Ciberterrorismo: una amenaza real y creciente

En la sociedad moderna, cada vez más dependiente de los sistemas informáticos, la posibilidad de causar graves perjuicios a un Estado a través del asalto a nódulos de comunicación por medio de ataques cibernéticos se ha convertido en una amenaza real con un riesgo creciente. Este tipo de agresiones se agrupan bajo la denominación de "ciberterrorismo", término acuñado hace aproximadamente una década por el profesor Barry C. Collin, del Institute for Security and Intelligence[1], y definido por la doctora Denning, de la Universidad de Georgetown[2], como el "ataque ilegal contra ordenadores, sus redes y la información contenida en ellos cuando se lleva a cabo con la finalidad de coaccionar a un gobierno o a su población para conseguir objetivos políticos o sociales".

El miedo ante un eventual estallido de la guerra cibernética ha flotado en la atmósfera internacional en los últimos tiempos, pero una serie de ataques de origen ruso y chino a las redes de información occidentales a lo largo del pasado año hicieron saltar de nuevo todas las alarmas.

El colapso de un país: el caso de Estonia

A finales de abril, Estonia fue víctima de una oleada de asaltos informáticos contra empresas e instituciones que dejaron inaccesibles los sitios web de bancos, periódicos, escuelas y organismos públicos, causando el caos en un país en el que más del 60% de la población se conecta diariamente a Internet para consultar las decisiones de su Consejo de Ministros, comunicarse con su médico por videoconferencia, realizar todo tipo de operaciones comerciales e incluso votar electrónicamente en las elecciones generales. Los ataques de denegación de servicio distribuidos (técnicas que tienen por objeto dejar un servidor inoperativo provocando su colapso[3]), que se prolongaron varias semanas,

[1] Instituto de Seguridad e Inteligencia estadounidense.

[2] www.georgetown.edu

[3] Denegación de servicio: ataques con los que se busca sobrecargar un servidor para que los legítimos usuarios no puedan acceder a los servicios prestados; el ataque consiste en saturar el servidor con peticiones de servicio hasta que este no puede atenderlas, provocando su colapso. Un método más sofisticado es el ataque de denegación de servicio distribuido (DDoS, *Distributed Denial of Service*), mediante el cual las peticiones son enviadas de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños; puede conseguirse mediante el uso de programas *malware* que permitan la toma de control del equipo de forma remota, con ciertos tipos de gusano o bien porque el atacante haya entrado directamente en el equipo de la víctima.

causaron tal impacto que el ministro de Defensa estonio, Jaak Aaviksoo, no dudó en compararlos con una acción terrorista[4].

Esta consideración no sólo se basaba en el grado de organización de la operación y en los daños causados sobre el conjunto de la sociedad de la república báltica; pronto se identificó el origen ruso de los ataques, lo que llevó a la conclusión de que los motivos de los *hackers* eran de índole política. Unos días antes, las autoridades estonias habían procedido a la reubicación de un monumento erigido a los militares soviéticos caídos combatiendo el nazismo en Tallin, y los *ciberataques* se entendieron como una represalia más en el contexto de la grave crisis diplomática abierta entre rusos y estonios.

Los ordenadores de los gobiernos y redes militares occidentales sufren miles de intentos de intrusión al día; sin embargo, el caso estonio adquirió especial relevancia, no sólo por la magnitud de los daños ocasionados, sino también porque fueron muchos los expertos que vislumbraron en el ataque las huellas del Kremlin. Finalmente, y ante la imposibilidad de confirmar la implicación de las autoridades rusas, el Gobierno de Tallin terminó aceptando la idea de que podría haber sido obra de activistas tecnológicos.

China, la 'reina de los troyanos'

Esta misma duda se plantea respecto a los cada vez más frecuentes ataques a redes gubernamentales europeas y norteamericanas procedentes de China. El caso más sonado se produjo el pasado mes de junio, cuando un grupo de *hackers* penetró en el sistema de seguridad de la red del Pentágono, accediendo a servidores con información compartida. El Departamento de Seguridad Interior estadounidense (*Department of Homeland Security*[5]) reconoce sufrir intentos de ataque a sus sistemas a diario, pero en esta ocasión los piratas informáticos llegaron más lejos que nunca, precipitando el apagado de 1.500 terminales y entrando en el servidor de correo electrónico del mismo secretario de Defensa, Robert Gates. El rastreo del ataque condujo al Ejército de Liberación del Pueblo (PLA, *People's Liberation Army*), esto es, al ejército chino. No obstante, aún no se ha confirmado que las autoridades del país oriental estuvieran directamente implicadas, dado

[4] http://www.elpais.com/articulo/internet/crisis/Estonia/Rusia/llega/Internet/elpeputec/20070517elpepunet_4/Tes

http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598&CFID=69779&CFTOKEN=4acaeb8afb7e0e70-0FDE9DC5-B27C-BB00-0127B47C57FFEECD

[5] http://www.dhs.gov/index.shtm

que, si bien puede averiguarse de dónde procede un *ciberataque*, es prácticamente imposible conocer de quién parte la iniciativa[6].

En cualquier caso, cada vez existen más informes sobre ataques informáticos a países occidentales con origen en el gigante asiático. La canciller alemana, Angela Merkel, informó del hallazgo de programas de espionaje en los ordenadores de varios ministerios, ataque que también fue atribuido al ejército de la República Popular China[7]. Posteriormente, fuentes oficiales británicas declararon que varios departamentos gubernamentales de Reino Unido han sufrido intrusiones en sus sistemas con origen en China en los últimos meses[8], y el secretario general de Defensa de Francia, Francis Delon, confirmó que el país galo ha sido igualmente víctima de estas agresiones.

Mientras, el Gobierno de Pekín niega tajantemente su responsabilidad y califica los informes como el fruto de la mentalidad típica de la Guerra Fría. Lo cierto es que los expertos en seguridad y defensa llevan meses alertando del recrudecimiento de los asaltos informáticos contra empresas y redes de información occidentales en busca de información confidencial o secretos industriales. Es significativo que el director general del MI5 (servicio de seguridad británico)[9], Jonathan Evans, dirigiera a finales de noviembre una carta a más de 300 empresas británicas que operan en el *gigante asiático* advirtiéndoles del peligro de los ataques dirigidos por organizaciones estatales, consistentes en el robo de información confidencial en beneficio de las compañías locales.

Como viene siendo habitual, un oficial de la embajada china en Londres, Zhao Shangse, se apresuró a negar todas las acusaciones[10]. Sin embargo, hay indicios de la implicación gubernamental en los ataques: de acuerdo con el informe anual de 2007 enviado por el Departamento de Defensa al Congreso de Estados Unidos, el ejército chino ha invertido

---

[6] http://www.elmundo.es/navegante/2007/09/04/tecnologia/1188895913.html

http://www.elpais.com/articulo/internet/Ejercito/chino/penetra/red/Pentagono/elpeputec/20070904elpepunet_4/Tes

[7] http://www.elpais.com/articulo/reportajes/troyanos/espian/Alemania/elpepusocdmg/20070902elpdmgrep_5/Tes

[8] http://www.elmundo.es/navegante/2007/09/05/tecnologia/1188980588.html

[9] MI5: www.mi5.gov.uk

[10] http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/12/01/wspy101.xml

http://news.bbc.co.uk/2/hi/business/7123970.stm

grandes cantidades de dinero en el desarrollo de técnicas de ataque, defensa y aprovechamiento de redes informáticas[11].

De hecho, los estrategas militares norteamericanos temen que China se esté preparando para la *ciberguerra*, por lo que el recién creado Mando Ciberespacial de las Fuerzas Aéreas (Air Force Network Operations Command), que defiende las redes militares de comunicaciones y datos, ha dirigido sus esfuerzos a investigar cómo deshabilitar las redes informáticas de un rival y destruir sus bases de datos.

La necesidad de una respuesta global

Los recientes acontecimientos han supuesto, en suma, la materialización de los temores gestados en los últimos años respecto a las posibilidades de que la guerra del futuro se libre en la Red. En tal caso, la principal amenaza estaría relacionada con la integridad de la información: los ataques silenciosos pueden robar o modificar datos clave, lo que haría que ciertas partes indispensables de los sistemas dejaran de funcionar o, lo que entraña un mayor peligro, que la información sensible dejase de ser fiable. La economía global depende del intercambio de información, y su interrupción provocaría problemas comparables a los ocasionados por la alteración de recursos básicos. En el contexto de la Sociedad de la Información, no dejan de ser preocupantes los daños que tales acciones causarían no sólo a las instituciones, sino sobre la propia población civil.

Con el fin de evitarlos, todas las infraestructuras cuyo funcionamiento depende de complejos sistemas informáticos y de comunicaciones deben dotarse de elementos de protección suficientes. Por otro lado, junto a la creación de unas estructuras tecnológicas adecuadas, se hace necesaria la configuración de un marco legal internacional que considere estas agresiones una forma más de terrorismo, crimen organizado internacional o agresión contra el Estado.

Además, la propia naturaleza de Internet hace que el marco geográfico ya no sea una referencia en la identificación del agresor, por lo que pueden surgir conflictos jurídicos en cuanto al lugar real donde se cometió el delito con las implicaciones para las relaciones internacionales que ello supone. Se trata, en definitiva, de ataques con máquinas, por lo que los estados deben dotarse de las tecnologías apropiadas para combatirlos y cooperar entre ellos, derribando las fronteras.

[11] http://www.economist.com/world/international/displaystory.cfm?story_id=9752625

http://www.economist.com/world/international/displaystory.cfm?story_id=9769319

El Consejo de Europa abordó los delitos informáticos en el Tratado sobre Cibercrimen de 2001, primer instrumento internacional que implica la elaboración de leyes contra los ataques a la integridad, confidencialidad y disponibilidad de los ordenadores y redes (acceso, virus, interceptación de comunicaciones, etc.), fraude, contenidos ilegales y derechos de autor. Pero su alcance es limitado: entró en vigor en 2004, suscrito únicamente por seis estados miembros de la Unión y, aunque posteriormente se han adherido otros países, incluyendo Estados Unidos y Japón, otros, como China y Rusia, aún no lo han hecho.

Recientemente, los ministros de Justicia de la Unión Europea abordaron por vez primera y aprobaron por unanimidad la propuesta de perseguir el uso de Internet como herramienta terrorista; la Comisión Europea había propuesto a comienzos de noviembre la adopción de medidas para criminalizar el uso de Internet con fines terroristas, como por ejemplo reclutar activistas o difundir instrucciones para fabricar artefactos explosivos, lo cual es un síntoma evidente de la preocupación por el potencial de las nuevas tecnologías como instrumentos delictivos[12].

Por su parte, la OTAN no define los *ciberataques* de forma expresa como una acción militar, por lo que las provisiones del Artículo V del Tratado, relativas a la defensa mutua, no son extensibles a estos casos. No obstante, fuentes oficiales de la Alianza declararon, tras los ataques informáticos a Estonia, que se trataba de un problema de seguridad operacional y que se estaba tomando muy en serio, por lo que se espera que en un futuro cercano esta cuestión quede resuelta[13].

Ya en la Cumbre de Riga de noviembre de 2006, la OTAN acordó poner en marcha un sistema de defensa del ciberespacio con una cobertura superior a la que actualmente se proporciona a los sistemas de información que se usan en las operaciones militares, pero las medidas propuestas aún no se han hecho efectivas.

Por último, la Unión Internacional de Telecomunicaciones (UTI)[14], dependiente de la Organización de las Naciones Unidas y formada por 191 estados, contempla en su Agenda sobre Ciberseguridad Mundial[15] los siguientes objetivos:

---

[12] http://www.elpais.com/articulo/internet/UE/perseguira/uso/Internet/herramienta/terrorista/elpeputec/20071207elpepunet_7/Tes

[13] http://www.economist.com/world/international/displaystory.cfm?story_id=9228757

[14] International Telecommunications Union: www.itu.int

[15] http://www.itu.int/osg/csd/cybersecurity/gca/

i. La elaboración de estrategias para el desarrollo de un modelo de legislación del cibercrimen de aplicación global y compatible con las medidas nacionales y regionales ya existentes.

ii. La creación de estructuras organizativas y políticas adecuadas contra el *cibercrimen*.

iii. La definición de unos estándares de seguridad para aplicaciones y sistemas.

iv. La creación de un marco internacional para la vigilancia, aviso y respuesta a incidentes que garantice la coordinación entre las iniciativas ya existentes y las nuevas.

v. La creación y el respaldo de un sistema de identidad digital genérico y universal.

vi. El diseño de una estrategia global que facilite el desarrollo de la capacidad humana e institucional para aumentar el conocimiento y el *know-how* en los sectores y áreas antes mencionados.

vii. El asesoramiento en relación con la cooperación, el diálogo y la coordinación internacionales.

El espionaje industrial y político siempre ha existido y seguirá existiendo. Sin embargo, las Tecnologías de la Información y las Comunicaciones, y especialmente Internet, han abierto un nuevo y amplio abanico de posibilidades delictivas que muchas empresas y organismos públicos aún no pueden combatir. La Sociedad de la Información concede a las TIC el poder de convertirse en nuevos motores de desarrollo y progreso, pero este potencial constituye al tiempo un foco de vulnerabilidades que puede ser explotado en un contexto internacional hostil. Por todo ello, se hace cada vez más necesaria la cooperación entre países encaminada a la protección de las redes de comunicación, de los ciudadanos y las organizaciones y de sus derechos.