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".

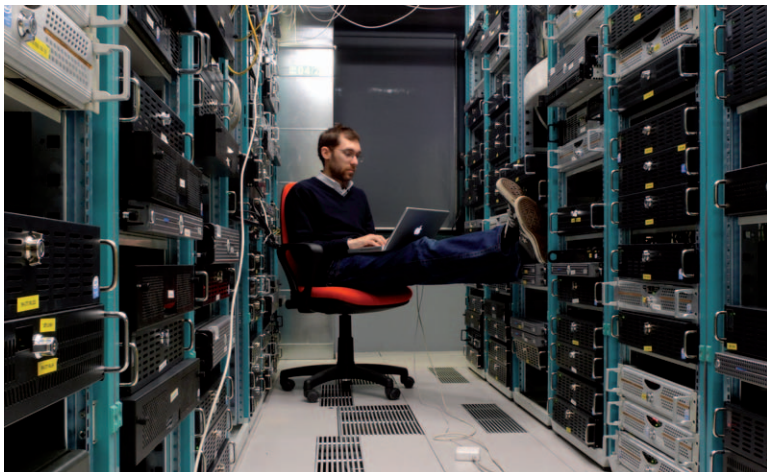
Samuel Álvarez afirma que "nos encontraremos con unas amenazas que nos hacen preguntar si seremos capaces de encontrar vectores de ataque a tiempo, si nuestra inteligencia estará preparada, porque se requiere que sea en tiempo real". ■

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.

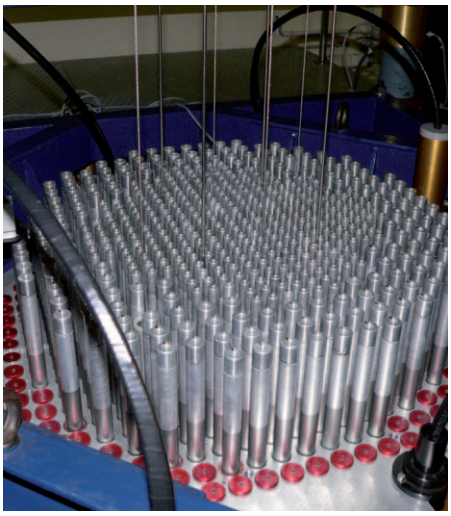
La primera vez que una nación utilizó un APT fue en el 2007, cuando China atacó los sistemas de las Fuerzas Militares y de la NASA de Estados Unidos. Se conoció como *Titan Rain* y como consecuencia se creó el Mando Conjunto de Ciberdefensa de Estados Unidos al año siguiente. Otro APT muy dañino ha sido *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

de ataque a una infraestructura nuclear. La víctima fue Irán, y logró lesionar la producción de energía de sus plantas, algunas de las cuales estuvieron inactivas varios años. *Stuxnet* sigue siendo replicado e imitado. Las infraestructuras en *Scada* (*Supervisory Control And Data Acquisition*) son altamente vulnerables porque trabajan con sistemas operativos anticuados, sin soporte de protección".

Bill Marmie, Creative Commons.

Los sistemas informáticos de la banca surcoreana fueron atacados por Corea del Norte entre el 2011 y el 2013.



Crédito: Foto: Rama CC BY-SA 2.0

El virus Stuxnet infectó los computadores utilizados para el enriquecimiento de uranio de las centrales nucleares de Irán. Comenzó a actuar el primero de febrero del 2009 y causó estragos hasta el 24 de mayo del 2010, cuando por fin pudo controlarse. En la foto, un reactor nuclear.

> **"Stuxnet, que apenas tenía 500 kilobytes, es el caso más importante de ataque a una infraestructura nuclear. La víctima fue Irán y logró lesionar la producción de energía de plantas nucleares, algunas de las cuales estuvieron inactivas varios años".**
>
> **Samuel Álvarez**

Tendencias

- Ciberespionaje.
- Los ataques como servicio.
- Fusión de técnicas y procedimientos utilizados por el ciberespionaje y la ciberdelincuencia.
- Estabilización de los ataques *hacktivistas*.
- Herramientas de ataque para dispositivos móviles (principalmente Android).
- El "secuestro" de organizaciones por ransomware.
- Incremento de los ataques contra cajeros automáticos y procedimientos de pago.
- Ataque contra infraestructuras críticas.

Fuente: Samuel Álvarez, director general del Grupo In-Nova.

El ciberconflicto en teoría

En un ciberconflicto, cada bando desarrolla capacidades para enfrentar al otro en el ciberespacio y determinar cuál será superior en el ejercicio de dominar y controlar. Estas son defensivas, ofensivas, persuasivas (diplomáticas), disuasivas (aún están en investigación) y de inteligencia. Además, la población civil convive con los actores enfrentados. Así lo advirtió Jeimy Cano, director de Seguridad de la Información de Ecopetrol, quien explicó los ámbitos de este nuevo espacio de confrontación.

En el contexto general, la ciberdefensa cruza los cuatro dominios de operación de las Fuerzas Militares: tierra, mar, aire y espacio, atravesado por el dominio ciber con manipulación del espectro electromagnético, degradación y compromiso de la información, engaño deliberado de la contraparte y operaciones psicológicas. En este escenario, las infraestructuras críticas tienen una alta probabilidad de ser impactadas.

En el mundo, las industrias más afectadas son las de petróleo y gas (energía), seguidas por la de defensa. Para llevar a cabo su ofensiva, los atacantes delinean estrategias, lo que produce dos tipos de agresiones: las dirigidas, caracterizadas por una estrategia de poco diseño y un objetivo muy claro, ya sean empresas o países. Y las persistentes avanzadas (APT), que se distinguen por ser muy bien construidas, pero dirigidas a un blanco poco determinado.

Jeimy Cano afirma que aún hay cuestiones por resolver en el ámbito de la ciberdefensa y el ciberconflicto, tales como ¿cuál es la frontera para el desarrollo de las operaciones militares en el ciberespacio?, ¿qué se entiende por un acto de guerra?, ¿ciberinteligencia: cómo balancear los derechos y garantías individuales?, ¿qué se considera una ciberarma y quiénes podrían desarrollarlas? ■