DELITOS EN INTERNET: CLASES DE FRAUDES Y ESTAFAS Y LAS MEDIDAS PARA PREVENIRLOS

Gemma Sánchez Medero
Profesora de la Universidad Complutense de Madrid

La enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos está haciendo que éstas sean más vulnerables a los posibles ataques cibernéticos y el fraude en la Red. Además, Internet es un medio de fácil acceso, donde cualquier persona, sin tener que relevar su identidad, puede proceder a realizar un ataque que es complicado de asociar, virtualmente indetectable y difícil de contrabandear, por no hablar de alto impacto que alcanza una acción de este tipo al golpear directamente y por sorpresa al adversario. Con lo cual, la Red se está convirtiendo en ese lugar ideal para que los delincuentes lleven a acabo sus acciones y actividades. Por tal razón, a la lo largo de este artículo nos hemos dedicado a estudiar el uso que cada uno de estos actores están haciendo de Internet (clases de estafas y fraudes) y que medidas se están tomando para evitar los posibles ataques cibernéticos y las actividades delictivas, comprando que están obteniendo un resultado parcialmente positivo.

Introducción

Las Tecnología de la Información y el Conocimiento (TIC) han ocasionado una revolución sin precedentes cuyo alcance todavía es insospechado. La globalización está sacudido los pilares de las instituciones y las bases de nuestra sociedad, hasta el punto de sugerir el nacimiento de otra sociedad paralela –a la meramente física– que se conoce como Sociedad de la Información y del Conocimiento. El ciberespacio se está convirtiendo en un punto de encuentro para millones de personas, gracias a su flexibilidad en el uso y a la cantidad de información que pone a disposición de los usuarios. Y esto indudablemente está contribuyendo a que la Red no deje de crecer, llegándose incluso a afirmar que su aparición ha marcado un antes y un después en la era de la información y la comunicación.

Es más, hoy en día todo parece estar interconectado, los sistemas de seguridad, defensa, comerciales, energéticos, sanitarios, comunicación, transporte, bancarios, alumbramiento, bibliotecarios, etc. De tal manera que nos encontramos ante un mundo hiperconectado, donde la Red es un elemento crucial y vital para las sociedades más avanzadas. Pero a pesar de los avances que ha podido suponer no todo ha sido positivo, ya que la Red está favoreciendo el surgimiento de nuevos problemas a los que tiene que hacer frente la sociedad. Así, los términos cibercrimen, ciberdelitos, ciberdelincuencia, ciberterrorismo o ciberguerra se están haciendo un hueco entre nosotros, hasta tal punto que los ciudadanos están aprendiendo a convivir con esta nueva realidad, ya que cada vez está siendo más frecuente encontrar noticias sobre algún hecho ilícito que se ha producido a través de la Red. De ahí que a lo largo de este artículos hayamos marcado como objetivo estudiar las actividades que están realizando los delincuentes en la Red, y que soluciones se están dando y buscando para intentar contrarrestar este tipo de actividades delictivas.

La presencia de los delincuentes y criminales en la Red

La ciberdelincuencia es aquella actividad que emplea los ordenadores o las redes como una herramienta delictiva (1). De ahí, que el ciberdelito suponga un peligro, tanto para los ordenadores como para la información recogida a través de ellos. Más cuando en la mayoría de los países del todo el mundo no existen leyes contra este tipo de delitos, y por no hablar que esta tecnología proporciona a los delincuentes rapidez, comodidad y anonimato. En cualquier caso entre este tipo de delitos cabe destacar: el acceso ilegal a sistemas ajenos, la intercepción ilegal, la interferencia y la pérdida de datos, la interferencia de sistemas, la pornografía infantil, los delitos contra la propiedad intelectual, el robo, la extorsión y el fraude electrónico, etc.

---

(1) La Convención sobre la Ciberdelincuencia del Consejo de Europa define los delitos informáticos como «los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.» *Council of Europe Convention on Cybercrime*, número 185, disponible en: *http;//conventions.coe.int*.

Obtener dinero de forma fraudulenta

Tal vez el más corriente de los fraudes a través de la Red sea el *mail spoofing* y la *web spoofing*. El primero es un procedimiento mediante el cual se pretende suplantar el correo electrónico de un usuario o crear correos electrónicos supuestamente verídicos a partir de un dominio para poder enviar mensajes como si formasen parte de esa identidad. Por ejemplo, cada vez es más frecuente encontrar en nuestros correos mensajes de una entidad bancaria como el Banco Bilbao-Vizcaya-Argentaria o la Caja de Ahorros para el Mediterráneo que dispone de una dirección correo electrónica que solemos identificar con *nombre@bbva.es* o *nombre@cam.org*. En estos mensajes los presuntos clientes suelen recibir la siguiente información:

> «Este mensaje fue enviado automáticamente por nuestro servidor para verificar su dirección de correo electrónico. A fin de validar su dirección de correo electrónico, por favor haga clic en el enlace de abajo.»

De esta manera, obtienen la dirección de su correo electrónico y sus datos, pero también es común que el *mail spoofing* se emplee como una estratagema de ingeniería social para solicitar el número de las tarjetas de crédito a determinados usuarios confiados, que piensan que la procedencia del mensaje se deriva supuestamente de la propia empresa de la que son clientes. El segundo, consiste en una técnica de engaño mediante la cual se hace creer al internauta que la página que está visitando es la auténtica cuando en realidad se trata de una réplica exacta de la misma, pero que se encuentra controlada y monitorizada por un ciberdelincuente que pretende extraerle información y dinero, dependiendo, si se limita a seguir, vigilar, leer y grabar todas las actividades que realice el usuario, o bien, si se dedica a manipular algunos de los datos o, simplemente, le sustrae dinero o utiliza estos datos para efectuar compras en su nombre.

Otro de fenómeno relacionado con este aspecto sería los ciberocupas, que son aquellos individuos o empresas que registran para sí dominios asociados a marcas, empresas o instituciones con la intención de obtener un beneficio revendiéndolo a su propietario legítimo. Otra cuestión son las llamadas telefónicas, un fraude que se realiza entre el módem del ordenador y el proveedor de Internet. Este proceso se realiza habitualmente mediante un nodo local de modo que la tarifa telefónica a pagar le corresponde a una llamada local, de ahí, que el fraude consista en desviar

inadvertidamente la llamada del nodo local a otros prefijos de tipo comercial muchos más caros.

Otro tema es el cibersexo, uno de los negocios más rentables de la Red, ya que la libertad de acceso y el supuesto anonimato contribuye a este hecho. El sexo en Internet no esta penalizado, siempre y cuando cumpla con todos los requisitos legales. El problema es que éste se convierte en ilegal cuando hacemos referencia a la pornografía infantil, o la venta de sexo sin consentimiento a través de Internet, o cuando se engaña a los clientes haciéndoles creer que el acceso a los contenidos de sus páginas es gratuito, cuando son tarifados por una línea de alto coste.

Otro lugar frecuentado por los ciberdelincuentes son los portales de subastas, desde los cuales se ofrece un gran surtido de productos y servicios. El problema es que en la mayoría de las ocasiones estos productos pueden ser falsos o, simplemente, son adquiridos por un comprador pero nunca le son entregados, es decir, pagar sin recibir nada a cambio. La venta de productos farmacéuticos es otro espacio permisible para el fraude. En España la comercialización de medicamentos está prohibida por Internet, sin embargo, cada vez es más frecuente acudir a este medio para hacerse con una serie de productos que en nuestro país sólo pueden ser adquiridos bajo preinscripción médica.

Pero los ciberdelincuentes también se están valiendo de la Red para vender estupefacientes y crear verdaderos mercados temáticos sobre las drogas con una información muy diversas: suministrar, bajo un precio, información sobre todo tipo de actividades ilícitas como, por ejemplo, las debilidades de sistemas de alarma y antirrobo, trucos sobre cómo abrir un coche, asaltar una casa, burlar los sistemas de seguridad, etc., ofrecerse para adentrarse en los sistemas o los ordenadores de empresas o instituciones para robarles, manipular o dañar los datos a cambio de dinero; robar información para después venderla al mejor postor, crear foros dedicados exclusivamente a la compra-venta de datos robados, como números de tarjetas de créditos y otros elementos relacionados con el fraude, sólo mencionar algunos casos.

La estafa nigeriana es otro fraude dentro de esta categoría. Éste consiste en enviar mensajes electrónicos para pedir ayuda a los destinatarios, y de esta forma poder transferir importantes cantidades de dinero a terceros con la promesa de darles un porcentaje si aceptan esa operación a través de sus cuentas personales. Piden también que les transfieran a su nom-

bre una pequeña cantidad de dinero para verificar los datos de la cuenta bancaria con la que se hará la transacción, o que simplemente les envíen los datos de la cuenta bancaria. Una vez que envíen el dinero, las víctimas no volverán a saber nunca más nada de esos estafadores.

Bloquear páginas web

Consiste en adentrarse en las *web* de instituciones, organizaciones, empresas o gobiernos para paralizarlas durante un determinado tiempo con el fin de generar caos, confusión e incertidumbre. Tal vez, el más conocido haya sido el protagonizado por Estonia el 27 de abril de 2007, cuando las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reformas quedaron bloqueadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos estuvieron inaccesibles durante varias horas por una serie de ataques Distribuidos de Denegación de Servicio, DDoS *(Distributed Denial of Services).* Hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallin de un monumento de la época soviética.

Pero también los que se produjeron durante el conflicto bélico entre Rusia y Georgia. Los mismos tuvieron como consecuencia que distintas páginas *web* gubernamentales se viesen comprometidas, con continuos ataques de denegación de servicio distribuidos contra otras páginas del Gobierno, teniendo como resultado la migración de ciertos sitios a servicios de *posting* de Estados Unidos. Incluso un grupo de ciberactivistas proruso proporcionó ayuda en su página oficial para potenciar a los usuarios de Internet con herramientas para realizar ataques distribuidos de denegación de servicio, proporcionar una lista de páginas georgianas vulnerables a inyección SQL y publicar una lista de direcciones de correos de políticos georgianos para ataques dirigidos y *spam* (2).

Propagar malware

La cantidad de *malware* y la evolución de sus técnicas de infección y propagación se han incrementado de manera considerable a través de los últimos años. No obviemos, que cuando hablamos de *malware* pode-

(2) Informe Cibercrimen de 2008, en: *http://www.s21sec.com/descargas/S21sec-ecrime-Informe-Cibercrimen-2008.pdf*

mos hacer referencia a un virus, un caballo de Troya, una puerta trasera *(backdoor)*, un programa espía *(spyware),* o un gusano. Además, a causa de un *malware* puede derivarse otros ataques como puede ser: DDoS, distribución de correo *spam*, propagación de virus y gusanos hacia otras redes, sitios *phishing*, expansión de *botnets* (redes de equipos comprometidos), fraudes de banca electrónica, *pharming* y *driving*, entre otros muchos otros (Fuentes, 2008; p. 4).

Difamación e información falsa

Internet puede utilizarse para la divulgación de información errónea con la misma facilidad que la información fidedigna. Los sitios *web* pueden contener información falsa o difamatoria, especialmente en los foros y salas de charla donde los usuarios pueden publicar sus mensajes sin la verificación de los moderadores. La difamación puede dañar la reputación y la dignidad de las víctimas en un grado considerable, dado que las declaraciones en línea son accesibles por la audiencia mundial. Aunque la información se corrija o se suprima poco después de su publicación, puede haber sido duplicada «en servidores espejo» y esté en manos de personas que no desean retirarla o suprimirla.

Robo de identidad

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada *IP Spoofing*, mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección *IP* correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado. Otro posible ataque sería el secuestro de sesiones ya establecidas, lo que se conoce como *hijacking*, donde el atacante trata de suplantar la dirección *IP* de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir.

Con el secuestro de sesiones, se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes, siempre que en ese momento se encuentra conectado al servidor de una entidad financiera. Pero también, se pue-

de enviar mensajes con remitentes falsos, *masquerading*, para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente. O simplemente se puede capturar las contraseñas, y suplantar la identidad de la persona atacada, o conectarse a conexiones pertenecientes a otras personas.

Espionaje informático

El espionaje consiste principalmente en la obtención no autorizada de datos almacenados en algún fichero automatizado, con lo cual se produce una violación del secreto de información. Para ello, se suele emplear distintas técnicas como, por ejemplo, el «pinchado de líneas» o *wiretapping*, que consiste en la intercepción programada de las comunicaciones que circulan a través de las líneas telefónicas, con el objetivo de procurarse ilegalmente información. O, la «recogida de información residual», que es fruto del propio descuido del propio usuario por no mantener mínimas medidas de seguridad.

¿Cómo intentar reducir los peligros en la Red?

Realmente está resultado sumamente difícil poder encontrar soluciones que resulten efectivas para intentar poner freno a todas aquellas actividades relacionadas con el cibercrimen y la ciberdelincuencia.

La primera solución

Desconectar al ordenador de la Red, aunque está parece totalmente imposible ante unas sociedades que también cada vez se hayan más hiperconectadas.

La segunda solución

Identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto sólo se puede conseguir con la ciberinteligencia. El problema que se plantea es que Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos; además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, etc., máquinas populares de acceso a Internet y otras donde de forma anóni-

ma las personas puede conectarse y realizar actividades ilícitas. Lo mismo ocurre con las redes inalámbricas libres al alcance de equipos con conexiones capaces de conectarse a esas redes con el anonimato de la no pertenencia al grupo autorizado (Ruiloba, 2006; p. 53).

Pero éstas no son las únicas dificultades a las que deben hacer frente los policías cuando realizan investigaciones en la Red. Por ejemplo, cuando los posibles delincuentes saben que una máquina está comprometida por ser accesible a través de una conexión pueden convertirla en una *work station virtual* para navegar a través de su dirección sin ser detectados; o cuando utilizan las máquinas cachés de algunos proveedores de comunicaciones para optimizar su rendimiento, ya que garantizan el anonimato de los usuarios para delinquir (Ruiloba, 2006; p. 53).

En todo caso, para evitar estas posibles deficiencias jurídicas están tipificando gran cantidad y variedad de delitos informáticos. Por ejemplo, en nuestro país son considerados como delitos, el ataque a datos y a redes, así como la intercepción de datos. Además son castigados penalmente: la modificación, el borrado, la destrucción o la alteración y el acceso no autorizado a bases de datos, textos o programas mediante el *cracking* y la diseminación de virus. O en Estados Unidos la legislación federal, de fecha 15 de abril de 2002, establece penas para: el acceso no autorizado de sistemas informáticos, previendo específicamente el acceso a sistemas del Gobierno relacionados con la seguridad de Estado, por lo que se encuentra castigada la comunicación, la entrega, la transmisión e incluso el sólo intento de realizar los actos antes mencionados; el uso de cualquier computador de uso oficial o que se esté utilizando en algún momento como oficial que afecten al gobierno; y el acceso de computadoras sin la autorización, o quien tenga acceso a la misma se exceda del permiso que obtuvo (Orta Martínez, 2005).

El problema es que la mayoría de las legislaciones están vigentes en los diferentes países están dirigidas a proteger básicamente la utilización indebida de la Red, incluso algunas de ellas prevén la creación de órganos especializados que protejan los derechos de los ciudadanos, pero poco más. Ahora el Convenio sobre Cibercrimen (3) contiene contenidos de diverso carácter como, por ejemplo, delitos de intrusión en el que se integran infracciones penales contra la confidencialidad, integridad y dis-

(3) Convenio sobre Cibercrimen del Consejo de Europa, celebrado en Budapest, 23 de noviembre de 2001.

ponibilidad de datos y sistemas informáticos, delitos patrimoniales (falsificaciones y fraudes a través de Internet como *phishing* y *pharming*), delitos de contenidos en el que exclusivamente se incluyen delitos de corrupción de menores en su modalidad de pornografía infantil, y delitos de infracción de la propiedad intelectual y derechos conexos que comprende todos los delitos contra la propiedad intelectual y de los derechos afines según la legislación de cada parte, y otros delitos entre se produzcan en Internet.

La tercera solución

Dotarse de medios de seguridad, aunque siempre considerando que existe la posibilidad de que sean vulnerados. Pero establecer una buena política de seguridad en el ciberespacio exige constituir primero un lugar de partida, que debe consistir en analizar los riesgos y las amenazas, para después conocer sus puntos fuertes y sus vulnerabilidades. Después hay que construir un marco normativo que regule la seguridad en el ciberespacio, y en el que intervengan todas las partes. Posteriormente, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable que sea capaz de coordinar a todas las entidades públicas y privadas implicadas en esta materia. Y todo ello, sin olvidar la cooperación internacional a este respecto y fomentar una cultura de ciberdefensa y una promoción de la investigación en el sector de la ciberseguridad. El problema es que los Estados están haciendo más o menos eso, pero de una forma desorganizada y descoordinada, moviéndose a rachas, lo que está conduciendo a que cada país haga la guerra por su cuenta y de una manera precipitada, lo que reducen notablemente la eficiencia de sus estrategias de seguridad nacional e internacional.

La cuarta solución

Intentar adelantarse a cualquier acto delictivo mediante el control de los Sistemas de Información, como pueden ser: Echelon, Enfopol y Carnivore.

SISTEMA ECHELON

Un Sistema automatizado de intercepción global de trasmisiones operado por los servicios de inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Su objetivo inicial era

controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados durante la guerra fría. Aunque en la actualidad se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar tramas terroristas y planes de narcotráfico, inteligencia política y diplomática. Su funcionamiento básico consiste en situar innumerables estaciones de intercepción electrónica en satélites y en otros puntos para capturar las comunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Después cada estación selecciona, mediante la aplicación de unas palabras claves, toda aquella información que guarda relación con el fin que persigue el Sistema Echelon.

Además, cada uno de los cinco países que componen el Sistema facilitan a los demás «diccionarios de palabras claves» para que los incorporen como «filtros automáticos» a los aparatos de intercepción de las comunicaciones. Lógicamente estas «palabras claves» y «diccionarios» varían con el tiempo y de acuerdo con los intereses particulares de los países integrantes del Sistema.

SISTEMA ENFOPOL

Es consecuencia directa del deseo de los gobiernos europeos de no quedarse atrás en esta carrera de escuchas cibernéticas. Por esta razón, pusieron a funcionar su propio plan de interceptación de telecomunicaciones en: Europa, Estados Unidos y Australia, pero también en otros países. Enfopol intenta imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tenga acceso total a las comunicaciones de sus clientes, así como a la información sobre los números marcados y los números desde los que se llama. En el caso de Internet, los proveedores deben facilitar «una puerta de atrás» para que puedan penetrar a sus anchas por los sistemas privados.

Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas) (Añover, 2001). Todo sin que sea necesaria una orden judicial (Añover, 2001). Pero todavía es más exigente para la criptografía. Se pide que sólo se permitan este tipo de servicios siempre que estén regulados desde un «tercero de confianza», que deberán entregar automáticamente cuando le sea solicitado: la identificación completa del usuario de una clave, los servicios que usa y los parámetros técnicos del método usado para implementar el servicio criptográfico.

SISTEMA CARNIVORE

Es la generación de los sistemas de espionaje de redes de la Oficina Federal de Investigación (FBI). Un sistema que ha sido diseñado por el FBI para capturar aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la Agencia. Se especula incluso que sea capaz de espiar el disco duro del usuario que se considere sospechoso y, todo ello, sin dejar rastro de su actividad. Para ello, se coloca un chip en los equipos de los proveedores de servicios de Internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos, así cuando encuentra una palabra clave, eso sí con el visto bueno de la Corte, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hacen a sitios de la Red y las sesiones de *chat* en las que participa. Esto junto con el control de las direcciones de *IP* y de los teléfonos de conexión, permite la detección de lo que consideran «movimientos sospechosos» en la Red (Busón, 2009).

La quinta solución

La creación de ejércitos de cibersoldados para intentar garantizar los sistemas informáticos de sus respectivos países.

ALEMANIA

La Unidad Estratégica de Reconocimiento del Ejército alemán ha coordinado un equipo de soldados que están involucrados en el ensayo de nuevos métodos de infiltración, manipulación y explotación –e incluso de destrucción– de las redes informáticas. Por ello, este equipo está aprendiendo a instalar *software* maliciosos en ordenadores sin el conocimiento de los usuarios, robar contraseñas y datos confidenciales, etc.

ESPAÑA

El Ejército de Ciberdefensa de las Fuerzas Armadas españolas está compuesto por militares especialistas en telecomunicaciones e informática, que han hecho cursos avanzados, militares y civiles, en seguridad de las TIC, al mismo tiempo que se han incorporado ingenieros superiores civiles de la Ingeniería de Sistemas para la Defensa de España, S. A., especializados también en seguridad cibernética. Su entrenamiento con-

siste en asaltar los ordenadores enemigos, mientras que defienden los propios, dentro de una red creada expresamente para ello.

ESTADOS UNIDOS

Ha reunido un grupo de *hackers* de elite que se estarían preparado para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como JFCCNW *(Joint Functional Component Command for Network Warfare)*, una unidad que se cree que está integrada por personal de la Agencia Central de Inteligencia (CIA), la Agencia Nacional de Seguridad, el FBI, las cuatro ramas militares, algunos civiles expertos y representantes militares de naciones aliadas. Tiene la responsabilidad total de defender la Red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información, dañar las comunicaciones rivales hasta inutilizarlas y trabajar con una variedad de socios fuera y dentro del Gobierno de Estados Unidos. Un comando que tiene como contraparte el Grupo Especial de Tareas para la Libertad de la Internet Global, GIFTF *(Global Internet Freedom Task Force)* en sus siglas en inglés), una organización multiagencias subordinada al Departamento de Estado.

Además, con vista a la implantación de un sistema planetario de guerra ciberespacial y el lanzamiento del primer mando militar múltiple del mundo, el mando del Equipo Operativo Conjunto de la Red Global de Operaciones del Departamento de Defensa de Estados Unidos fue disuelto oficialmente para pasar a integrarse en el nuevo Cibermando (en inglés, CYBERCOM).

Éste servirá para fusionar el abanico de operaciones que lleva a cabo el Departamento de Defensa en el ciberespacio, y sus funciones serán liderar la defensa diaria, proteger las redes de información, coordinar las operaciones del Departamento de Apoyo a las Misiones Militares, dirigir las acciones y defensa de redes de información especificadas por el Departamento de Defensa, etc. Así, el USCYBERCOM centraliza el comando de operaciones ciberespaciales y fortalece las capacidades ciberespaciales del Departamento de Defensa. Además, el Cibercomando de la Fuerza Área (AFCYBER) ha creado también programas específicos de ciberguerra, entre los que se incluye: adversario, un sistema de objetivo de guerra de la información de la Fuerza Aérea; y ARENA, un programa de simulación «basado en objeto» para crear estudios por país; como casi tres docenas de otros programas y/o ejercicios de ciberguerra.

CHINA

En el pasado, el papel previsto para las fuerzas de reserva era el de apoyar al Ejército de Liberación Popular (ELN) en la defensa contra cualquier intervención extranjera. En cambio, hoy en día tienen la capacidad para emplear armas electrónicas y de información para alcanzar a un adversario en otro continente (Thomas, 2001). Por ello, entre sus funciones se encuentran: interrumpir el sistema de información, sabotear la estructura para la conducción de operaciones, debilitar la capacidad para contrarrestar una ofensiva, dispersar las fuerzas, armas y fuego del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuego de las unidades propias, confundir al contrario y lanzar simultáneamente una ataque sorpresivo de información para que tome una decisión errónea o bien realizar una acción equivoca (Thomas, 2001; p. 76).

Además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares y ha creado escuelas que se especializan en la guerra informática. También está contratando a graduados en informática para desarrollar sus capacidades en la guerra información y, así, crear un ejército de *hackers* civiles. Todo, tal vez porque los chinos se han dando cuenta que, de momento, no pueden ganar a Estados Unidos en un guerra convencional y, por tanto, están buscando nuevos campos de batalla donde puedan ser superiores, como en el ciberespacio (Brookes, 2007).

La sexta solución

El establecimiento de organismos gubernamentales destinados a luchar contra los posibles ataques cibernéticos. En este sentido, habría que mencionar que un gran número de gobiernos están creando Oficinas de Seguridad Informática para desde la legalidad combatir al cibercrimen, al ciberterrorismo y a la ciberguerra.

ESTADOS UNIDOS

Se creó la CIAO *(Critical Infrastructure Assurance Office)*, NIPC *(National Infrastructure Protection Center)* y el US-CERT *(United States-Computer Emergency Readiness Team)* para salvaguardar las redes de infraestructuras y los sistemas del país de los ataques cibernéticos, identificar las vulnerabilidades, difundir información sobre alertas de amenazas de seguridad, y coordinar las actividades de respuesta antes de incidentes

cibernéticos. Además, en el Departamento de Defensa existen muchas iniciativas tanto de los tres Ejércitos como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas como la Agencia de Seguridad Nacional. Esta Agencia, por ejemplo, tiene un departamento encargado del aseguramiento de la información, NSAIDA, que se centra en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad. Además, el Departamento de Defensa financia el CERT-CC que tiene como misión principal establecer un foro de coordinación entre los CERT nacionales.

Asimismo, con la llegada de Obama se han reforzado todo este tipo de iniciativas relacionadas con la ciberseguridad. Por ejemplo, ha elaborado un informe sobre la seguridad cibernética que servirá para luchar contra los delitos informáticos y el robo de información confidencial, o ha anunciado el nombramiento de un responsable de ciberseguridad que formará parte del Consejo de Seguridad Nacional en la Casa Blanca, o ha ordenado al Pentágono que preparé la creación de un nuevo mando especializado en la ciberguerra (4).

Además, después del 11 de septiembre de 2001 (11-S) Estados Unidos cambió su estrategia de seguridad centrándola en: el establecimiento y reordenación relativas a la seguridad del territorio, el desarrollo de la legislación relativa a la Seguridad Nacional y la ciberdefensa, la implantación de planes y estrategias relativas a la Seguridad Nacional, y la ejecución de ejercicios periódicos en ciberseguridad. Además, se apuesta por la colaboración con otros Estados, tal es así, que Estados Unidos ya está enlazando algunos ordenadores de defensa con los de sus aliados, incluso se están llegando a acuerdos de intercambio de información, tecnología e inteligencia con sus aliados.

FRANCIA

Se ha creado la Autoridad Nacional de Seguridad de los Sistemas de Información para vigilar las redes informáticas gubernamentales y privadas, con el objetivo de defenderlas de ataques cibernéticos. Sus funciones

(4) «La Conferencia de Seguridad de Múnich», *Documento Informativo*, Instituto Español de Estudios Estratégicos (IEEE), febrero de 2011.

son: la detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes; el desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos; el asesoramiento de seguridad a organismos gubernamentales y operadores de infraestructuras críticas; la difusión de información a empresas y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación. Este organismo dependen la Subdirección de Estrategia y Reglamentación, el Centro de Formación y el Centro Operacional de la Seguridad de los Sistemas de Información (COSSI), que son los responsables de la realización de las inspecciones y auditorías de seguridad a sistemas gubernamentales, las misiones de desarrollo de productos de cifra, los ejercicios que evalúen la seguridad, el despliegue de los sistemas de detección, y la coordinación de la respuesta gubernamental.

En el COSSI se encuentra además, el Centro de Expertos del Gobierno en el Tratamiento de Ataques Informáticos (CERTA), creado en el año 1999, que facilita la aplicación de buenas prácticas y mejora la atención a los usuarios en todo el territorio. Pero el Gobierno francés también ha elaborado el *Libro Blanco de la Seguridad y Defensa Nacional* (5), donde se contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar como son: el conocimiento y la previsión (con la necesidad de mejora de las capacidades técnicas de las agencias de inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

REINO UNIDO

Ha decidido crear el Centro de Operaciones de Ciberseguridad y la Oficina de Ciberseguridad, para supervisar la protección de importantes sistemas de tecnología de la información usados por el Gobierno británico y el sector privado, y para coordinar las medidas de ciberseguridad de todos los departamentos gubernamentales, respectivamente. El primero será una entidad multidepartamental con sede en Cheltenham, y ligado al GCHQ *(Government Communications Headquarters)*. Desde el que se

(5) *Livre Blanc Sur la Défense et la Sécurité Nationale*, en: *www.livreblancdefenseetsecurite.gouv.fr/information*

proporcionará protección coordinada a los sistemas de infraestructuras críticas del país. La segunda, coordinará las políticas y supervisará el programa de trabajo entre las distintas agencias gubernamentales. Estos dos Centros formaran parte del I Plan Estratégico de Ciberseguridad del Reino Unido, donde también se contemplará la creación de un grupo de asesores técnicos, y el establecimiento de las líneas estratégicas de seguridad cibernética del país: reducción del riesgo del uso del ciberespacio por el Reino Unido actuando sobre la amenaza, las vulnerabilidades y el impacto; aprovechamiento de las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y que actué contra los adversarios, y, por último, el impulso de una doctrina sobre el ciberespacio.

ALEMANIA

Se ha creado la Oficina Federal de Seguridad de la Información, dependiente del Ministerio Federal de Interior. Sus funciones son la protección de las redes del Gobierno federal, el desarrollo de productos de cifra, el análisis de nuevas tecnologías, la seguridad de los productos *software*, la protección de infraestructuras críticas, y el soporte del CERT para ciudadanos y pequeñas y medianas empresas. Además se ha aprobado un Plan Nacional de Protección de Infraestructuras de la Información (6), donde se establece como objetivos la prevención (las actividades críticas son divulgar información sobre riesgos y posibilidades de protección o empleo de productos y sistemas confiables), la preparación (las actividades son recolectar y analizar la información para proporcionar alertas y avisos) y la reacción (mejorar las capacidades técnicas propias y desarrollar productos con tecnología nacional). Además, a partir de abril de 2011, el Gobierno alemán abrirá un Centro Nacional de Ciberseguridad para defenderse de los ataques cibernéticos externos a sus infraestructuras críticas. También podrá en marcha un Consejo de Ciberseguridad Nacional, para mejorar la cooperación entre el Estado y los representantes del sector financiero y económico.

---

(6) Federal Ministry of the Interior: «National Plan for Information Infrastructure Protection», Berlín, 2005, en: *www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure_Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.*

ESPAÑA

A lo largo de los últimos años, se han tomado acciones para incrementar la seguridad del ciberespacio. En nuestro país, el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, tiene la responsabilidad de gestionar la seguridad del ciberespacio dependiente de cualquiera de los tres niveles de las Administraciones públicas (Fojón, 2010). Entre sus funciones cabe destacar: elaborar y difundir normas, instrucciones y recomendaciones para garantizar la seguridad de las TIC en la Administración; formar el personal de la Administración especialista en el campo de la seguridad de las TIC; constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito; valorar y acreditar la capacidad de productos de cifras y Sistemas de las TIC; coordinar la promoción, el desarrollo, la obtención, la adquisición y la puesta en marcha de las tecnologías de seguridad de los sistemas antes mencionados; velar por el cumplimiento de la normativa, y establecer las relaciones necesarias con otros actores e instituciones.

A nivel nacional, también existen otros organismos con competencias en la materia: el Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio de Interior, son responsables de combatir la delincuencia que se produce en el ciberespacio, etc. A nivel autonómico, existen centros homólogos a los referidos a nivel nacional, que igualmente tienen responsabilidades en la gestión de la ciberseguridad en su ámbito territorial. Además, a nivel internacional nuestro país forma parte de las organizaciones que promueven la defensa del ciberespacio, como, el Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) y en organismos como la Agencia Europea de Seguridad de las Redes y la Información (ENISA), *Antiphising Working Group* y *Data Protection Working Party.*

UNIÓN EUROPEA

Ha creado la ENISA, con sede en Heraklion (Grecia), para ayudar a los Estados miembros a obtener unos niveles altos de seguridad, asesorando técnicamente y prestando asistencia a los Estados miembros, así como a las instituciones de la Unión Europea sobre las cuestiones vin-

culadas a la seguridad de las redes y de la información, y fomentando la cooperación entre el sector público y privado. Para garantizar estos objetivos, las tareas de la Agencia (7) consiste, principalmente, en: acopio y análisis de datos relativos a aspectos vinculados a la seguridad y a los riesgos emergentes; cooperación con los distintos protagonistas, creando asociaciones entre el sector público y el privado con empresas que ejercen sus actividades en la Unión Europea y/o a nivel mundial; sensibilizar a los usuarios en la problemática de la seguridad de las redes y de la información, y promover métodos de evaluación de riesgos y mejores prácticas con el fin de encontrar soluciones interoperativas de gestión de los riesgos; el seguimiento del desarrollo de las normas sobre productos y servicios en la Sociedad de la Información y en las redes; asistir a la Comisión y a los países de la Unión en el diálogo que mantienen con las empresas para gestionar los problemas de seguridad; y presentar sugerencias.

Su estructura gira en torno al Consejo de Administración, el director ejecutivo, y el grupo permanente. La primera está compuesto por representantes de los Estados miembros y de la Comisión, así como de las empresas y expertos universitarios en la materia, y consumidores sin derecho al voto. A través de esta institución, los Estados miembros pueden formular sus necesidades en relación a esta materia. El segundo es nombrado por el Consejo de Administración a partir de una lista de candidatos propuestos por la Comisión. El tercero lo forman las partes interesadas, y es creado por el director ejecutivo y está compuesto por representantes de las empresas, los consumidores y expertos universitarios.

Así, viendo esta organización se podría concluir que ENISA es el centro neurálgico para fomentar el intercambio de información y cooperación entre todas las partes interesadas (organismos de la Unión Europea, miembros de la Unión Europea: Estados, la industria, el mundo académico y las organizaciones de consumidores de interés) en el campo de la seguridad en el ciberespacio. Además, en diciembre de 2002 la Unión Europea aprobó la Estrategia Europea de Seguridad, pero será en su revisión, en diciembre de 2008, cuando se recoja un apartado dedicado a las nuevas amenazas y riesgos, la seguridad de los sistemas de información.

---

(7) En: *http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_es.htm*

Pero, además, para incrementar la ciberseguridad, la Unión Europea ha decidido crear un centro dedicado a la defensa frente al cibercrimen en el año 2013. Su misión será coordinar la cooperación entre los Estados miembros, las instituciones europeas y los socios internacionales (Cabanillas, 2010). También se está contemplando la puesta en funcionamiento de un sistema de alerta y compartición de información, cuyo objetivo será facilitar la comunicación entre los equipos de respuesta urgente y las autoridades policiales. Asimismo, se pretende poner en marcha en 2012, la Red de Equipos de Respuesta Informática Urgente, CERTS *(Computer Emergency Response Teams)*, de la que existirá una por país miembro. Por otra parte, la Comisión y la Unión Europea han anunciado la creación, junto con las autoridades estadounidenses, de un grupo de trabajo dedicado a la ciberseguridad, que empezará a proporcionar información al respecto a partir de 2010 (Cabanillas, 2010).

LA OTAN

Ha creado en Tallin (Estonia) el Centro de Excelencia para la Cooperación en Ciberdefensa, cuyo objetivo es estudiar ciberataques y determinar las circunstancias en las que se deben activar el principio de defensa mutua de la Alianza Atlántica. En la actualidad forman parte de él: España, Italia, Alemania, Eslovaquia, Estonia, Letonia, Estados Unidos, Hungría, Italia, Lituania y Turquía. Su misión será, según se manifiesta en su memorándum fundacional, proteger a los Estados de los ciberataques, entrenar a militares, investigar técnicas de defensa electrónica, desarrollar un marco legal para ejercer esta actividad, dar respuesta y soluciones globales a problemas concretos, y para ello, los proyectos son acometidos por equipos multidisciplinares, en los que se involucran al personal experto en ciberseguridad, y especializado en tres ramas: asuntos operativos, funcionales y militares; asuntos tecnológicos, académicos y científicos; y asuntos legales. Este Centro depende jerárquicamente de un Comité de Dirección compuesto por representantes de los países componentes y de la OTAN, y tiene el estatus legal de Organización Militar Internacional.

La séptima solución

La propuesta realizada por algunos investigadores estadounidenses de crear Internet 2. Una red separada de la Internet comercial, que une labo-

ratorios y universidades de todo el mundo, y que trabaja en el desarrollo de los sistemas de transmisión de información a grandes velocidades y a través de la fibra óptica (Sánchez Medero, 2009). Pero a diferencia del Internet comercial:

> «Internet 2 estará extraordinariamente regulado y una Comisión Federal de Comunicaciones o el propio gobierno aceptara solamente "contenidos apropiados". Además las directrices y las propuestas que están realizando, tanto la Unión Europea como Estados Unidos, para la retención de datos permitirán la regulación absoluta de la red» (Waston, 2007).

De esta manera, Internet 2 no escapará al control gubernamental, y por tanto, será menos permisible a las acciones delictivas.

Conclusiones

Internet se ha convertido en el espacio ideal para la ciberdelincuencia, ya que les ofrece fácil acceso, poco o ningún control gubernamental, anonimato, rápido flujo de información, altísimo impacto, escaso riesgo, barato y indetectable. Además, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarias de seguridad de los Estados es imposible garantizar la seguridad plena de los sistemas informáticos. La única solución realmente efectiva y eficaz es apagar Internet o suprimirlo, pero esta alternativa no es, lógicamente, razonable en mundo como el actual, pese a las excepciones particulares como son las de los Emiratos Árabes Unidos, Corea del Norte o China.

También existe otra posibilidad, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten, y esperar a ver cual es el resultado final. Las otras soluciones aquí planteadas como han sido los sistemas de control de comunicación, la creación de agencias y de cibersoldados, de momento, no están resultado ser totalmente efectivas. Es cierto, que están contribuyendo a detectar a ciberdelincuentes, pero todavía no son capaces de controlar ni impedir su actividad en la Red. Por no hacer referencia a las precauciones que debemos tener cualquier ciberinternauta como son, por ejemplo, no abrir correos de procedencia desconocida, no hacer clic encima de un enlace, usar contraseñas, cifrar la red inalámbrica, realizar copias de seguridad, revisar con cierta frecuencia las cuentas bancarias, etc.

Bibliografía

Añover, J.: *Echelon y Enfopol nos espían,* 2001, en: *http://www.nodo50.org/altavoz/echelon.htm*

Brookes, P.: «Contrarrestando el arte de la guerra informática», *Grupo de Estudios Estratégicos,* número 201, octubre de 2007, en: *http://www.gees.org/articulo/4637/*

Busón Buesa, C.: *Control en el ciberespacio,* 1998, en: *http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm*

— *Control en el ciberespacio,* conferencia en el Programa Modular en Tecnologías Digitales y Sociedad del Conocimiento, celebrada el 22 de agosto de 2009, en: *http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm*

Cabanillas, M.: «Preparados contra el cibercrimen», *PCWorld,* noviembre de 2010.

Caro Bejarano, M. J.: «Nuevo concepto de ciberdefensa de la OTAN», *Documento Informativo,* número 9, Instituto Español de Estudios Estratégicos (IEEE), marzo, 2011, en: *http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09_2011ConceptoCiberdefensaOTAN.pdf*

Fojón Chamorro, E. y Sanz Villalba, A. F.: «Ciberseguridad en España: una propuesta para su gestión», *ARI*, número 101, Real Instituto Elcano, junio de 2010.

Fuentes, L. F.: «*Malware,* una amenaza de Internet», *Revista Digital Universitario,* volumen 9, número 4, pp. 1-9, 2008.

Orta Martínez, R.: «Ciberterrorismo», *Revista de Derecho Informático,* número 82, mayo de 2005.

Pachón Ovalle, G.: «La red Echelon: privacidad, libertad y criptografía», *Virtualidad Real,* Programa de Doctorado en SIC, Universitat Oberta de Catalunya, Barcelona, 2004, en: *http://www.virtualidadreal.com/Red%20Echelon.pdf*

Rodríguez Pérez, C.: *Tecnologías de vigilancia e investigación: el caso Echelon. Informe: tecnologías de vigilancia e investigación,* Posgrado Conocimiento, Ciencia y Ciudadanía en la Sociedad de la Información, Universitat de Barcelona, Barcelona, 2008, en: *http://www.ub.es/prometheus21/articulos/obsprometheus/crodr_echelon.pdf*

Rogríguez Bernal, A.: «Los cibercrímenes en el espacio de libertad, seguridad y justicia», *Revista de Derecho Informático,* número 103, pp. 1-42, febrero de 2007.

Ruiloba Castilla, J. C.: «La actuación policial frente a los déficit de seguridad de Internet», *Revista de los Estudios de Derecho y Ciencia Política de la UOC,* número 2, 2006.

Sánchez Medero, G.: «Ciberterrorismo. La guerra del siglo XXI», *El Viejo Topo*, número 242, pp. 15-23, marzo de 2008.

— «21st Century to two new challenges: Cyberwar and Cyberterrorism», *Nómadas. Mediterranean Perspectives,* número 1, pp. 1-10, 2009.

THOMAS, TIMOTHY L.: «Las estrategias electrónicas de China», *Military Review,* pp. 72-79, julio-agosto de 2001.

TOFFLER, A.: «Onward Cyber-Soldiers», *Time Magazine,* volumen 146, número 8, agosto de 1995.

WASTON, S: «Científicos usamericanos quieren desembarazarse de la red de Internet», *Rebelión,* 2007, en: *http://www.rebelion.org/noticia.php?id=49932*