Mambrú se va a la ciberguerra

ROSA MIRIAM ELIZALDE :: 01/07/2019

El Cibercomando del régimen de EEUU está en zafarrancho de combate

La amenaza ha pasado por debajo de los radares y, con los ecos del último *tweet* de Mambrú o de alguna modelo encuerada en Instagram, no ha habido tiempo para que las sirenas atraigan demasiada atención. Sin embargo, el fantasma que ahora mismo recorre el mundo y que puede tener impacto en todos sus habitantes, es el de la ciberguerra.

El Cibercomando de EEUU está en zafarrancho de combate. Es el autor de los ataques en línea contra los sistemas informáticos de la defensa iraní, que se produjeron el mismo día en que el presidente Donald Trump suspendió una incursión militar en toda regla contra el país islámico. Los pesos pesados de la prensa estadounidense señalaron también al Comando Ciberespacial como responsable de inocular sensores en las redes eléctricas rusas, como antes hicieron con las venezolanas.

Los informes del 21 y 22 de junio revelados por varios medios norteamericanos sobre el ciberataque de los EEUU a Irán "son significativos y no por accidente", afirma el blog especializado en ciberseguridad Ethical Hacking Consultores. EEUU no suele divulgar sus acciones ofensivas en el ciberespacio: "Esta decisión de EEUU de tratar la revelación de un ataque cibernético como un ataque físico cuando en realidad no hay imágenes, muestra claramente que este es el caso (excepcional)", añade.

Las alarmas no solo se han desatado en Teherán y Moscú, aunque el director de Servicio de Inteligencia Exterior de Rusia, Serguéi Narishkin, fue el primero en manifestarse: "Las consecuencias de la hostilidad de EE.UU. en el ciberespacio, no regulado por la comunidad internacional, pueden ser imprevistas y extremadamente destructivas, incluso para los atacantes". Durante una conferencia el martes en la Universidad de Tel Aviv, el ex jefe de la Agencia de Seguridad Nacional de EEUU y del Comando Cibernético, Mike Rogers, dio por sentado que "el ciberespacio, que ha sido un elemento continuo de la competencia diaria entre los estados, será parte del conflicto entre naciones".

Es sabido que, desde 2009, EE.UU. cuenta con una unidad informática de élite que comanda a diversos grupos especializados en la ciberguerra provenientes de cada uno de los cuerpos militares del Ejército, con un presupuesto anual superior a 3 mil millones de dólares. Posee carta blanca para realizar "actividades militares clandestinas" en redes, bajo los auspicios de la Ley de Autorización de Defensa Nacional de 2018 y otras prerrogativas de la Casa Blanca que se mantienen bajo el más estricto secreto y que, en la práctica, permiten ejecutar actos de guerra sin pasar por la aprobación del Congreso.

Según The Wall Street Journal, el general Paul Nakasone, jefe del poderoso Cibercomando y de la Agencia de Seguridad Nacional, ha articulado una visión de "participación persistente" en el ciberespacio con la intención de obtener acceso a redes de computadoras para planificar acciones y estar listos "con las respuestas apropiadas".

Como reveló el oficial de Inteligencia Edward Snowden, los desvelos de este superejército se deben no solo a los enemigos. La estrategia está diseñada para mantener múltiples opciones abiertas ante cualquier conflicto con otro país que requiera "ataques cibernéticos perturbadores o destructivos". Incluye acciones ofensivas contra sistemas de radares y de comunicación, además de redes, tan peligrosas o más que lanzar bombas en territorio ajeno.

Durante años, la llamada infraestructura crítica -energía, agua, transporte- ha sido un campo de batalla para EE.UU. Según The New York Times, las sondas de reconocimiento estadounidense en los sistemas de control de la red eléctrica de Rusia comenzaron a ser inoculadas en 2012.

Ahora han pasado al ataque. Los *softwares* maliciosos potencialmente incapacitantes ya están dentro del sistema ruso en una magnitud y agresividad comparadas con las de la Operación Farewell, ejecutada con éxito por la CIA contra la Unión Soviética en el verano de 1982, que provocó la explosión del gasoducto euro-siberiano. Lograron introducir una bomba lógica—código malicioso que puede ejecutarse a distancia- en el software canadiense que gestionaba el sistema. El estallido alcanzó una energía de 3 kilotones y partes de las gruesas paredes del gasoducto fueron encontradas a más de 80 kilómetros del lugar.

En septiembre de 2010, las centrifugadoras del programa de enriquecimiento de uranio en Irán fueron infiltradas con Stuxnet, un troyano desarrollado y financiado por dos gobiernos, Israel y EE.UU. Un año después, durante los ataques aéreos de la OTAN contra Libia, la administración Obama consideró bloquear los radares de alerta temprana para ocultar la presencia de los aviones de guerra y silenciar las señales de alarma. El Cibercomando tiene expertos en "spoofing", una técnica que suplanta la señal de posicionamiento de un artefacto tripulado o no tripulado (dron), y permite pilotar aeronaves a distancia con simuladores de vuelo y reemplazar cualquier señal GPS.

Hoy se pueden atacar los sistemas de control desde cualquier lugar en el mundo sin dejar rastros del agresor. Que cualquiera pueda ser acusado de criminal, sin otra prueba que la palabra del Cibercomando, es idílica para la fábrica de mentiras de John Bolton. El asesor de Seguridad Nacional de Trump y veterano de las falsedades de Iraq, reconoció el pasado 11 de junio que EE.UU. ahora estaba adoptando una perspectiva amplia sobre posibles blancos digitales "para decirle a Rusia, o a cualquier otro país que participe en operaciones cibernéticas contra EEUU: 'Tendrás que pagar el precio'". Tom Bossert, ex asesor de Trump en temas de Seguridad Interna y Ciberseguridad, enseñó aún más las uñas: "Nuestro ejército ha sabido por mucho tiempo que podríamos hundir todos los buques de Irán con un margen de menos de 24 horas, si es necesario."

Así andan las cosas. La táctica es tomar todos los caminos que le permitan a Mambrú atornillarse otros cuatro años en la Casa Blanca, incluso haciendo florecer un término propio de la ciencia ficción, la ciberguerra. Qué dolor, qué dolor, qué pena.

Cubadebate
