Estados Unidos incita la guerra cibernética contra Rusia

Por: Omar Pérez Salomón
Globalizacion, 16 de marzo 2022
La pupila insomne 15 March, 2022

Región: EEUU, Rusia
Tema: Espionaje, Guerra

A diario se reportan a través de las autoridades de ciberseguridad de los países ataques a los sistemas cibernéticos, no importa si pertenecen a países desarrollados o subdesarrollados. El 14 de marzo pasado Rusia Today en español publicó la noticia que la autoridad cibernética de Israel confirmó que varias páginas web del gobierno sufrieron un ataque de denegación de servicio (DDoS).

Según este medio lo que sería el mayor ciberataque «jamás realizado contra Israel» se llevó a cabo contra las páginas que utilizan el dominio 'gov.il', con lo cual se bloqueó el acceso a las páginas web de los ministerios del Interior, Salud y Justicia, así como el de Bienestar y la Oficina del Primer Ministro.

A su vez existen gobiernos interesados en que el ciberespacio sea un escenario de guerra permanente. En varias ocasiones el gobierno o el congreso de EE.UU han acusado a China, Rusia, Irán, Corea del Norte, Venezuela o Cuba de patrocinar el terrorismo o de realizar ataques cibernéticos a entidades de ese país. Todo depende de la situación internacional en ese momento y a quién conviene adjudicarle el papel de villano.

Por ejemplo, dos días antes del ataque terrorista a las torres gemelas en New York, el 9 de febrero de 2001, Cuba se convierte en el primer Estado acusado de planear ataques cibernéticos contra Estados Unidos, cuando en la audiencia del Comité selecto del Senado sobre Inteligencia, que trató el tema de "la amenaza mundial", el entonces director de la Agencia de Inteligencia de Defensa, Almirante Thomas R. Wilson, identificó a la Mayor de las Antillas como un posible país "ciberatacante".

Esta situación se convierte en crítica cuando estas acciones se producen en medio de una guerra militar, económica y mediática. La agencia Xinhua reportó el pasado 12 de marzo que China detectó desde finales de febrero, "continuos ciberataques, a través de los cuales organizaciones extranjeras han intentado hacerse con el control de ordenadores ubicados en el gigante asiático para atacar a Rusia, Ucrania y Bielorrusia.

Un análisis realizado por el Equipo Técnico Nacional de Respuesta a Emergencias de Redes Informáticas / Centro de Coordinación de China (CNCERT/CC) – organización china encargada de prevenir, detectar, alertar y gestionar las amenazas e incidentes de seguridad cibernética – reveló que la mayoría de las direcciones de Internet que lanzaron los ataques tenían su sede en EE.UU. y un número pequeño de direcciones con sede en

naciones europeas como Alemania y los Países Bajos. Refirió también que el 87 % de los ataques tenían como objetivo Rusia.

No podemos olvidar que a mediados de la década de l980 los servicios de inteligencia de EE.UU., de varios países europeos y Japón mantenían estrechos vínculos en la guerra que sostenía el imperialismo contra la Unión Soviética. De esa época es el conocido dossier Farewell, que provocó el primer caso conocido de ciberguerra, ejecutado contra la URSS. Se introdujo un Caballo de Troya en el software que operaba las bombas, turbinas y válvulas del gasoducto que debía llevar gas natural desde los yacimientos de Urengoi en Siberia hasta los países de Europa Occidental. Poco después de que comenzó su operación se produjo una gran explosión e incendio que provocó considerables daños, incluido afectaciones considerables a la economía soviética.

Como en aquella época dañar la producción y transporte de petróleo y gas de Rusia es una de las prioridades de EE.UU. y sus aliados europeos. Solo que no estamos en la década de 1980 y Rusia conoce muy bien las intenciones de Occidente.

Omar Pérez Salomón