Escrito por Omar Pérez Salomón | La pupila insomne
Martes, 12 de Marzo de 2019 15:52

Recuerdo que cuando el gusano informático Stuxnet afectó el programa nuclear iraní, muchos no reconocieron la participación estadounidense e israelí. Todo cambió cuando el diario The New York Times hizo público el 16 de enero de 2011, opiniones de expertos militares y de Inteligencia norteamericanos, donde reflejaron que la central nuclear de Dimona (al sur de Israel) se convirtió en un laboratorio para examinar y ensayar el virus Stuxnet que afectó a gran parte del mundo y se reportó en las redes cubanas el 13 de julio de 2010.

Es un hito cómo en la década de 1980 se utilizó por primera vez un arma cibernética, cuando la CIA introdujo un software defectuoso en el sistema de operación del nuevo gasoducto transiberiano que debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia a través de Kazajstán, Rusia y Europa oriental hasta los mercados de divisas de Occidente, causando grandes pérdidas económicas y contribuyendo al colapso de la URSS.

El virus *Stuxnet* puso de manifiesto la debilidad de las infraestructuras críticas de varios países en sectores claves como la Banca, Energía, Información, Telecomunicaciones, Hidráulico, Salud y Transporte; con vulnerabilidades en los sistemas de seguridad informática, de la información y en los programas de vigilancia del tráfico en la red de redes.

En la actualidad las empresas diseñadoras y productoras de hardware, software y sistemas, como
Microsoft
,
IBM
,
Oracle
,
INTEL

y otras, están obligadas, por su participación en los sistemas de gobierno en Estados Unidos y otros países, a introducir los requerimientos de los servicios especiales en el funcionamiento de sus productos, implementando puertas traseras y programas troyanos que actúan como procedimientos almacenados que permiten acceder a los datos y claves de acceso, sin que los usuarios se percaten.

En el artículo, "Venezuela bajo ataque: 7 apuntes sobre el shock eléctrico", publicado en el sitio *Misión Verdad*, se dan a conocer algunos elementos de este sabotaje:

"Esta vez no hubo un ataque a subestaciones o a líneas de transmisión eléctrica, como se había ensayado en distintas ocasiones con anterioridad, según manuales de sabotaje de la CIA contra la Nicaragua sandinista de los 80, ya desclasificados.

"Cabe acotar que el software usado (llamado Scada) en el Sistema de Control Automatizado (SCA) que operativiza el funcionamiento de los motores es el creado por la empresa ABB, que desde hace años no trabaja en el país. Esta empresa ABB, que en Venezuela trabajó como Consorcio Trilateral ABB (ABB Venezuela, ABB Canadá, ABB Suiza), diseñó un proyecto de modernización del Guri a finales de la década pasada, durante el gobierno de Hugo Chávez, en el que describe a profundidad tanto el sistema atacado como la organización básica del Guri.

"El analista geopolítico Vladimir Adrianza Salas, en entrevista con Telesur, relaciona el ataque con el consorcio. Explicó que el embalse del Guri 'requiere un sistema de control que técnicamente se llama sistema scada, el cual no es otra cosa que un sistema de supervisión, control y requisición de datos que permite, desde la perspectiva informática, controlar todos los elementos de generación de energía. Si saboteas esto, saboteas el funcionamiento. Pero para sabotear esto necesitas dos cosas: o debes tener acceso desde afuera o debes tener complicidad interna para modificar los procesos'.

"Precedentes de este tipo se encuentran en países atacados o presionados directamente por Estados Unidos, como Irak y el Líbano, donde los apagones han sido sistemáticos y de forma consecutiva, uno tras otro durante decenas de horas. Las 'réplicas' en la interrupción del suministro de energía responderían a estas secuencias de ofensivas que ya han sido experimentadas en otros contextos de guerra asimétrica e irregular".

En el ataque cibernético a la red eléctrica de Venezuela todos los caminos conducen a EE.UU. De seguro habrá que esperar que el NYT publique la noticia para que se conozca y se crea.

Hay mucho en juego para no estudiar al detalle esta experiencia y adoptar las medidas

necesarias para impedir ataques cibernéticos de esta naturaleza o de otro tipo que sirvan de pretexto para una escalada desde Estados Unidos contra Venezuela.