La guerra SILENCIOSA

Un pirata informático puede anular claves bancarias, redes de comunicación y transporte y toda clase de infraestructuras críticas de servicios públicos

Muchas son las voces que alertan ya sobre el nuevo fantasma que recorre el mundo: la ciberguerra, y muchos son también los expertos en seguridad que vaticinan la aparición de un nuevo teatro de operaciones de alcance mundial: Internet. Un territorio virtual, casi desconocido hasta hace poco, sobre el que se apoyan sistemas industriales, financieros, estratégicos y militares, repleto de datos cuya pérdida o fuga es asunto crucial de Estado. La ciberguerra es capaz de infringir daños superiores a los de las armas convencionales: puede provocar alteraciones sociales que agoten la capacidad de resistencia de un adversario sin necesidad de entablar batalla directa con medios tradicionales.

Las ciberarmas tienen caducidad rápida y un solo uso. Su utilidad depende sobre todo de que el atacado ignore la existencia de la brecha en su seguridad por la que se infiltra el atacante. Pero cualquier ataque deja detrás un rastro digital que puede ser analizado y neutralizado con *parches* informáticos que impiden nuevos ataques similares. Una característica de la ciberguerra es la dificultad de crear sistemas de alerta temprana o prevención, debido al escaso tiempo que transcurre entre la decisión de llevarlas a cabo y sus efectos. Por lo cual, el entorno estratégico es altamente inestable, y aumentan las posibilidades de descontrol por errores tecnológicos o fallos humanos.

No siempre resulta posible rastrear la procedencia última de un ciberataque. El proceso es muy complejo técnicamente y requiere tiempo y buenos recursos. Los ataques se pueden ejecutar utilizando miles de ordenadores repartidos por todo el mundo. Estas máquinas actúan a modo de *zombis*, al poder ser controladas remotamente sin conocimiento de sus usuarios. Eso hace muy difícil la respuesta del atacado, que no tiene conocimiento seguro de quien maneja realmente los ordenadores agresores. Además, la existencia de los *hackers*, que actúan fuera del control de los Estados, permite a estos negar su responsabilidad directa en un ciberataque, atribuyéndolo a grupos marginales. Y, al igual que ocurre en el espionaje clásico, los gobiernos pueden también contratar los servicios de piratas informáticos para efectuar operaciones encubiertas y enmarañar la procedencia de los ataques.

En el ciberespacio actúan indistintamente agentes públicos y privados, y eso impide con frecuencia limitar las tareas defensivas al entramado puramente estatal o militar. Existen ciberarsenales muy complejos y avanzados en manos privadas, por lo que resulta imprescindible una cooperación estrecha y continua entre las empresas, las instituciones y las FAS para enfrentar con eficacia la amenaza.

El experto en planteamientos estratégicos de ciberguerra, Manuel Ricardo Torres, en un trabajo publicado en la revista *Ejército*, apunta que las diferentes FAS preparan el campo de batalla cibernético, en tiempo de paz, tratando de infiltrarse en los sistemas «enemigos y plagarlos de *bombas lógicas* y *puertas traseras*, que serán utilizadas en el momento deseado, cuando comiencen las hostilidades declaradas. Algo que termina difuminando la línea divisoria entre situaciones bélicas o pacíficas, lo que hace más difícil denunciar el quebrantamiento de normativas internacionales».

ACUSACIONES MUTUAS

El pasado 20 de marzo Corea del Sur aseguró que había conseguido situar el origen del grave ciberataque que había sufrdio horas antes en una dirección IP (siglas en inglés de Protocolo Internet) de China. Es más, Seúl señalaba a su vecino del Norte como responsable último de la incursión informática que afectó a más de 32.000 ordenadores.

Al cierre de esta edición no se había producido ninguna reacción oficial de Pekín. Es realmente complejo demostrar el origen último de los ataques y las acusaciones mutuas han sido práctica habitual en los últimos meses. China había hecho público recientemente un informe en el que acusaba a EEUU de estar detrás de una gran parte de los ataques exteriores contra sus redes institucionales y compañías estatales Según informó la agencia oficial *Xinjua*, no todos los ataques venían de EEUU, pero de ese país procedían 39 de las 85 webs que ataca-

Hélène Gicquel

ron, así como el 73 por 100 de los *phishing* (estafa disfrazada de webs de supuestos bancos o compañías comerciales).

El anuncio de China era la réplica a una acusación similar por parte estadounidense, al denunciar ciberataques chinos programados y masivos. Esta acusación se produjo a mediados de febrero, y estaba basada en un informe de la empresa de seguridad estadounidense Mandiant, que acusó al Ejército chino de manejar una serie de ciberataques, desde un edificio militar en un barrio de Shanghái, hasta empresas, instituciones e infraestructuras norteamericanas. Una acusación que fue rechazada frontal y oficialmente por las autoridades chinas.

Según Mandiant, las FAS chinas disponen de una unidad especial (Unidad 61389) en la que trabajan miles de personas dedicadas a penetrar las redes de corporaciones como Dow Chemical, Symantec, Adobe, Yahoo, Lockheed Martin, Google o Northrop Grumman, además de otros proveedores de servicios estatales que controlan los oleoductos o el suministro eléctrico. Las corporaciones de seguridad norteamericanas creen que la estrategia china para adquirir información valiosa es vital para su desarrollo económico, y combina la inversión en I+D, las compras en empresas occidentales de tecnología punta, y el ciberespionaje industrial. El gobierno chino niega toda implicación en estos ataques, que pueden ser redirigidos desde cualquier parte del mundo a través de Internet. Pekin sostiene también que las denuncias norteamericanas buscan fomentar la desconfianza hacia sus empresas informáticas para favorecer a las compañías estadounidenses. Las acusaciones de Mandiant «carecen de pruebas y base legal», según las autoridades chinas, ya que solo se basan en que los ataques proceden de direcciones IP basadas en China, lo cual es fácilmente manipulable. Es posible perpetrar ciberataques continuos en Internet ocultando la verdadera procedencia. «Los ataques denunciados —dijo un portavoz del Ministerio de Defensa chino— son transnacionales y anónimos, por lo que resulta muy difícil identificar su origen auténtico».

El reciente ataque a Corea del Sur constata la vulnerabilidad de los sistemas

Jeffrey Carr, fundador de la empresa de ciberseguridad Taia Global, asegura que los chinos no son los únicos atacantes en este juego, y afirma que el informe de Mandiant crea un precedente peligroso. «Pese a que China —dice— es claramente sospechosa, no se puede acusar sin pruebas al Ejército chino, porque nos hace correr el riesgo de una escalada. Rusia, Francia o Israel son también países muy activos en ciberespionaje y hay más de 30 países desarrollados y emergentes que aumentan día a día sus unidades militares de ciberespionaje, y todas las grandes agencias de inteligencia están implicadas».

NASA

Algunos analistas hablan ya de «ciberguerra fría» entre Estados Unidos y China

La opinión de Carr difiere radicalmente de la de otro experto, Dan Goodin, para quien el informe Mandiant ha servido para explicar cómo China ha obtenido cantidades ingentes de información valiosa de más de 140 organizaciones estadounidenses en los últimos siete años, incluyendo industrias punteras como la aeroespacial y farmacéutica. El presidente del Comité de Inteligencia de la Cámara de Representantes, Mike Rogers, opina que EEUU está perdiendo la ciberguerra contra China, y advirtió que la situación se agrava rápidamente.

Los ingenieros de Mandiant, igual que antes hicieron los de Symantec, han conseguido videos que muestran cómo opera, supuestamente, la unidad militar secreta 61398, instalada en un discreto edificio de Shanghái. El informe asegura que desde allí trabaja un grupo de piratas informáticos identificados como APT-1, que cuenta con apoyo directo del ejército chino para realizar campañas continuas de espionaje cibernético en todo el mundo. «Este informe —criticó el diario *Global Times* de Pekín— sirve para alimentar la idea de una amenaza china y ayuda a justificar ante la opinión pública las enormes inversiones que EEUU lleva a cabo en tecnología de ciberespionaje».

CIBERGUERRA FRÍA

Fuentes de prensa rusas, por otra parte, anuncian una respuesta norteamericana contundente a los presuntos ciberataques de China, que incluiría multas y restricciones comerciales contra las naciones que alberguen a piratas informáticos. Una medida que podría afectar a España que, según algunos expertos-, cuenta con *hackers* de gran nivel. El español es el tercer idioma más utilizado en el cibercrimen, por detrás solo del inglés y del chino y por delante incluso del ruso.

La pregunta que se hacen muchos expertos es si el mundo se encuentra ya inmerso en una ciberguerra. Una cuestión que responde al hecho de que en cualquier futuro conflicto internacional el factor cibernético tendrá una decisiva influencia. El diario *New York Times* califica ya de «ciberguerra fría» las relaciones actuales entre EEUU y China. «Un conflicto —dice el periódico— menos peligroso que la confrontación EEUU-URSS que siguió a la II Guerra Mundial, pero también más complicado, puesto que detectar los ciberataques y su procedencia lleva un tiempo que hace imposible la respuesta inmediata.

A esta dificultad se añade el hecho de que China es un rival económico de EEUU, pero también principal proveedor y cliente, además de ser uno de los mayores acreedores de la deuda pública estadounidense. Eso hace que no haya muchas represalias posibles por parte de Washington, aparte de bloquear las inversiones de las compañías de tecnología avanzada que operan en China.

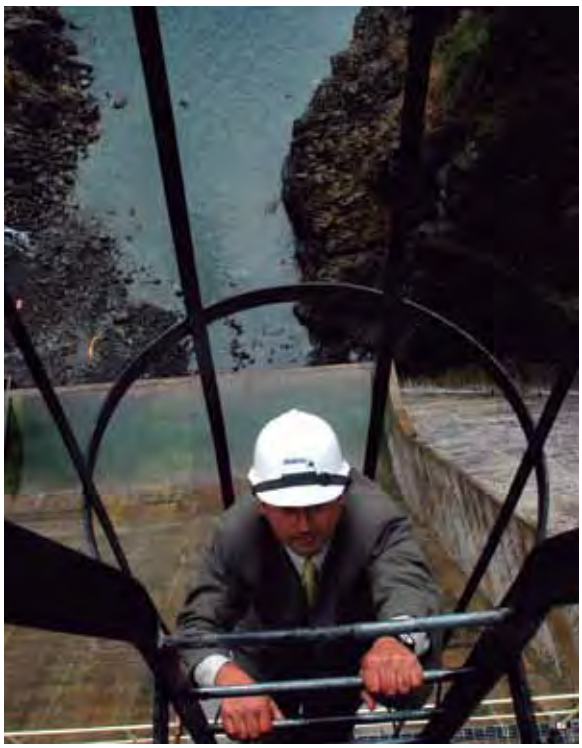
En 2012 el intercambio comercial entre los dos países llegó a 425.000 millones de dólares, y China desbancó a EEUU como principal potencia comercial en el mundo, aunque el país norteamericano siga siendo la mayor economía global, y el PIB (Producto Interno Bruto) chino continúe todavía bastante por detrás del estadounidense. En términos nominales el PIB de China es de unos 8,25 billones de dólares, contra 15,65 billones de EEUU, pero la diferencia es mucho menor si se considera la paridad del poder adquisitivo en ambos países.

El subsecretario de Defensa norteamericano, William J. Lynn, estima que unas 15.000 redes del Pentágono y siete millones de dispositivos informáticos están siendo escudriñados miles de veces diariamente. Se trata de una contienda asimétrica, donde no funcionan los tradicionales modelos de disuasión por la dificultad de identificar a los instigadores reales de los ataques.

Todos los países de Oriente Medio son objetivos importantes del gobierno de Washington, que ha incrementado fondos y personal para llevar a cabo actividades en el ciberespacio, y el Pentágono ha decidido aumentar de 900 a más de 4.500 los militares empleados dedicados a esta actividad.

Una de las brechas más importantes en el sistema de ordenadores militares de EEUU la produjo en 2008 una agencia de inteligencia extranjera que consiguió insertar un código malicioso en un ordenador portátil militar norteamericano, emplazado en Oriente Medio, que estaba conectado a una red dirigida por el Comando Central de las fuerzas armadas estadounidenses.

El código se extendió sin ser detectado tanto en sistemas clasificados (secretos) como abiertos, y estableció una cabeza de puente digital que transfería datos a servidores de otro país. La operación del Pentágono para contrarrestar este ciberataque, conocida como *Operación Buckshot Yankee,* marcó un hito en la estrategia ciberdefensiva de los Estados Unidos, y



Iván Alvarado/EFE

El ataque al sistema informático de una central hidroeléctrica podría anular a todo un país.

Abedin Taherkenareh/EFE

En 2010 se detectó un ataque contra las centrales nucleares iraníes. En la foto, la central de Busheir (Teherán).

muchas de las medidas adoptadas desde entonces por Washington para impedir fugas similares permanecen secretas. Una de las claves de estas unidades de ciberguerra es intentar que los ataques queden silenciados. Es decir, si se produjera una nueva incursión sería parte de la defensa el que nadie ajeno al sistema se enterase de que el sistema es vulnerable.

LA AMENAZA FLAME

La importancia de este conflicto, de dimensiones globales, ha venido subrayada por acontecimientos recientes, como la aparición del virus *Stuxnet* contra Irán en 2010, que dañó y retrasó el desarrollo nuclear iraní al destruir casi 1.000 de las 6.000 centrifugadoras destinadas al enriquecimiento de uranio en ese país. Otro ejemplo es el virus *Flame*, detectado en 2012 y considerado el software de espionaje más complejo descubierto hasta ahora. Ambos virus han sido atribuidos a Israel y Estados Unidos.

Flame fue diseñado para rastrear en secreto redes informáticas de Irán, robar datos a gran escala, interceptar las comunicaciones y controlar los ordenadores iraníes. En esta campaña de guerra cibernética encubierta han participado la Agencia de Seguridad Nacional estadounidense, la CIA y el ejército de Israel, que en ocasiones parece haber actuado unilateralmente, sin avisar a Washington. El ministro de Defensa israelí, Ehud Barak, admitió recientemente que Israel —que dispone de una importante unidad militar dedicada a la ciberguerra— desarrolla tanto la defensa como el ataque en el ciberespacio. «A diferencia de la guerra convencional —comentó—, en este tipo de lucha es más importante invertir en la defensa que en atacar al enemigo».

Flame se instaló hace cinco años y resultó indetectable durante largo tiempo. Además de recoger información y grabar conversaciones, alteraba la configuración de datos y obtenía direcciones y números de teléfonos, y se infiltró en ordenadores de Irán, Siria, la Autoridad Nacional Palestina, Líbano, Sudán y Egipto. Eugene Kaspersky, el fabricante ruso de antivirus, calcula que para crearlo se necesitaron unos 100 millones de dólares destinados a los ingenieros, analistas y expertos que participaron en su creación. «*Flame* puede hacer mucho daño —dice Kaspersky—. Ya no se trata de ciberguerra sino de ciberterrorismo. No sabes dónde ni cuándo será el próximo ataque, y si no se actúa rápido las cosas irán a peor, porque los países no tienen defensas suficientes (...) Puede ser el fin del mundo que conocemos si no hay cooperación internacional contra este peligro». Según el diario *Washington Post*, los ataques cibernéticos contra el programa nuclear de Irán se iniciaron hacia 2005, en el segundo mandato del presidente George W. Bush, y en una primera fase consistieron en identificar blancos potenciales y desarrollar sistemas para destruirlos. En 2008, el programa operativo contra Irán fue desplazado del Pentágono a la CIA. Expertos en Inteligencia dan por supuesto que *Flame* y *Stuxnet* son el preludio de un ataque más amplio que sigue su curso para intentar detener el programa nuclear iraní.

Durante cinco años, Israel consiguió interceptar los sistemas iraníes

El gobierno de Teherán reconoció en septiembre de 2010 que *Stuxnet* había infectado a unos 30.000 ordenadores dentro de su territorio y continuaba activo. Se trata del primer gusano informático que ataca plantas industriales. Según algunos expertos, tiene capacidad para hacer estallar la instalación atacada y no está por completo controlado.

La complejidad del programa *Stuxnet* permitía suponer que —tal como opinaban algunos especialistas— no podía ser obra de un mero pirata informático, sino de un Estado, o Estados, con elevado potencial cibernético. *Stuxnet* es un virus de tipo troyano (que penetra con apariencia inofensiva) muy sofisticado, que aprovecha la vulnerabilidad de los sistemas operativos empleados en los programas utilizados en plantas de tratamiento de aguas, centrales eléctricas, oleoductos y centrales nucleares. El virus queda camuflado y latente en el sistema infectado hasta que el agresor decida activarlo, ataca infraestructuras vitales, y puede alterar cualquier parámetro de los progra-

Diego Azubel/EFE

Glosario para un nuevo arte de la guerra

BOMBA LÓGICA
Bajo esta denominación se incluye un amplio conjunto de operaciones de *software* con el propósito de dejar una puerta abierta y oculta en los sistemas atacados, para ser utilizada más tarde.

Una forma simple y efectiva de *bomba lógica* son los comandos que borran toda la información contenida en el equipo donde se encuentra alojada, incluyendo la propia *bomba*. Eso permite llevar a cabo un ataque que no deja rastro y puede inutilizar los sistemas informáticos del enemigo. Hay otras versiones de bombas *lógicas* que provocan daños en el *hardware* por medio de una subida de la tensión eléctrica, la temperatura o la desviación de cualquier otro factor.

LAMMERS
Personas sin gran preparación teórica, en muchos casos adolescentes, que aunque no saben programar, ejecutan programas de otros para dañar sistemas mediante ataques masivos constantes y descentralizados.

HACKERS
Expertos aficionados informáticos capaces de crear programas y entrar en sistemas protegidos. Suelen actuar sin ánimo de lucro, para demostrar la vulnerabilidad de determinados sistemas.

CRACKERS
Son *hackers* que buscan el daño o el lucro con sus acciones piráticas en la Red.

GUSANOS
Virus que tienen la capacidad de duplicarse a sí mismos y ralentizar o detener el *hardware* que los alberga. Utilizan las partes automáticas de un sistema operativo que normalmente son invisibles para el usuario.

.

TROYANOS
Virus que entran en un sistema operativo sin que el usuario se aperciba, y ejecutan programas indeseados o permiten la entrada de *intrusos* por control remoto.

DDOS
Saturación de los servidores que hospedan las páginas web, al hacer más peticiones de las que el servidor soporta, con lo que este queda inutilizado.

CIBERESPACIO
Dominio global y dinámico compuesto por infraestructuras de tecnología de la información que incluye Internet, redes sociales, redes de telecomunicaciones y sistemas de información.

CIBERATAQUE
Acción producida en el ciberespacio que compromete o destruye la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan. Pueden ser contra entidades públicas o privadas.

mas automatizados de servicios básicos. El ataque informático contra Irán surgió en 2006, con la infiltración en las redes informáticas de la planta nuclear iraní de Natanz por la Agencia de Seguridad Nacional norteamericana, principal encargada del espionaje electrónico. La operación fue denominada «Juegos Olímpicos», y con los datos obtenidos en esta primera fase, los Estados Unidos e Israel diseñaron el virus para frenar el proyecto nuclear iraní. Cuando Obama llegó a la Casa Blanca, esos ataques por Internet no solo se mantuvieron, sino que se intensificaron, al considerar Washington que eso evitaría un ataque relámpago de Israel a Irán, con consecuencias desestabilizadores en todo Oriente Medio. Al parecer, cuando los responsables del programa nuclear iraní detectaron el virus en Natanz, ya estaba fuera del control norteamericano, y terminó infectando a miles de ordenadores en Indonesia, India e Irán, además de EEUU.

OTROS ATAQUES

Otro caso fue la serie de ciberataques contra Estonia procedentes de Rusia en 2007 que bloquearon departamentos oficiales, bancos y medios de comunicación, aunque nunca se demostró que el Kremlin coordinara la agresión. Un episodio que desembocó en conflicto diplomático y en la creación de un centro de análisis de ciberamenazas de la OTAN en territorio estonio, destinado a diseñar sistemas de defensa contra ataques en Internet. En el centro participa España junto a otros seis países. También Corea del Sur, además del padecido este mes de mazo, sufrió fuertes ataques cibernéticos en 2009 y 2011, de los que acusó a su vecino Corea del Norte.

En febrero de 2010 fue detectado un ataque informático a gran escala, mediante el virus *Zeus*, que afectó a más de cien países. De acuerdo con los datos de la empresa de seguridad NetWitness, el ataque permitió a los agresores, que no fueron identificados claramente, el control de 74.000 ordenadores, y los países más afectados fueron EEUU, Arabia Saudí, Egipto y Turquía. El *Zeus* capturaba contraseñas, cuentas de correo y redes sociales, y permitía el control remoto de los ordenadores para manejar cuentas corrientes, información financiera y toda clase de datos privados. Un año después,

Canadá denunció un ciberataque procedente de China que alteró el sistema de contraseñas del Ministerio de Finanzas. Pero las autoridades canadienses, a pesar de que las máquinas utilizadas estaban en territorio chino, no fueron capaces de asegurar que el ataque procediera del gobierno de Pekín, ya que, como es habitual en estos casos, los ordenadores pudieron ser manejados por control remoto.

Otra importante agresión fue la que sufrió Taiwan en septiembre de 2003 desde territorio chino continental, que afectó a dependencias gubernamentales, la Junta electoral y el Banco Central. Se considera el primer caso documentado de ciberguerra, puesto que los ataques contra la Serbia de Milosevic en 1998, durante la contienda de Kosovo, corrieron mayormente a cargo de ciberactivistas voluntarios de todo el mundo deseosos de poner freno a los crímenes de guerra de Belgrado.

EMPRESAS PRIVADAS

No todo son amenazas creadas por algunos Estados para atacar a otros. Grupos como *Anonymous* o *Lulzsec* han podido entrar en los sistemas informáticos de instituciones o compañías públicas para publicar datos comprometedores o información reservada. En agosto de 2011, *Anonymous* anunció que había logrado penetrar en los sistemas informáticos de unas 70 páginas web vinculadas a las fuerzas de seguridad de EEUU y el Reino Unido. La intención de *Anonymous*, una organización surgida en Internet que carece de estructura y tiene miembros en varios países, era publicar masivamente información confidencial para «humillar, desacreditar e incriminar» a la que califican de «cultura corrupta inherente a las fuerzas policiales» de Estados Unidos.

La ofensiva de *Anonymous* se consideró una venganza por las detenciones de 16 miembros de esa organización llevadas a cabo por el FBI en California, Florida y Nueva Jersey, a raíz de una serie de operaciones en las que colaboraron fuerzas de seguridad británicas, relacionadas con las filtraciones de *Wikileaks*. Las redes sociales, como *Twitter*, *Facebook* y *Apple*, ya han admitido haber sido víctimas de ataques, y *Google*, en 2010, denunció intrusiones en gran escala en su correo desde algún lugar de China. La amenaza ha llegado a la prensa. Periódicos como el *Washington Post* o el *Wall Street Journal* lo han reconocido abiertamente.

La aparición del virus *MiniDuke,* que busca información de inteligencia geopolítica, ha puesto también en alerta a la comunidad internacional, ya que al menos 20 países, entre ellos Ucrania, Bélgica, Portugal, Hungría y la República Checa, pueden haber sido sus víctimas. Se trata de un ataque innovador y muy diferente, aseguró un destacado investigador de seguridad de Kaspersky Lab.

Los piratas informáticos atacaron en esta ocasión al aprovechar un fallo en la herramienta utilizada para leer documentos en formato PDF. El ataque empieza al recibir un correo con un PDF adjunto sobre un tema de gran relevancia bien elaborado. Cuando el usuario abre el envío su ordenador puede ser monitoreado y descargado para obtener cualquier información buscada.

US Secretary of Defense

En los últimos años, el Pentágono ha aumentado de 900 a 4.500 su personal dedicado a ciberdefensa.

MANDO PROPIO

EEUU lleva muchos años desarrollando ciberarmas, pero la presidencia de Barak Obama ha acelerado esos trabajos con la creación de un mando propio. Los ataques cibernéticos tiene ya para Washington el mismo rango que las acciones de guerra con armas convencionales. En su último discurso sobre el estado de la Unión, el 13 de febrero, el presidente norteamericano enfatizó que uno de los principales objetivos de su gobierno es reforzar la defensa cibernética del país, y anunció una orden ejecutiva para combatir el cibercrimen y compartir con los proveedores de Internet estadounidenses las firmas digitales de los principales grupos dedicados a la piratería informática.

Una semana después, el fiscal general, Eric Holder, informó de la creación de un organismo especial para centralizar el trabajo de las distintas agencias de Inteligencia dedicadas a combatir el cibercrimen, y presentó una lista de ataques informáticos comprobados contra empresas privadas o departamentos estatales estadounidenses. En esa lista, China aparecía como el país de origen de la mayoría de tales ataques, y por tanto sería el blanco principal de la guerra contra el cibercrimen anunciada por la Casa Blanca.

La orden ejecutiva de Washington para reforzar la vigilancia en Internet estipula que las agencias federales notificaran sobre peligros informáticos a las empresas privadas, y establece un marco de seguridad cibernética destinado a blindar a todas las empresas consideradas cruciales en asuntos de seguridad nacional.

Por otra parte, a finales de febrero, el Tribunal Supremo de Estados Unidos rechazó una demanda de Amnistía Internacional, y otras organizaciones, contra un programa federal de vigilancia electrónica norteamericano creado después de los atentados de septiembre de 2001. Se trata de la Ley de Vigilancia de Servicios de Inteligencia Extranjeros para prevenir ataques terroristas. La sentencia implica que el gobierno norteamericano seguirá espiando las comunicaciones telefónicas y electrónicas de sus ciudadanos dentro y fuera del país sin órdenes judiciales. Con este fin Estados Unidos ha gastado 2.000 millones de dólares en desarrollar una gran instalación de espionaje. Es un inmenso centro de grabación repleto de servidores en el estado de Utah, que se terminará a medidos de este año y permitirá grabar todas las comunicaciones que entran y salen de EEUU por Internet, fax o teléfono. Unos 40 de los principales países del mundo tienen unidades de Inteligencia Cibernética y, sin duda, cada vez serán más.

Fernando Martínez Laínez