidentes. Este es un reto para el Gobierno colombiano y así lo dijo la viceministra de Tecnologías y Sistemas de la Información, María Isabel Mejía, quien reconoció que a la región no le va bien en temas de cooperación: "Estamos planeando una agenda para saber qué vamos a pedir a cada país, de acuerdo con sus fortalezas".

> **"En la *deep web* se pueden contratar ciertos "servicios": por 200 dólares un *hacker* viola una cuenta de Facebook; por 500 se consigue un ataque de denegación de servicio a una pyme y por 1500 se suplanta la identidad de alguien en Skype".**
> **Samuel Álvarez**

Las cifras del cibercrimen

Este no es un negocio pequeño, representa 130.000 millones de dólares al año, según datos de IBM, y la Interpol lo equipara

Capacidades del Centro de Experimentación

Experimentación básica: gestión y monitoreo de eventos de seguridad, correlación de eventos, detección de intrusos y control de acceso a datos y redes, sistemas de auditoría de vulnerabilidades y herramientas de *hacking* ético y de parcheo.

Experimentación avanzada: simuladores, sistemas antifuga de datos, análisis forense y sistemas robustos.

Experimentación en nuevas tecnologías: neutralización de *botnets* (robots informáticos), gestión dinámica de riesgos, mitigación de ataques DDoS (denegación de servicio, por sus siglas en inglés) y contra dispositivos de enrutamiento de redes de comunicaciones.

Inteligencia: recolección de información de fuentes abiertas, filtrado de datos y alerta temprana.

Experimentación en ciberarmas: investigación y desarrollo y automatización de *malware*, análisis de vulnerabilidades en software (certificación de desarrollos seguros) y código dañino y utilización de vulnerabilidades (creación de *exploits*).

http://www.interpol.int/Crime-areas/Cybercrime/Activities/Digital-forensics

La Interpol instaló un laboratorio forense digital en Singapur. Su Centro de Ciberfunción, que da soporte operacional, es de última generación y dará acceso a bases de datos de inteligencia.

con el terrorismo y el narcotráfico. Uno de sus objetivos es la pornografía infantil (ver Acciones conjuntas, imprescindibles contra la pornografía infantil, pág. 44). De acuerdo con Inhope (*International Association of Internet Hotlines*), red colaborativa internacional que lucha contra este delito en internet, el término está entre los más requeridos en la web: su búsqueda en el mundo se incrementó en un 63 % del 2013 al 2014. Pero además, las amenazas contra los diversos blancos se han multiplicado por 5 en 18 meses; el 76 % de las compañías las considera cada vez más difíciles de contrarrestar, con el *spear fishing* a la cabeza (71 % de los casos). Los delincuentes tienen más claro lo que persiguen; por eso sus ofensivas son más dirigidas: para suplantarlos y hacer operaciones en su nombre van tras el correo electrónico del que maneja el área financiera de una empresa o de quien tiene los datos y la información de los clientes. Las mipymes, que por lo general no están bien protegidas, son un blanco fácil y frecuente. De acuerdo con Felipe Silgado, de Symantec, 1 de cada 2.2 correos de las empresas pequeñas están expuestos (con un crecimiento de 26 % con respecto al 2013) y 1 de 1.6 en las medianas (30 % de crecimiento).

Además, las fugas de información están asociadas con el robo de dispositivos (58 %). La extorsión digital (*ransomware*) también creció: 45 veces más personas tuvieron problemas en sus tabletas o celulares, que hoy son los más apetecidos: hay registros de más de 200 millones de móviles infectados con mecanismos de APT (*Advanced Persistent Threat*). Uno de los lugares donde con más frecuencia actúa el *malware* es en los aeropuertos, razón por la cual se desaconseja cargarlos allí.

Según Felipe Silgado, el código dañino se incrementa y se adapta: en el 2014 hubo 317 millones, lo que implica 1 millón de nuevas amenazas por día. Los sectores más afectados por megafugas de datos fueron el de la salud, con más millones de registros atacados, en segundo lugar el de *retail* (por compras con tarjetas de crédito), seguido por el educativo y el financiero.

Por otra parte, la identidad de cerca del 12 % de usuarios de redes sociales en América Latina alguna vez ha sido sustituida. Sin embargo, las entidades de Gobierno siguen siendo el principal objetivo: 35 % han sido víctimas de algún ataque. De acuerdo con Álvaro José Chávez, director de la Seguridad Pública e Infraestructura del Ministerio de Defensa, en Colombia, los portales oficiales son un blanco frecuente por fallas en la seguridad y por malas prácticas de implementación y aseguramiento de los sitios web, gubernamentales y privados. Entre los distintos tipos de incidentes de los últimos años, el mayor porcentaje corresponde a vulnerabilidades, lo cual ha permitido a los delincuentes atacar la confidencialidad, la integridad de la información y la disponibilidad de los sistemas que contienen los servicios. "Aunque se ha avanzado en los esfuerzos institucionales, persisten vacíos

> **"Aunque la tendencia del mundo es evolucionar hacia la seguridad virtual, primero hay que transformar el concepto de seguridad informática en seguridad de la información, pues se debe velar por la protección de los datos almacenados, transmitidos o procesados".**
>
> **Wilmer Antonio Prieto**

Aspecto de la mesa de instalación del 2.º Foro de Ciberdefensa y Ciberseguridad, que se llevó a cabo en agosto del 2015. Aparecen, de izquierda a derecha, Luc Dandurand, de la Unión Internacional de Telecomunicaciones; Samuel Alberto Yohai, de la Cámara Colombiana de la Informática; David Luna, ministro TIC; Aníbal Fernández de Soto, viceministro de Defensa, y Yezid Donoso, profesor del DISC.

importantes en la coordinación y desarrollo de actividades en materia de ciberseguridad y ciberdefensa. Resulta preocupante evidenciar que subsiste una debilidad en la difusión, en la concientización y en la generación de una cultura de prevención y acción segura", señala.

En Colombia, la penetración de internet se consolida con cada año que pasa, lo cual ha generado un ecosistema a su alrededor. En el 2015, el 66 % de la población era usuaria, así como el 50 % de los hogares y el 74 % de las mipymes. Este beneficio también amplía el espectro para el accionar criminal. El coronel Freddy Bautista García, jefe del Centro Cibernético Policial, asegura que en el 2014 se hicieron casi 12.000 denuncias que la Policía emplea en "ingeniería forense del *malware* e ingeniería inversa a tabletas y dispositivos a donde ha migrado el código malicioso. El Laboratorio Técnico Forense es el encargado de atender las denuncias de los ciudadanos cuando son víctimas del secuestro de datos en la modalidad de *criptolocker*, secuestro de dispositivos por medio de software con el que el delincuente cifra archivos y computadoras para impedir el acceso de los usuarios a sus sistemas. Si no pagan un 'rescate', las empresas de distintos sectores ven frustrados sus procesos".

Según Lorenzo Villegas-Carrasquilla, de la Cámara de Comercio Electrónico, los ataques de denegación de servicio afectan gravemente el comercio virtual, pues, al contrario del físico, cuando alguien acude a un sitio que no funciona, no vuelve. "Pierdo mi cliente con un clic. Pero además, una página caída refleja una vulnerabilidad y esta persona va a pensar que eso le puede pasar en medio de una transacción con su tarjeta de crédito y no quiere correr ese riesgo. Por eso, para una empresa es importante demostrar que su canal transaccional es robusto".

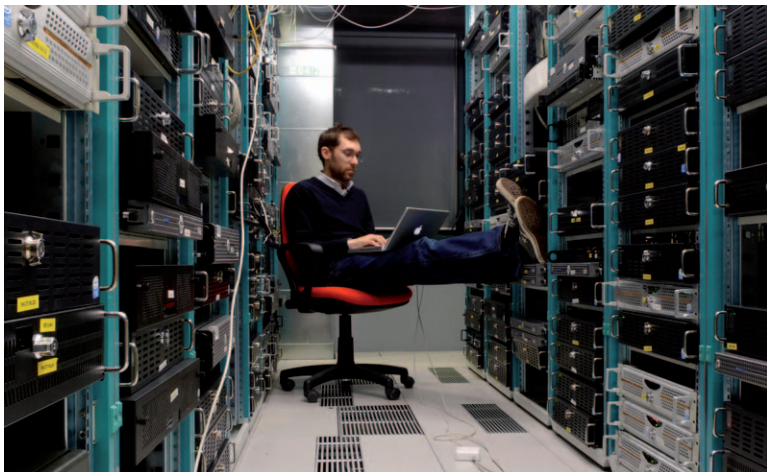
Samuel Álvarez afirma que "nos encontraremos con unas amenazas que nos hacen preguntar si seremos capaces de encontrar vectores de ataque a tiempo, si nuestra inteligencia estará preparada, porque se requiere que sea en tiempo real". ■

Ciberguerra, la próxima confrontación

Con el paso de los años se ve más clara la posibilidad de que un conflicto entre naciones se desarrolle también, o solamente, en el ciberespacio. Una parte de la tarea pendiente es entender cómo es ese escenario. Pero aún hay muchas cuestiones por dilucidar.

Apesar de que en 1993 se mencionó por primera vez la ciberguerra, todavía no hemos vivido una. Sin embargo, dos agresiones entre países son consideradas hitos en esta historia. La primera se registró en el 2007: Rusia atacó y afectó a buena parte de las instituciones gubernamentales y los sistemas financieros de Estonia. La segunda ocurrió en el 2008, en Georgia, y combinó la acción de la ciberdefensa con las fuerzas de artillería y se reconoció el ciberespacio como el quinto dominio de la guerra.

Samuel Álvarez, director general del Grupo In-Nova, hizo un recuento de estos hechos, entre los que las *Advanced Persistent Threat (*APT, amenazas persistentes) se muestran como las más peligrosas y de mayor evolución. Son de bajo perfil y por lo tanto difíciles de descubrir, de tal forma que su accionar puede durar días, meses o años hasta cuando son detectadas.



Leonardo Rizzi, Creative Commons.

Las infraestructuras críticas se vuelven blanco preferido de los ataques en el ciberconflicto. La ciberdefensa debe proteger la prestación y gestión de los servicios TIC.

La primera vez que una nación utilizó un APT fue en el 2007, cuando China atacó los sistemas de las Fuerzas Militares y de la NASA de Estados Unidos. Se conoció como *Titan Rain* y como consecuencia se creó el Mando Conjunto de Ciberdefensa de Estados Unidos al año siguiente. Otro APT muy dañino ha sido *Blackson Yanqui*, que actúa a través de memorias USB y en Estados Unidos causó grandes estragos durante 14 meses.

El director de In-Nova contó que para estas agresiones no se necesita un *malware* muy sofisticado. Para demostrarlo se refirió al caso de *Stuxnet*, que apenas tenía 500 kilobytes: "Es el caso más importante