El oscuro arte de la ‘ciberguerra’

Alastair Gee

¿Los ataques virtuales constituyen una guerra? Es mucho más complicado de lo que parece.

Este verano, los dos candidatos presidenciales de Estados Unidos -acostumbrados a lidiar cada uno con su rival- fueron objeto de otro tipo de ataque. El FBI y el servicio secreto de EE UU informaron a los equipos de Obama y McCain de que unos *piratas informáticos* habían entrado en sus redes en busca de pistas sobre futuras estrategias políticas. Estas maniobras procedían seguramente de China. Según varias informaciones, en meses recientes, otros *cibercriminales* de dicho país se han infiltrado en la Casa Blanca y el Pentágono. Y, durante el conflicto entre Rusia y Georgia del pasado verano, las páginas web del Gobierno georgiano también sufrieron agresiones vía Internet, presuntamente organizados por particulares desde Rusia.

RAIGO PAJULA/AFP/Getty Images

¿La primer *ciberguerra*?
Flores frente al Soldado de Bronce, momumento conmemorativo soviético en Estonia, cuya eliminación generó *ciberataques* sin precedentes en 2007.

Ahora bien, ¿cuándo deja un ataque virtual de ser una molestia y se convierte en una

declaración de guerra? No es una pregunta meramente retórica: en el caso de la Casa Blanca y el Pentágono, se corrió el riesgo de que quedaran al descubierto secretos importantísimos para la seguridad nacional de Estados Unidos. Y, si Georgia hubiera sido un país miembro de la OTAN, otros miembros quizá se habrían visto obligados, por la cláusula de defensa mutua, a responder a Rusia, no sólo por su agresión terrestre sino también por sus acciones a través de la Red.

Sin embargo, en un mundo cada vez más restringido por las leyes internacionales, existe escasa infraestructura legal para hacer frente a este nuevo tipo de lucha. Pocos países disponen de legislación detallada, y no existe más que un gran tratado internacional, el Convenio sobre Delitos Cibernéticos del Consejo de Europa, firmado en 2001 y que no han ratificado más que 23 países.

Este vacío legal puede causar problemas, se inquieta Duncan Hollis, profesor en la Facultad Beasley de Derecho de la Universidad de Temple (EE UU). “Si [un país] considera [los *ciberataques*] actos de guerra, tiene derecho, según las leyes internacionales, a defenderse, y no tiene por qué ser sólo a través de la informática”, dice Hollis. “Debemos reunirnos y, por lo menos, tratar de decidir cuáles son las reglas del juego”, sostiene.

Consciente de que sus miembros pueden acabar en el punto de mira de los *piratas informáticos* , la OTAN ha empezado a estudiar con más detalle las leyes de la *ciberguerra*. La organización inauguró hace poco el Centro de Cooperación para la Defensa Cibernética en Tallin, la capital de Estonia, y uno de los principales focos de atención va a ser cómo llenar los huecos que las agresiones virtuales han revelado en los sistemas legales (si bien los investigadores también van a estudiar otras cuestiones políticas y estratégicas, como la manera de hacer frente a los ataques y el derecho de los usuarios de Internet a la intimidad).

Los investigadores confían en que algunas de sus sugerencias puedan ayudar a otras entidades que están trabajando contra el delito en la Red y la *ciberguerra*, dice Kenneth Geers, miembro de la delegación estadounidense en el centro de Tallin. “En EE UU, las fuerzas policiales, en general, no saben con exactitud qué pueden y qué no pueden hacer, [porque] las leyes cambian a toda velocidad”, explica.

Los investigadores de la OTAN dicen que uno de sus retos más difíciles será el de definir, para empezar, quién es el adversario. La guerra convencional enfrenta a dos enemigos cara a cara, pero los atacantes virtuales son prácticamente anónimos o, en el mejor de los casos, difíciles de localizar. El tráfico de Internet atraviesa continentes en fracciones de segundo. Aún más, un código malintencionado enviado por un delincuente puede atravesar muchos Estados, y esos países pueden negarse a facilitar los datos de los que dispongan a los investigadores. Los

criminales pueden aprovechar la vaguedad de las leyes internacionales.

“Si yo fuera un *pirata informático* estadounidense, desviaría mi tráfico a través de países con los que Estados Unidos tenga escasa cooperación legal”, dice Geers. “De esa forma, de pronto, uno es totalmente anónimo”.

Otro problema delicado al que se enfrenta la Alianza Atlántica es saber cuándo un ataque virtual causa suficientes daños reales como para considerarlo un acto de guerra. En este nuevo ámbito, en vez de soldados que disparan proyectiles desde un campo de batalla, “unos técnicos bien alimentados, que trabajan desde la seguridad de unas salas con aire acondicionado, en su propio país, pueden llevar a cabo un acción contra una instalación en otro Estado de una dimensión y unos efectos tales como para considerarlo una agresión armada”, afirma Davis Brown, antiguo fiscal militar adjunto en el Organismo de Sistemas de Información de Defensa estadounidense. El año pasado, se filtró un vídeo del Laboratorio Nacional de Idaho (en EE UU) que mostraba cómo podría suceder algo así. Los científicos simularon una agresión informática contra una central energética y lograron que ésta acabara apagándose.

Además, el derecho penal nacional suele estar anticuado en lo que se refiere a los ataques informáticos. Se vio, por ejemplo, con el incidente de abril de 2007 en el que las autoridades estonias quitaron del centro de Tallin un monumento bélico de la era soviética. Estallaron violentas manifestaciones de la importante minoría étnica rusa y hubo una reacción en el mundo virtual. Hubo numerosos acciones a través de la Red que acabaron cerrando las web de bancos, ministerios y periódicos estonios.

Sin embargo, los atacantes podrían recibir una condena máxima de sólo unos cuantos años de cárcel, dice Eneken Tikk, un experto legal estonio que trabaja en el *cibercentro*. “Aunque estaba prohibido introducirse ilegalmente en una red, el castigo para ese delito era tan pequeño que fue burocráticamente imposible emprender una investigación encubierta”, explica. Además, las autoridades rusas se negaron a cooperar con la investigación. Desde entonces, los procesamientos han sido limitados: en enero, se impuso una multa a un ciudadano estonio de etnia rusa por haber participado en estas acciones.

Los expertos sugieren que es poco probable que un tratado de ámbito mundial resuelva todos estos aspectos; seguramente no lo ratificarían todos los países, ni incluiría los detalles necesarios para que las instituciones y los abogados lleven a cabo las investigaciones y los procesamientos.

Existen asimismo propuestas de que los abogados discutan, además de la *ciberdefensa*, los tipos de guerra virtual en los que pueden participar los ejércitos. Si los ataques están

restringidos al ámbito de Internet, dicen esas voces, los conflictos del siglo XXI podrían ser mucho menos sangrientos que los del siglo XX. “Podríamos tener menos daños colaterales si podemos decidir cuándo está permitida la *ciberguerra*”, dice Hollis.

Artículos relacionados

- El Ejército virtual del Kremlin. ***Evgeny Morozov***
- Luchas en la Red: Putin ataca Estonia.
- La 7 historias que se perdió en 2007: El comienzo de las *ciberguerras.*

Fecha de creación
17 noviembre, 2008