La Ciberguerra en la era Trump

Fuente:
Tomado de Razones de Cuba Raúl Capote

El 20 de septiembre del 2018 el presidente Donald Trump firmó el plan de la nueva Estrategia Cibernética Nacional que oficialmente autoriza al Gobierno estadounidense a realizar ciberataques ofensivos.

«Vamos a hacer muchas cosas de modo ofensivo y creo que nuestros adversarios tienen que saberlo», declaro entonces el ex Consejero de Seguridad Nacional John «Bomba» Bolton en una rueda de prensa. Este documento contribuirá a «garantizar internet seguro»; ahora los órganos competentes podrán «identificar, contrarrestar, desmantelar, degradar y disuadir las acciones contrarias a los intereses nacionales».

Deberán preocuparse, declaró el Consejero de Seguridad Nacional, «las personas que han perpetrado o se están preparando para perpetrar acciones hostiles contra nosotros en el espacio cibernético», y enfatizó que las respuestas a estas agresiones no se limitarían al ciberespacio, sino que se contemplarían, además, respuestas legislativas, sanciones económicas y acciones militares.

En el documento se acusa a Irán, Rusia, China y la República Popular Democrática de Corea (RPDC), entre otros, de usar el ciberespacio como instrumento para agredir a EE. UU. Y Bolton menciona ejemplos de ataques «perpetrados» por Rusia y la RPDC.

Según Associated Press (AP), hackers rusos consiguieron secretos militares de Washington, incluidos los de sus aviones no tripulados y de su tecnología de defensa crítica. El grupo de hackers rastreó al menos 87 personas que trabajaban en ámbitos delicados del sector militar del país como drones, misiles, cohetes y cazas furtivos, entre otros.

La Oficina de Administración de Personal, una agencia independiente del Gobierno de EE. UU., comunicó que los hackers han realizado distintos ataques contra importantes páginas web estadounidenses, entre ellas la red informática del Pentágono, las cuentas de Twitter y YouTube del Mando Central de Estados Unidos (Uscentcom), además de que los piratas robaron los datos de acceso de millones de funcionarios de Estados Unidos, incluyendo a empleados del Departamento de Defensa.

Moscú refutó dichas acusaciones y consideró que se trata de un invento. El Gobierno ruso ha dicho en repetidas ocasiones que las acusaciones son «absurdas» y representan un intento de desviar la atención de los asuntos domésticos de ee. uu. y de su responsabilidad en los ataques realizados contra instalaciones, empresas, unidades militares y civiles, servicios públicos y privados de Rusia, Irán, la RPDC y China.

Quién ataca a quién

El Gobierno estadounidense, sus servicios e instituciones de inteligencia, empresas vinculadas al complejo militar-industrial, desarrollan desde hace un decenio una fuerte ofensiva contra la República Islámica de Irán.

En el 2010, un ciberataque realizado contra una central electronuclear iraní provocó desperfectos en el sistema de enfriamiento de la planta, lo que pudo provocar un grave incidente de consecuencias imprevisibles. Este es considerado el primer ataque informático que produce daños en el mundo físico.

Diversas fuentes aseguran que el virus Stuxnet afectó a las centrifugadoras del sistema nuclear iraní. Una vez dentro de la planta, aumentó la presión de las centrifugadoras hasta hacerlas fallar sin que se detectara, confundiendo a los técnicos que creyeron se trataba de fallos físicos. La intención fue sabotear y retrasar el desarrollo del programa nuclear iraní, existen hoy elementos para considerar que, en el ataque, estuvieron involucrados los servicios especiales estadounidenses e israelíes.

Aunque parezca asunto de ciencia ficción, además de los ataques a las infraestructuras, los cibercriminales pueden atentar directamente contra la vida humana, se pueden hackear marcapasos que tienen función inalámbrica y terminar con la vida de un «enemigo», declararon fuentes cercanas a la CIA.

Según contó al programa de la CBS 60 minutos, en el 2007, el médico del vicepresidente de Estados Unidos durante el mandato de George Bush, Dick Cheney ordenó que se desactivase la función inalámbrica de su marcapasos, por temor a que pudieran hackearlo y acabar con su vida.

FireEye, empresa de investigación en áreas vinculadas a la protección en materia de seguridad cibernética, que está relacionada estrechamente con la CIA, a través de Robert Bigman, ex CISO (director de Seguridad de la información) de esta agencia, con quien ha firmado numerosos contratos para investigaciones sobre el uso de malware, exploits de día cero (ciberataques que se producen el mismo día en que se descubre una vulnerabilidad en el sistema) y tácticas apt (soluciones técnicas a la Amenaza Avanzada Persistente, apt por sus siglas en inglés).

FireEye ha sido señalada como posible responsable de fabricar falsos ataques con el objetivo de señalar a Rusia e Irán como países ciberdelincuentes.

Rusia fue acusada en el 2017 de realizar un ciberataque a nivel global que causó pérdidas de miles de millones de dólares en Europa, Asia y América. «El ataque se extendió rápidamente en el mundo»; en un comunicado el Reino Unido acusó a Rusia de estar detrás de esa agresión cibernética, acusación que fue apoyada por la Casa Blanca.

«Esto no tiene nada que ver con Rusia», declaró de inmediato, durante una visita a China, el presidente ruso Vladimir Putin. «Microsoft lo dijo directamente, que la fuente del virus eran los servicios de inteligencia de Estados Unidos».

Ahora que «nos damos cuenta que un genio ha salido de su botella (…) puede revolverse contra sus progenitores», «(…) es necesario que el tema se trate inmediatamente a un nivel político serio», añadió Putin.

Las operaciones de blackout nacional en Venezuela marcaron una escalada en las nuevas modalidades de la guerra, hubo un ataque cibernético contra el sistema SCADA, software del cerebro electrónico que controla de manera computarizada las funciones de la Central Hidroeléctrica Simón Bolívar de Guri.

El ataque a la Central Hidroeléctrica venezolana fue extremadamente grave, por su alcance y por sus consecuencias humanas y materiales. Pero no es nada nuevo, el plan Nitro Zeus, tenía las intenciones de afectar drásticamente el sistema eléctrico iraní bajo diferentes tipos del sabotaje, incluidos la ciberguerra y operaciones en el terreno, «Nitro Zeus», se creó originalmente bajo la administración de Bush para ser desarrollado plenamente durante la administración de Obama y usarlo contra Irán. El plan estaba dirigido contra las defensas aéreas, los sistemas de comunicaciones y partes cruciales de su red eléctrica.

El ex secretario de la fuerza aérea Thomas Reed en sus memorias «Cerca del Abismo: Una historia de la Guerra Fría (2004)» confiesa que la CIA transfirió de manera encubierta tecnología informática «defectuosa» que provocó la explosión del gasoducto siberiano en 1982, «la explosión y el fuego no nuclear más grande jamás visto desde el espacio». para sabotear la economía de la Unión Soviética e impedir que Europa occidental importara gas natural soviético.

El «terabyte de la muerte» y otras lindezas

El Departamento de Defensa de Estados Unidos ha anunciado repetidas veces que podría producirse, en cualquier momento, un gran ataque cibernético de magnitud desconocida a escala global. El portavoz del Pentágono, Alan R. Lynn, afirmó que hace algunos años recibir un ataque de uno o dos gigas suponía un asunto importante.

«En la actualidad nos estamos enfrentando a ciberataques de 600 gigabytes y a ofensivas cibernéticas que antes no podíamos ni imaginar», precisó.

El Pentágono habla de un eventual efecto masivo de un terabyte (mil gigabytes). «Que se produzca un ataque de ese tipo es solo cuestión de tiempo», ha advertido Lynn.

El 12 de mayo del 2017, el virus extorsionador WannaCry infectó a 200 000 usuarios de más de 150 países. El WannaCry es un programa informático cuyo objetivo es «secuestrar» los archivos de una computadora para posteriormente pedir su «rescate» a los usuarios a cambio de dinero.

«El tamaño del ataque nos hace pensar que tal vez no se trate de lobos solitarios», afirmó a Russia Today el bloguero José Luis Camacho, argumentando que ataques de esta envergadura requieren importante financiamiento.

Parte del código de este virus corresponde a una «ciberarma» de la nsa llamada EternalBlue, según informa Bleeping Computer. Con esta herramienta, el ataque aprovecha una conocida brecha de seguridad del sistema operativo Windows que permite tomar el control de una computadora.

El Plan aprobado justifica los ataques cibernéticos contra supuestos adversarios

Trump derogó la llamada «directiva presidencial 20», un documento confidencial firmado por Obama y que se hizo público en el 2013, cuando el exanalista de la nsa, Edward Snowden, expuso 1,7 millones de archivos sobre los programas de espionaje de EE. UU.

Esa normativa obligaba al Pentágono y a las agencias de inteligencia a obtener el visto bueno de otros departamentos del Gobierno antes de lanzar ataques cibernéticos. Ahora esa puerta ha quedado abierta y el Pentágono recibe el autorizo para actuar de forma agresiva, dejando detrás, según Bolton, «la posición defensiva mantenida hasta ahora».

El documento legaliza los hackeos y ciberataques contra otras naciones. ¿Qué se puede esperar entonces de los expertos en fabricar pretextos, ataques de falsa bandera, autoagresiones, ataques simulados o agresiones permitidas con el fin de lograr oscuros propósitos, como algunos señalan que fue lo ocurrido el 11 de septiembre del 2001?

El plan estadunidense abrió un escenario más de peligro para la paz mundial, la humanidad debe cerrar filas para detener la locura guerrerista que se extiende al ciberespacio.