La guerra cibernética

Henning Wegener

La era de la información se desarrolla bajo la creciente amenaza de las intrusiones criminales en las redes. El abanico de posibles ataques pone de manifiesto la fragilidad de la sociedad actual y rebasa todo concepto territorial de la defensa nacional.

La digitalización de datos y las redes que conectan los modernos sistemas de información y comunicación se están convirtiendo en principios rectores del funcionamiento de la sociedad actual. Con ellos se abre una gama de posibilidades de almacenamiento, acceso y proceso de información y conocimientos desconocidos hasta hoy. Se estima que hay ya más de quinientos millones de ordenadores en el mundo y el volumen de datos transmitidos se duplica en menos de un año.

Cada día, millones de usuarios acceden de manera legítima a datos de cualquier lugar del mundo por medio de redes internas o a través de los diversos servicios que ofrece Internet (*world wide web*, *e-mail*, *telnet*, *ftp*, *IRC*, *usenet NEWS*). En el otro extremo, también crece la frecuencia de los accesos no autorizados por parte de individuos que se sirven de los canales mencionados para infligir daños a los sistemas de información y cuya importancia y significado no parece percibir la opinión pública, por más que las espectaculares hazañas de los *hackers* (intrusos informáticos) menudeen últimamente en los titulares de prensa. Las amenazas que para la comunidad internacional supone la vulnerabilidad informática de las sociedades civiles y sus infraestructuras de seguridad constituirán el objeto del presente artículo. Asimismo, se analizarán las iniciativas internacionales emprendidas para afrontarlas.

A los ataques malintencionados perpetrados a través de cauces electrónicos contra las bases de datos se les denomina guerra de la información o "ciberguerra". Dependiendo de sus fines, se habla de delincuencia o terro-

Henning Wegener ha sido embajador de Alemania en España (1995-99) y secretario general adjunto de la OTAN (1986-91).

rismo cibernético. Un intruso informático puede acceder y emplear información privada referida a determinado grupo al que no pertenece. De este modo, destruye la confidencialidad y, al mismo tiempo, la confianza en la seguridad que ofrecen las nuevas tecnologías, requisito básico para el correcto funcionamiento de la sociedad de la información. Más allá, el intruso puede manipular archivos introduciendo datos propios o alterando los existentes. Puede, también, reprogramar sistemas de información que controlan importantes procesos mediante la introducción de comandos falsos y destruir la integridad del sistema, o bien comprometer la disponibilidad de determinados datos suprimiéndolos o modificando los servicios que proporcionan, de modo que sistemas enteros dejen de funcionar.

Mediante el envío masivo de información, se puede bloquear un servidor temporalmente o hacer que quede por completo inservible (denegación de servicio). Para ello, el malhechor puede ordenar el envío simultáneo de programas no autorizados y autoinstalables a gran cantidad de ordenadores que no cuentan con la suficiente protección. Dichos programas, controlados remotamente, enviarán a su vez de forma masiva paquetes de datos que bloquearán e inutilizarán las redes al saturar su capacidad de procesamiento de información (denegación de servicio distribuida).

Los virus informáticos se pueden inocular en el sistema como portadores de un material nocivo que se transmitirá de archivo en archivo o, a mayor escala, irá infectando otros sistemas conectados a la misma red. Al pirata le es posible limitar la capacidad del ordenador que ataca, o bien alterar la lógica interna del sistema de manera que éste produzca respuestas absurdas cuando no nocivas (bombas lógicas). Directamente o a través del *software* al que se accede mediante descarga desde la red, se puede introducir en el sistema un virus del tipo "caballo de Troya" que actuará sobre él una vez transcurrido el tiempo determinado por el programador.

Igualmente, el pirata puede ocultar su identidad o falsificarla –modificando, por ejemplo, el remitente desde el que envía los paquetes de datos (*IP-Spoofing*)–, de forma que la autenticidad de determinados archivos quede destruida, o bien emplear un ordenador al que ha accedido como estación intermedia (*hopping station*) desde la que emprender nuevos ataques a terceros sistemas. Las medidas de defensa o represalia del sistema agredido podrían, de este modo, emplearse en contra de inocentes, lo que acarrearía numerosos problemas legales. Un ataque enmascarado por una o varias estaciones intermedias no sólo dificulta las medidas de defensa y la identificación del agresor, sino que, además, puede hacer imposible la ubicación geográfica del ataque.

Por otra parte, podría suceder que el presunto origen se localizara en un país en el que al malhechor no se le pueda incriminar porque aquél no participe en el desarrollo de la cooperación internacional en materia de protección de la información, ya que los delitos informáticos no conocen fronteras. También existe la figura del atacante pasivo, esto es, aquel basándose,

por ejemplo, en los conocimientos que le proporciona hallarse dentro del sistema o programando una serie de "funciones especiales" en el *software*, extrae de modo ilícito determinada información.

Espectro de amenazas

Respecto a los ataques que atentan contra la seguridad de la información, se pueden distinguir tres ámbitos:

En primer lugar, los perpetrados contra la redes de comunicación del sector económico. Precisamente, este sector está empleando cada vez más las redes de acceso público para interconectar sus sistemas informáticos. Aparte de las posibilidades de integración que aporta la actual tecnología (Intranet), las empresas tienden hoy a conectarse entre ellas. Todo eso constituye un valor económico capital, tanto más urgente será garantizar su seguridad y fomentar la confianza en este tipo de procesos entre empresas. Los ataques informáticos pueden facilitar el acceso a información reservada o, más grave aún, posibilitar la falsificación de datos (espionaje industrial, violaciones del *copyright*, piratería; véase el espectacular robo de datos personales y de grandes empresas en el Foro Económico Mundial en Davos el pasado febrero), amenazan algunos de los principios básicos de la competencia.

Sus repercusiones pueden extenderse hasta propiciar la falsificación de un entorno de decisión determinado y la consiguiente confusión de la dirección de las empresas, el fraude, el potencial de coacción, etcétera. Si se produce la temida denegación de servicio, algunas empresas pueden quedar paralizadas. El virus *I love you* inutilizó tres millones de ordenadores en todo el mundo y ocasionó daños que se calculan en torno a los 10.000 millones de dólares. Sólo en Alemania, los daños –registrados– por delitos informáticos han sido cifrados en unos cuarenta millones de euros anuales pero se estima que las repercusiones reales en su economía pueden ascender a los 10.000 millones de euros.

En segundo lugar, la política de defensa de la información respecto a los ataques perpetrados contra infraestructuras clave dentro de cualquier sociedad. La creciente digitalización implica que casi todos los aspectos de la vida se sometan hoy día al control y gestión de los ordenadores: los sistemas bancarios, con sus variantes *on-line* y su interconexión a escala global, los de distribución de electridad, los oleoductos, los sistemas de control y servicios sanitarios, que incluyen la gestión de grandes hospitales, la seguridad social, el tráfico aéreo y ferroviario, los servicios estatales de seguridad y protección (policía, bomberos), la regulación de presas y diques, etcétera. Un ataque a gran escala contra determinados componentes de estas infraestructuras sociales, bien sea provocando una situación de denegación de servicio por saturación de las redes o destruyendo los sistemas de control, po-

dría ocasionar a un país unos daños que agravados por la oleada de pánico que, a buen seguro, se desataría, harían peligrar el equilibrio de la sociedad. Los escenarios catastróficos en que se recrea la ficción dan una idea de la tremenda fragilidad que caracteriza a la sociedad actual.

En tercer lugar, si cabe aún más preocupante –y aquí es donde el término guerra de la información adquiere todo su sentido– es cuando los ataques se dirigen contra las estructuras de seguridad nacionales e internacionales. En la medida en que los servicios de información y telecomunicaciones de las fuerzas armadas dependan de la digitalización de los sistemas armamentísticos y de la computerización de los centros de mando, y que las operaciones se planifiquen en campos de batalla virtuales –y ésa es la tendencia actual de la moderna "revolución de los asuntos militares"– que pueden ser objeto de un ataque informático, mayor será el peligro y más amplia la gama de sus posibles escenarios.

El virus I love you *inutilizó tres millones de ordenadores en todo el mundo*

Las estrategias de violación en este ámbito van de la simple lectura –es decir, el acceso a importante información militar de carácter estratégico o táctico– a la introducción de datos erróneos en los sistemas del rival; la inoculación de virus silenciosos (*stealth viruses*) o mutantes, indetectables en ambos casos; la manipulación de sistemas de control de determinado armamento; la inutilización de los sistemas de radar y detección vía satélite y el colapso de importantes redes informáticas, en particular las que se relacionan con los centros de mando. Las denominadas operaciones de información, que se ocupan de calibrar todos los aspectos de un posible ataque contra la información y las funciones informativas del rival, además de garantizar su propia protección están adquiriendo una importancia cada vez mayor en la política de defensa de las grandes naciones y de la OTAN. Asimismo, algunos países del Tercer Mundo y China están desarrollando sus sistemas de "ciberdefensa".

No se trata sólo de perfeccionar los sistemas nacionales de información y garantizar la protección contra ataques informáticos, sino también de procurarse la posibilidad, en caso de crisis, de compensar los desequilibrios armamentísticos y, en último extremo, de poder llevar a cabo operaciones militares con una menor participación humana. El hecho de que al comienzo de las operaciones de la OTAN en Kosovo cientos de *hackers* trataran de penetrar en los sistemas de información de la Alianza, o de que en 1998 otros lograran acceder a los ordenadores del Pentágono y se apropiaran de miles de claves, muestra en qué medida pueden ser reales algunos de los escenarios planteados. Es precisamente desde la perspectiva de la política de seguridad donde queda claro que la ciberguerra supera y relega el pensamiento tradicional en materia de seguridad, concebido sobre una base territorial.

En la era de la informática ya no hay cabida para los Estados que se dediquen únicamente a defender sus fronteras con medios militares.

Los límites entre estos tres grandes ámbitos son, en último extremo, permeables. Un ataque a gran escala contra la economía, con los consiguientes efectos nocivos o el colapso de determinadas infraestructuras estatales provocado por agresiones informáticas, tiene tanta importancia para la seguridad nacional como la neutralización de determinados sistemas militares o las posibles y peligrosas consecuencias de un mal funcionamiento provocado. Un atacante a cuenta de un país beligerante combinaría, sin duda, sus "ciberoperaciones" de modo que afecte al mayor número de objetivos.

Las técnicas ofensivas se pueden emplear en cualquier lugar. Los ataques en contra de la seguridad informática se caracterizan por un enorme –y creciente– desequilibrio entre la causa y el efecto: una acción nimia ocasiona tremendos daños. Un solo "ciberterrorista" con un ordenador portátil conectado a Internet puede provocar una catástrofe. Así, las autoridades estadounidenses en materia de seguridad, con la ayuda de unos pocos expertos informáticos, han podido adentrarse en centrales de control de distribuidoras eléctricas de su país o acceder a los mandos militares, lugares contra los que les habría resultado perfectamente posible comenzar cualquier tipo de ataque. ¡Para inutilizar las estructuras militares digitales de todo un país se emplean hoy día bits en vez de bombas! Por otra parte, las técnicas de ataque no sólo se desarrollan a una gran velocidad; además, resultan cada vez más sencillas de utilizar. Los piratas informáticos no dejan de descubrir los puntos débiles de los sistemas informáticos y de distribuir información que facilite el comienzo de ataques contra éstos por canales públicos como Usenet, listas de correo y páginas *web* desde los que cualquiera puede descargarla sin la menor traba e, incluso sin ser un gran experto, emplearla como guión para un efectivo ataque informático.

Resulta plausible pensar que muchas de estas acciones de piratería dadas a conocer últimamente no han sido sino la travesura de unos jóvenes con ansias de experimentación y sin intención de hacer daño. Sin embargo, las dirigidas hacia objetivos políticos crece a diario en volumen y calidad. Y lo malo es que las mismas posibilidades técnicas están al alcance de empresas competidoras, criminales financieros, terroristas, sectas como Aum Shinrikyo y Estados rivales. Necesariamente, los denominados Estados "delincuentes" se habrán interesado ya por el desarollo de este tipo de operaciones ofensivas. Pero, al igual que sucede con los "ciberataques" a gran escala, no es sencillo diferenciar entre malhechores al servicio de un Estado y piratas independientes.

El fácil acceso a estas técnicas, junto al enorme crecimiento del número de ordenadores conectados a las redes, ha llevado a que, en los países donde ya se están investigando y registrando estos actos, la cifra de ataques se duplique cada año y haya alcanzado magnitudes millonarias.

El perfil del problema define, asimismo, las medidas que deben adoptarse: protección contra ataques, prevención de éstos, sobre todo los emprendidos contra infraestructuras y estructuras de seguridad clave de la sociedad, medidas de defensa oportunas en caso de ataque, dispositivos policiales y sanciones penales. Los conceptos objeto de protección parecen claros: la seguridad, autenticidad, integridad e identidad de los datos, así como la disponibilidad permanente de los sistemas. Igualmente, garantizar la confianza del ciudadano en la seguridad de los sistemas de información y la fiabilidad de los datos se antoja un requisito básico para el funcionamiento de la economía y, más ampliamente, del conjunto de las sociedades democráticas, y resulta una condición cada vez más necesaria para la seguridad nacional.

Protección, defensa y prevención

La protección contra "ciberataques" es una tarea en la que el usuario individual, la industria informática, la de servicios, el sector económico en general y las agrupaciones internacionales deben colaborar para consolidar el desarrollo del concepto integrado de seguridad común. En primer lugar, debe desarrollarse una conciencia del peligro que supone esta amenaza y de las medidas de seguridad que son necesarias para contrarrestarlo. Para esto falta aún un largo trecho: un reciente análisis muestra, por ejemplo, que en Alemania únicamente el cuatro por cien de las empresas encriptan su correo electrónico o que sólo el uno por cien provee a todas sus comunicaciones de protección encriptada. Pero es de suponer que en cuestiones de defensa se tenga mayor conciencia del problema.

Existen al respecto medidas de protección, defensa y prevención. Éstas, no obstante, se hallan ante el viejo y controvertido dilema armamentístico entre ataque y defensa. En vista de que, en su confrontación, ambos disponen de la misma tecnología en progreso, el problema de la protección técnica no ha dejado ni dejará de plantearse: no hay sistema informático que esté completamente a salvo de ataques y, de hecho, la tendencia concede ventaja a los agresores, máxime desde el momento en que el acceso inalámbrico a las redes se puede efectuar con un teléfono móvil.

Los usuarios finales pueden servirse de unas sencillas técnicas previas de protección (contraseñas, control de acceso, evaluación de la integridad del sistema, procedimientos de encriptado y firmas digitales), en las que se combinan claves de identificación públicas y privadas y a las que se concede certificación oficial, garantizan la seguridad en el intercambio comercial y procuran cierta protección contra la delincuencia cibernética. Además, es importante aislar mediante cortafuegos las redes internas de contactos con las públicas, focos habituales de ataques, si bien esto no ofrece protección contra los perpetrados desde dentro del sistema.

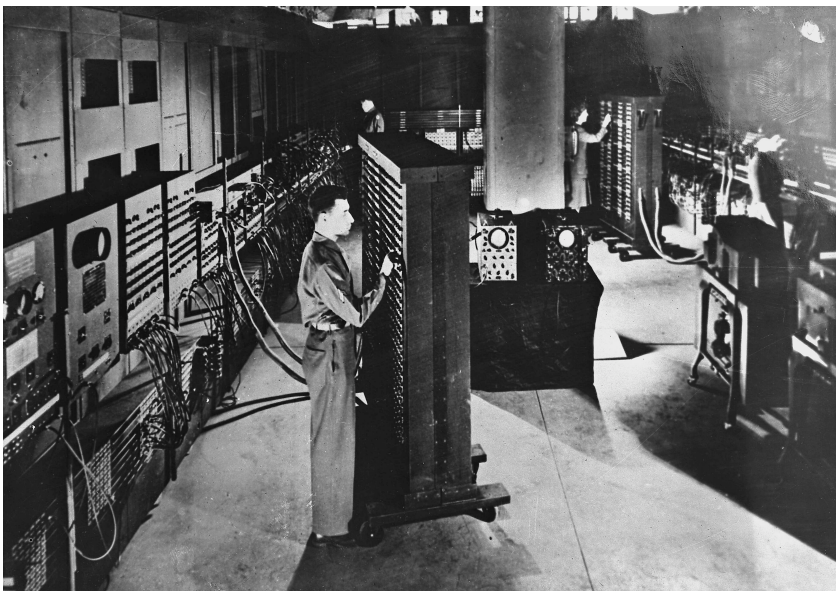
Los programas antivirus son efectivos únicamente si se les somete a una constante actualización; del mismo modo, para evitar el ataque contra puntos débiles del propio sistema o del servidor, resulta preciso garantizar una revisión permanente y asegurar el principio de redundancia de la información para evitar su pérdida. Las medidas automáticas de detección de ataques (*intrusion detection systems*, IDS) han alcanzado un gran nivel de desarrollo; se encargan de detectar anomalías en el sistema teniendo en cuenta multitud de parámetros, si bien identifican únicamente modelos de agresión conocidos. Habitualmente, los IDS operan en combinación con los IRS (*intrusion response systems*), cuyas medidas suelen consistir en la desconexión total o parcial del sistema o la reparación automática de daños. De cualquier modo, ninguno de los métodos descritos es del todo efectivo.

La estenografía constituye una técnica de cifrado prácticamente imposible de violar. Consiste en la manipulación de la información que se pretende ocultar tras datos de acceso normal (datos "envoltorio") con una pequeña alteración de su estructura binaria. De este modo, se pueden ocultar y transmitir, por ejemplo, hasta cuarenta páginas de texto confidencial en un complejo gráfico de color. El cifrado y la posterior recuperación de los datos se efectúan a través de algoritmos que resisten a las técnicas de descifrado. El problema de la estenografía digital estriba en que es una técnica también al alcance del agresor, de modo que éste se puede servir de ella para introducir "caballos de Troya" en cualquier sistema.

No hay ningún sistema informático que esté por completo a salvo de ataques

Mientras que en los sistemas de información y comunicación de determinadas infraestructuras clave, y en particular en las instalaciones militares, el interés por la seguridad es evidente y no precisa ningún tipo de estimación de rentabilidad, las empresas privadas son muy cuidadosas a la hora de calcular el coste de sus inversiones en seguridad en relación con las posibles pérdidas en caso de un ataque informático. En una encuesta realizada por el FBI, el 75 por cien de las empresas decía haber sufrido ataques informáticos; en el 59 por cien de los casos, las pérdidas superaban los 400.000 dólares. Por ello, no sorprende que el mercado de seguridad informática, el "criptomercado", presente un índice de crecimiento anual del sesenta por cien.

Estados Unidos lidera actualmente el sector, con un 56 por cien de cuota de mercado. Sin embargo, el índice de crecimiento europeo en los últimos años es superior. En 1999 se comercializaron unos 1.700 "criptoproductos" en más de 35 países. El mercado global de la seguridad informática podría alcanzar este año un volumen de negocio cercano a los 30.000 millones de dólares. En aras de la seguridad de la información, varios Estados han vencido sus primeras reticencias en contra de los productos de encrip-



VIOLLET

Piratas en la red, asalto al poder

tado. Ya en 1997, la Comisión Europea se manifestó a favor del libre comercio en este sector. Desde 1999, este tipo de productos se fabrica y comercializa en Alemania sin ninguna traba. En EE UU se permite desde hace unos meses la libre exportación de productos encriptados a sus principales socios comerciales.

Junto a los usuarios que tratan de proteger sus sistemas de manera individual, el deber de colaborar en la defensa, reconocimiento e identificación de ataques cibernéticos ha de recaer igualmente en los otros agentes de la cadena tecnológica: los productores de *software* y "criptoproductos", los operadores de telecomunicaciones en la red y los servidores (PSI), en resumidas cuentas, en toda la denominada comunidad de tecnología de la información. Resulta obvio su interés por garantizar la seguridad y la confianza en los sistemas informáticos. Asimismo, pueden desempeñar un papel crucial en la eliminación de los ataques (evitando la propagación de paquetes de datos falsos, filtrando determinada información, colaborando en el establecimiento de protocolos defensivos, eliminando puntos débiles en el sistema). Algunos de estos sectores económicos se han unido ya en varios países para combatir la delincuencia informática europea e internacional (EuroISPA, European Internet Services Providers Association; Business Software Alliance).

Como nexo entre la ciencia y la economía, los equipos de respuesta informática urgente (*computer emergency response teams*, CERT), de financiación mayoritariamente pública, son hoy día cruciales en todos los siste-

mas de intercomunicación de los países industrializados. Desde estos puntos de recepción de alarmas y denuncias de ataques informáticos se proporciona asesoría respecto a la puesta en práctica de medidas protectoras, se ofrece ayuda en caso de daños, se coordina y supervisa la detección de los responsables, se detectan los puntos débiles del sistema, etcétera. El centro de coordinación CERT se halla en Pittsburgh, Pensilvania. En España operan los centros IRIS-CERT y ESCERT; en Alemania el centro de organización mixta privada-universitaria DFN-CERT perteneciente al Consejo de Investigación alemán y el BSI-CERT –de gestión pública– dirigido por la Oficina Federal de Seguridad en la Técnica de Información.

Actuación estatal

La seguridad informática es una obligación inexcusable de la administración pública a la que ésta ha de dar cumplimiento en solitario por mor de la protección de sus infraestructuras clave y que, en muchos aspectos, se ha de entender como una tarea conjunta con el sector económico. El Estado ha de proporcionar el marco legislativo, obrar de modo preventivo a fin de evitar todo tipo de vulnerabilidad (apoyo en el desarrollo de sistemas de seguridad, estrategias de seguridad informática para infraestructuras clave y autoridades interconectadas, concienciación ciudadana), establecer medidas policiales, garantizar la imposición de sanciones penales a los criminales informáticos y fomentar la cooperación internacional en todos los ámbitos descritos.

Los Estados se están esforzando, en diversa medida, por cumplir con estas tareas. Al respecto deberían darse algunos ejemplos que sirvieran para analizar, en primer lugar, la actual situación –y los déficit aún por solucionar– de los proyectos internacionales de cooperación. Los países cuentan hoy día con legislaciones marco relativas a los servicios de información y comunicación (en Alemania, por ejemplo, la ley de información y telecomunicaciones entró en vigor en 1997), en las que se regulan los servicios que debe prestar el ofertante, la protección de datos, las cuestiones referidas a la propiedad intelectual y las medidas generales de protección.

En la mayoría de los Estados, la actual legislación civil y penal permite la tramitación de los delitos perpetrados con ayuda de medios cibernéticos siempre que éstos se ajusten a la definición de figuras previas; el ciberespacio jamás ha sido un espacio sin ley, ni aun en sus comienzos. Los medios electrónicos ya están incluidos en las disposiciones del Código penal y otras legislaciones sancionadoras relativas a delitos económicos, contra el patrimonio y de violación de la confidencialidad. Sin embargo, los delitos verdaderamente nuevos están aún pendientes de definición. Los mecanismos de supervisión y los sistemas de coordinación policial han mejorado notablemente (así, en Francia, se ha creado una dirección central de seguridad interministerial para los sistemas de información y, recientemente, una ofici-

na central para la lucha contra la delincuencia informática dependiente de la policía judicial).

En Alemania operan conjuntamente varios ministerios y oficinas: el Bundeskriminalamt se encarga de la delincuencia en Internet, el Bundesnachrichtendienst atiende a las amenazas provenientes del exterior y el Bundesamt für Sicherheit in der Informationstechnik vela por la protección de las estructuras clave. El ministerio federal del Interior coordina todas las tareas "Sicheres Internet" (Internet seguro). Como queda patente, Alemania ha apostado por la coordinación y el desarrollo interdisciplinar.

En España, la policía nacional y la comisaría general de policia judicial colaboran en este tipo de actividades desde hace algún tiempo. Una unidad de investigación de la delincuencia en tecnologías de la información asume no sólo las competencias policiales relativas a los delitos cibernéticos y en las telecomunicaciones, sino que opera, además, en coordinación con unidades de trabajo menores del Centro Superior de Investigación de la Defensa (Cesid) y con la guardia civil. La tarea de gestionar la cooperación internacional recae, asimismo, sobre esta unidad, al igual que la elaboración de estudios y trabajos destinados a fomentar la seguridad en la información.

Los nuevos delitos están aún pendientes de su tipificación legislativa

Aunque sólo fuera en virtud de su enorme asignación financiera, merecen mención las directivas presidenciales 62 y 63 de EE UU en esta materia. Desde mayo de 1998 –con la adopción de la 63 sobre infraestructura crítica– la magnitud de la amenaza y las vulnerabilidades que pone de manifiesto la delincuencia cibernética se han convertido en un asunto de primer orden. Un coordinador junto al Consejo de Seguridad Nacional de la Casa Blanca, al que corresponde una Critical Infrastructure Assurance Office en el departamento de Comercio, se encarga de dirigir las relaciones dentro de la administración y de canalizar la correspondencia con el sector económico. La gran inversión puesta en juego ilustra la importancia que Washington concede al problema. En el ejercicio presupuestario de este año se le han asignado 2.060 millones de dólares (en 2000, 1.750 millones), de los cuales 616 millones se destinarán a I+D en los grandes centros estatales, veinticinco millones a becas sobre seguridad cibernética y buena parte de los recursos restantes para el blindaje de las infraestructuras informáticas de las autoridades federales, haciendo hincapié en el aparato de defensa.

Con independencia del modo en que cada Estado calibre la magnitud de las amenazas provenientes del ciberespacio y de las normas que se adopten al respecto, se acabarán por imponer unos estándares e índices de protección globales. Hasta el momento, las iniciativas nacionales resultan del todo deficitarias. Precisamente, el carácter global del problema

exige la adopción de reglamentos universales resultado de una estrecha colaboración internacional. Prevención, información, alarma ante ataques, protección y eventuales medidas de defensa, al igual que una serie de sanciones y medidas de retorsión deben funcionar a escala transfronteriza conforme a unos estándares uniformes. De este modo, se eliminarán los actuales "cibersantuarios".

Primeros pasos hacia una ordenación internacional

Trataremos de describir, en primer término, el estado actual de los esfuerzos emprendidos, entre los que se incluyen las actividades e iniciativas de las organizaciones y alianzas internacionales constituidas con objeto de establecer una jurisdicción mundial de signo cooperativo que regule la lucha contra la delincuencia cibernética. Corresponderá después evaluar las posibilidades que se derivan de la actual legislación internacional respecto a los Estados –en particular cuando uno de ellos es el que comete delito– que no participan en el desarrollo de dicho marco legal.

Parece oportuno comenzar con las actividades del G-8 (Grupo de los siete países más industrializados más Rusia). El interés de este grupo por las opciones de una legislación mundial en materia de información se plasmó el año pasado en la Carta de Okinawa sobre la sociedad global de la información y en la creación de un grupo de trabajo sobre oportunidades digitales. Desde el G-8 se han apoyado los esfuerzos por lograr un "ciberespacio libre y sin delincuencia" y se ha mostrado a favor de proteger las infraestructuras clave de la información, en colaboración con la industria.

Ya en 1997, los ministros de Justicia e Interior del G-8 reconocieron la necesidad de adoptar medidas y presentaron un plan de acción. Las conferencias específicas organizadas el pasado año (París en mayo; Berlín en octubre) trataron de manera especial los mecanismos de enlace: creación de una red de información de veinticuatro horas con centros de contacto nacionales que procuren ayuda ante indicios de posibles delitos electrónicos; fortalecimiento de la Interpol, de modo que se encargue de la supervisión de dicho sistema de enlace; ampliación del ámbito de competencias de la Europol para incluir entre ellas la persecución de la delincuencia electrónica; prestación de ayuda jurídica mutua; propuesta de los primeros estándares técnicos de seguridad. Dichas recomendaciones ya se están llevando a la práctica. En el caso de la Interpol, se precisa la aquiescencia de los 178 Estados asociados; para la Europol basta una resolución del Consejo de Ministros de la Unión Europea (UE). Las recomendaciones del G-8, en las que se convoca la ayuda de otras naciones, suponen un primer paso para la creación de redes preventivas de enlace y cooperación, pero todavía es necesario que se les confiera un carácter operativo. Con todo, la red de enlace ha

probado ya su buen funcionamiento en numerosos casos. Al G-8 se han adherido ya otros cinco países miembros de la UE.

Los ataques cibernéticos contra sistemas nacionales de seguridad son sólo en ciertos aspectos una cuestión de colaboración internacional en los ámbitos jurídico, político y policial. Su inhibición y defensa se sitúan tras las propias prioridades de la seguridad nacional. Cabe mencionar, asimismo, el papel de la OTAN en este tipo de situaciones. La seguridad de la información y la protección de las infraestructuras digitales son cuestiones de la mayor importancia para las autoridades militares de cada nación. Lo mismo sucede con la Alianza, en la que una consulta continua entre sus miembros se considera imprescindible.

La OTAN opera conforme al concepto genérico e integrado de las operaciones de información, bajo las que se engloban los mecanismos de protección eficaz de las infraestructuras de información propias y la destrucción o inutilización de las estructuras enemigas y, con ello, su capacidad de decisión y maniobra. Las operaciones de información abarcan, pues, todo lo relacionado tanto con la información y sus estructuras (operaciones psicológicas, política de información al público), como la guerra de la información o la potencia de comando y control que, en su vertiente ofensiva, se dirige a los dispositivos de mando del enemigo y, en la faceta defensiva, se ocupa de la preservación de la integridad y la optimización de los recursos propios. En 1999, el grupo de trabajo de las operaciones de información (NIOWG) redactó el documento básico MC-422, en el que se describen todos los posibles aspectos relacionados con el empleo y protección de los nuevos sistemas de información y las disposiciones necesarias para su correcto funcionamiento.

Marco jurídico

Una de las variantes de la "ciberguerra" que más costes puede acarrear a sus víctimas potenciales es la piratería, es decir, el robo y posterior uso ilícito de material protegido legalmente. Las enormes posibilidades de difusión y acceso a la propiedad intelectual, protegida por el *copyright* y otros derechos, que implican las nuevas redes digitales suponen, del mismo modo, un peligro para la integridad de esos derechos. Se ha hecho, pues, necesaria la adaptación a las nuevas circunstancias de las disposiciones internacionales en esta materia, en particular el Convenio de Berna redactado de conformidad con el Protocolo de París de 1971. La Organización Mundial de la Propiedad Intelectual (WIPO) ha asumido la tarea de modernización, la cual ha quedado plasmada en dos acuerdos, el WIPO Copyright Treaty y el WIPO Performances and Phonograms Treaty –conocidos como los "tratados de Internet"– ambos de 1996. En ellos se define el almacenamiento y la difusión de datos en medios electrónicos como una reproducción que precisa de per-

miso legal. Los autores disfrutan en exclusiva del derecho de autorizar en qué modo y a través de qué canal *on-line* debe transmitirse su trabajo para llegar al público. Los programas informáticos y las bases de datos disfrutan asimismo de protección intelectual. Los Estados firmantes están obligados a garantizar una adecuada protección jurídica y técnica contra la piratería y la violación de las medidas técnicas (encriptado, *watermarking*) que afectan a los autores en relación con la propiedad de sus obras. Para que ambos tratados entren en vigor se precisa la ratificación de treinta Estados, una cifra de la que, a día de hoy, apenas se ha alcanzado la mitad. Por otra parte, no está muy claro cuántos de entre los Estados firmantes han adaptado sus legislaciones nacionales a las disposiciones enunciadas en los tratados.

En el mismo sentido, una de las iniciativas más relevantes a escala internacional ha partido del Consejo de Europa, donde desde 1997 se está trabajando en la elaboración de un convenio sobre delincuencia cibernética que sería el primer proyecto importante de recopilación de medidas sancionadoras contra delitos informáticos. Su interés es, si cabe, mayor dado que, al trabajo emprendido por los 41 miembros del Consejo, se han incorporado Estados Unidos, Canadá, Rusia, Japón y Suráfrica y que, al margen de la sistemática clasificación criminal de los diferentes ataques informáticos, se están incluyendo disposiciones relativas a la persecución legal, la colaboración transfronteriza en materia de Derecho penal y el marco común de asignación de penas.

El Consejo de Europa trabaja desde 1997 en un convenio sobre delincuencia cibernética

El proyecto, que se halla actualmente en su vigésima quinta revisión (PC-CY (2000) Draft. núm. 25 Rev. 5, de 22-12-2000) ha llegado a la última fase de negociación y se espera la aprobación definitiva por parte del Consejo de Ministros del Consejo de Europa para su posterior firma a escala mundial este año. El convenio contiene disposiciones vinculantes para los Estados que se han de adoptar –de forma armonizada– en el ordenamiento jurídico penal y procesal de cada nación. Las disposiciones de Derecho penal sustantivo se agrupan en cuatro tipos de delitos: contra la confidencialidad, integridad y accesibilidad de los datos y sistemas informáticos (acceso y empleo no autorizado, sabotaje, alteración parcial del funcionamiento del sistema); relativos a los datos informáticos (falsificación, fraude); sobre el contenido (difusión de pornografía infantil); y contra la propiedad intelectual (refuerzo de las sanciones penales en caso de violación de las normas WIPO). Se trata de legitimar el acceso a determinados datos informáticos por parte de la policía y los tribunales y de definir técnicamente el proceso. La posibilidad de acceder a datos con contenidos ilegales según la legisla-

ción de un determinado país, asunto en el que nos concentraremos más adelante, resulta particularmente controvertida.

El convenio prevé la colaboración internacional en forma de prestación de ayuda mutua, intercambio de información, cooperación en cuestiones relacionadas con disposiciones transitorias y –en el marco de lo establecido por el G-8– la constitución de una red de enlace que opere las veinticuatro horas del día. Este proyecto supone una extraordinaria base para el desarrollo de unos estándares universales y un marco jurídico global en el que quede definida la lucha contra la delincuencia cibernética, si bien no puede conjurar –más allá de cuestiones legales– el peligro que suponen los ataques contra infraestructuras esenciales para la sociedad o contra la seguridad de las naciones.

A partir de 1997, la UE se viene ocupando de la delincuencia informática en diversos documentos del Consejo de Ministros, si bien, hasta la fecha, éstos han sido sobre todo análisis y estudios (COMCRIME de 1998) y una propuesta de armonización en el ámbito del Derecho penal (Consejo Europeo de Tampere). A excepción de una resolución del Consejo en contra de la pornografía infantil en Internet, se echan en falta actos jurídicos en esta materia. Hasta la reciente comunicación de la Comisión al Consejo y al Parlamento Europeo, del pasado 26 de enero, con el título de "Creación de una sociedad de la información más segura mediante la mejora de seguridad de las infraestructuras de información y la lucha contra los delitos informáticos", (COM (2000) 890 final) en la que se recogen propuestas realizadas por una serie de Estados miembros, entre ellos España, no se había llegado a una posición amplia que permitiera la adopción de medidas eficaces.

La comunicación, en la que, por otra parte, se ofrece un detallado análisis de los actuales déficit de los desiguales ordenamientos jurídicos nacionales, propone la adopción de las siguientes reglas: aproximación de las legislaciones de los Estados miembros en los delitos relacionados con la pornografía infantil; mayor aproximación del Derecho penal en la delincuencia de alta tecnología (en seguimiento de los dictámenes del Consejo); aplicación del principio de reconocimiento mutuo de los autos anteriores al juicio asociados con las investigaciones de delitos informáticos; la institución de un foro de la UE que obre como recopilador de información y promotor de futuras acciones conjuntas. Por otra parte, la comunicación de la Comisión contiene una serie de propuestas dirigidas a los Estados miembros y trata, asimismo, de establecer las bases de una posible colaboración con otras instituciones internacionales. Con todo, y pese al importante esfuerzo analítico que refleja, el programa resultante, ahora bautizado "Plan de Acción Europa 2002", sigue pecando de cierta modestia.

A fin de reflejar el espectro completo de las organizaciones internacionales, no podemos dejar de referirnos a la Asamblea General de las Naciones Unidas. Desde 1998, la ONU ha tratado la seguridad de la información –en el contexto de la seguridad internacional– en diversas resoluciones (la

más reciente, A/Res/55/28). No obstante, éstas no son más que una toma de conciencia del peligro que supone este nuevo tipo de amenaza y se incluye un llamamiento a las naciones a comunicar al secretario general de la ONU sus reflexiones en materia de seguridad de la información y la lucha contra la delincuencia y el terrorismo de alta tecnología.

Estos esfuerzos emprendidos por la comunidad internacional para combatir los ataques informáticos por cauces jurídicos y a través de acciones conjuntas parten de un modelo cooperativo y de un creciente consenso en materia de adopción de medidas a escala internacional. Sin embargo, si se comienza un ataque desde un país que (aún) no se haya incorporado al consenso mundial, o si, directamente, dicho país es el causante del ataque, de poco sirven los instrumentos de esta política cooperativa: el agresor no podrá ser detenido para que dé cuenta de sus actos. En casos como el descrito, al Estado agredido, obrando en beneficio de sus ciudadanos, no le queda más recursos que la diplomacia (en forma de presión política o de denuncia pública), el Derecho internacional (medidas de retorsión o, en determinados casos, represalias) y las posibilidades que confiere la Carta de las Naciones Unidas.

Si las agresiones son de gran magnitud, se plantea la cuestión de en qué momento un ataque informático se adecúa a la definición de empleo de violencia, y activa, con ello, las medidas sancionadoras previstas en el capítulo VII de la Carta. La cuestión del empleo de violencia no parece ofrecer dudas –y, por consiguiente, el contraataque quedaría justificado– si se tratara de un ataque informático a las infraestructuras militares del Estado agredido, o bien si los ataques a instalaciones aeroportuarias, presas, etcétera afectan a vidas humanas. Aunque las cuestiones relativas al tipo de contraataque lícito en estos casos, a la correlación entre la magnitud del ataque y la de la respuesta, así como a las medidas preventivas permitidas hayan sido recogidas en diversos estudios, sigue siendo necesario un tratamiento en profundidad del asunto para desarrollar soluciones consensuadas.

Tareas pendientes

Queda todavía mucho por recorrer en el camino hacia una sociedad de la información global y abierta, en la que se explote en beneficio de todos el potencial que ofrecen las nuevas tecnologías y donde se conjure con éxito la amenaza que supone la guerra de la información para la economía, el buen funcionamiento de las modernas sociedades y la seguridad nacional e internacional. Ya hay muchos Estados que han reaccionado de forma responsable y la economía y las fuerzas sociales se han movilizado con decisión. Con todo, el trabajo aún por hacer es difícilmente imaginable: algunos conflictos siguen sin resolverse debido a la inexistencia de una regulación internacional que todavía no se ha sido creado por falta de tiempo. También está pen-

diente de aclaración el alcance de las amenazas relacionadas con la guerra cibernética en las materias de Derecho internacional en caso de conflicto y, por ello, no procede ahondar en la cuestión. Sí merecen atención los siguientes puntos:

El factor tiempo y la universalidad. Los esfuerzos por adoptar una legislación internacional –por parte del Consejo de Europa o de la WIPO– dependen de una serie de factores íntimamente ligados al tiempo. Actos jurídicos como el Convenio sobre delincuencia cibernética están sujetos al compromiso de los Estados. La ratificación y la adopción por parte de las legislaciones nacionales de los países firmantes requieren, sin embargo, una gran –y, a menudo, desigual– cantidad de tiempo. De este modo, hasta que dichos elementos supranacionales se hayan incorporado a la legislación de los Estados firmantes, se hace necesaria la adopción de medidas prácticas de carácter urgente que regulen la lucha contra la delincuencia cibernética. Por otra parte, habrá que solventar la dificultad que plantea la diversidad de culturas jurídicas y las no menos desiguales percepciones del problema si se pretende alcanzar la necesaria universalidad.

La diversidad de culturas jurídicas complica la adopción de normas de alcance universal

Atribución y jurisdicción. En vista de la casi infinita capacidad de elección con que cuenta el delincuente cibernético respecto al sistema desde el que comienza el ataque, sigue sin resolverse la cuestión de los criterios conforme a los que éste ha de atribuirse a un Estado u otro. Esto es vital a la hora definir la jurisdicción y –más aún– para las cuestiones relativas a las retorsiones y represalias.

Asuntos prácticos de la cooperación internacional. Aun cuando exista unidad de principios, la capacidad operativa de los centros de control supranacionales evoluciona lentamente a consecuencia de la obligatoria adopción de un formato común.

Lucha contra la delincuencia y derecho a la libertad. Las nuevas tecnologías de la información potencian el debate en el seno de todas las democracias respecto al equilibrio entre los derechos privados y la creciente necesidad pública de persecución legal, ya que los nuevos sistemas de información permiten al malhechor ampararse en los principios de la intimidad, la confidencialidad de la información, el derecho al anonimato y la protección de datos. El debate ha comenzado con la necesidad de los Estados de limitar la encriptación de los datos o de asegurarse el acceso a las claves, el poder de interceptar información y de infiltrarse en los procesos, el de procurarse el acceso a datos individuales almacenados o requerirlo de los proveedores de servicios, y el derecho, en definitiva, de recortar el derecho de las personas físicas a la intimidad en el acceso y empleo de los servicios de la red.

En el desarrollo del Convenio sobre la delincuencia cibernética se ha prestado especial atención al concepto de interceptación, y éste volverá a aparecer en el momento en que los Estados firmantes procedan a adaptarlo a sus legislaciones nacionales. Los representantes de las organizaciones de libertades civiles ya han dejado oír su voz al respecto. Los fabricantes de *software* y los portavoces de la industria de seguridad informática se han manifestado a favor de una protección menos estricta de la integridad de los sistemas de información y comunicación aduciendo que la experimentación y evaluación de sus puntos débiles y la discusión pública que se suscita al respecto siguen siendo muy importantes a la hora de mejorar la eficacia de los sistemas de protección. En el otro extremo, los *hackers* vienen identificando su intrusión en las redes como un acto revolucionario en el que se manifiesta la transparencia de las modernas sociedades democráticas en la era de la información. Para solucionar estos conflictos será preciso esforzarse por alcanzar un compromiso equilibrado entre todas las posturas descritas.

Delitos cibernéticos relativos al contenido. Las enormes posibilidades que ofrecen los nuevos medios, en particular Internet, para la difusión de contenidos como pornografía infantil, propaganda racista, incitación al odio, la violencia o al consumo de drogas, suponen un problema legal adicional de difícil solución. En sentido estricto, no se trata de delitos informáticos, ya que únicamente se distribuye material, hecho que no afecta a la integridad de las redes o los sistemas. Desde la UE se defiende el punto de vista según el cual, si el material es ilegal fuera de la red, debe ser, asimismo, perseguido penalmente cuando se halla dentro de ésta.

En el caso de la pornografía infantil el consenso internacional es unánime: su difusión, y así queda recogido en el Convenio de Estrasburgo sobre la delincuencia cibernética, debería ser punible en todo el mundo. Tratándose de otros materiales, la cooperación no está asegurada, por más que la persecución internacional sea el único modo de inhibir la difusión a escala nacional. Baste recordar las dificultades del gobierno alemán para atajar la difusión de propaganda racista procedente de EE UU. En este punto están involucrados varios planteamientos, por una parte, la defensa de la libertad de expresión y, por otra, los temores de que la justificación de una política intervencionista dé pie a los Estados donde se disfruta de menores libertades a censurar todo tipo de contenidos que puedan parecer inconvenientes a los gobiernos. En resumen, resulta urgente alcanzar un consenso internacional conforme al cual se desarrollen unos criterios unitarios relativos a la persecución criminal de los materiales cuyos contenidos resulten claramente inadmisibles.