La guerra del ciberespacio

JUAN GELMAN :: 18/11/2011

El domingo 6, los dominios de Internet del Shin Bet, el Mossad y de dos Ministerios del régimen de Israel fueron inaccesibles para quien quisiera “visitarlos”

Hay gobiernos que trinan y no precisamente con dulzura. Japón sufre ciberataques varios: la Cámara de Diputados y aun algunas embajadas en el exterior han recibido e-mails con virus que infiltraron el Ministerio de Relaciones Exteriores. El Ministerio de Industria y Comercio fue espiado (www.wsj.com, 27-10-11). La policía investiga, pero Tokio está preocupado por la vulnerabilidad de sus sistemas cibernéticos. También Israel.

El domingo 6, los dominios de Internet del Shin Bet, el Mossad y de los Ministerios del Interior y Salud Pública fueron inaccesibles para quien quisiera “visitarlos”. Dos días antes, el grupo Anonymous había amenazado con hackearlos porque la marina israelí interceptó dos naves portadoras de ayuda para Gaza (www.jpost.com, 6-11-11). La voz de un video que el grupo subió a YouTube acusó a Israel de “piratería en alta mar” y señaló que “no había otra alternativa” que atacar si el gobierno israelí mantenía el cerco de Gaza. El verbo “atacar” suele formar parte del glosario bélico. En este caso, sin bombardeos, cañonazos o invasiones terrestres.

El desasosiego es mayor y más explícito en Gran Bretaña y EE.UU. “El volumen de los delitos y ataques por e-mail al gobierno y a la industria sigue siendo perturbador”, señaló Iain Lobban, director de la oficina de espionaje de las comunicaciones del Foreign Office. “Puedo dar testimonio –agregó– de los intentos de robar ideas y diseños británicos en los sectores de la defensa, energía, tecnología, ingeniería y otras industrias para obtener ventajas comerciales o aprovechar el conocimiento de arreglos contractuales secretos” (www.timesplus.co.uk, 31-10-11). Lobban lanzó un alerta: todo ello es una amenaza a la economía del país.

Una reciente investigación del Anti-Phi-shing Working Group revela que el número de dominios, falsos o reales, dedicados al espionaje cibernético, así como el de sus ataques, se incrementa en todo el mundo a pasos acelerados. En el período que se extiende de 2009 al primer semestre de este año, la cantidad de robos informáticos pasó de 55.698 a 115.472, y la de dominios, simulados o no, de 34.513 a 94.383 (www.fiercegovernmentit.com, 8-11-11). Los phishers han encontrado métodos para infectar “decenas, centenares y hasta miles de sitios a la vez, dependiendo del servidor”, subraya el estudio.

Un informe del Ejecutivo Nacional de Cointrainteligencia de EE.UU. destaca que el espionaje cibernético es la amenaza principal que se cierne sobre la economía estadounidense (www.odni.gov, octubre 2011). Indica que los servicios de inteligencia, las empresas privadas, las instituciones académicas y de investigación y ciudadanos de numerosos países saquean la información económica y tecnológica del país. Desde adversarios persistentes como China y Rusia hasta “algunos aliados... que gozan de un amplio acceso a los organismos del gobierno”. Lo hacen mediante todas las técnicas de

espionaje conocidas (Humint) y con métodos cibernéticos de vanguardia, como Rusia.

Las consecuencias de esta situación pueden ser catastróficas, según Richard Clarke, ex asesor de tres presidentes y ex jefe de los servicios de seguridad cibernética de EE.UU. Aseguró que, si continuara en su cargo, "aconsejaría al presidente que se abstuviera de atacar (militarmente) a otros países, porque mucho de ellos, incluidos China, Corea del Norte, Irán y Rusia, podrían responder con ataques cibernéticos que devastarían plantas de energía, redes bancarias o sistemas de transporte... Todo el sistema económico estadounidense podría ser aplastado, porque no tenemos hoy la manera de defenderlo" (www.nytimes.com, 7-11-11).

Hay quienes han propuesto métodos para evitar esos desastres eventuales. El ingeniero ruso Eugenio Kaspersky, especializado en seguridad antivirus, explica que "todo el mundo debería tener una identificación, un pasaporte de Internet" (www.theregister.co.uk, 7-11-11). Sería un excelente instrumento para detectar y clausurar las críticas a los gobiernos que los blogs y las redes sociales difunden. China anunció nuevos ajustes en la materia: el número de participantes en esos medios ascendió a 195 millones de personas a fines de junio, el triple de medio año atrás (www.guardian.co.uk, 26-10-11).

Días después, el subsecretario del Departamento de Seguridad Interior de EE.UU., Caryn Wagner, "declaró que el gobierno teme una inquietud social como la de Túnez en diciembre pasado y que desea utilizar los servicios de los medios sociales como Twitter para monitorear a su propia población" (www.corbettreport.com, 10-11-11). El premier británico David Cameron habló ya de la necesidad de establecer un equilibrio entre la ciberseguridad y la libertad de palabra (www.theregister.co.uk, 1-11-11). No hace falta mucha especulación para saber adónde esto conduce.

Página 12

---

https://www.lahaine.org/mundo.php/la-guerra-del-ciberespacio