EL CIBERESPIONAJE Y LA CIBERSEGURIDAD

Por Juan Puime Maroto

Introducción

El espionaje ha acompañado al ser humano desde el principio de los tiempos. Conocer los planes o actividades de un pueblo vecino podía dar ventajas sociales. A pesar de que el indicativo más antiguo de la existencia de espionaje lo constituye la existencia de métodos para encriptar la información escrita, es fácil suponer que esta actividad ya se realizaba con anterioridad.

Los avances tecnológicos sucesivos, como el telégrafo y la radio, han marcado la evolución de los métodos y procedimientos de interceptación y encriptación de la información, y con ello del espionaje. Un ejemplo de esta evolución es la legendaria máquina *Enigma*, utilizada por el Ejército alemán durante la Segunda Guerra Mundial.

Durante la guerra fría, los bloques utilizaron el espionaje como forma para conseguir información, pero también para desinformar al rival.

En la actualidad, ante el gran desarrollo y difusión de los sistemas de información, y la dependencia de ellos de las sociedades modernas, el ciberespacio se presenta como un gran campo para el espionaje. Sin embargo, ésta no es la única oportunidad que brinda a los potenciales agresores, ya que puede ser empleado también como vehículo para todo tipo de actividades ilegítimas.

Las tecnologías de la información han tenido una distribución rápida y generalizada desde su nacimiento. Se puede decir que en la actualidad

se emplea a nivel mundial para la gestión de casi cualquier actividad. Esto, que *a priori* prometía ser de una utilidad extrema, por lo que a términos de eficiencia se refiere, ha creado a su vez nuevas amenazas a la discreción y seguridad, al recaer la casi totalidad del patrimonio o control de los procesos de una organización en dichos sistemas. De tal forma que un experto podría conseguir efectos mayores en un ataque, o más información en menos tiempo de los que se podría tradicionalmente. Además, el hecho de que esta acción se pueda realizar a distancia y, normalmente, con mucha mayor dificultad para identificar al responsable, hace que estos métodos sean mucho más rentables y atractivos para el agresor.

Esta dependencia también afecta a las infraestructuras vitales de un país. Las infraestructuras críticas, compuestas de instituciones públicas y privadas, constituyen el sistema nervioso de las naciones desarrolladas. El ciberespacio es fundamental para su funcionamiento y, por ello, para la seguridad de la nación. La globalización de Internet hace que los centros de gravedad de un Estado sean más vulnerables a un ataque, al ser las fronteras de la red permeables. Un ataque contra el sistema informático de una infraestructura crítica puede generar muchos daños con un riesgo mínimo para el atacante.

Esta dependencia del ciberespacio puede ser aprovechada también por los Servicios de Inteligencia, que no dudarán en contratar a piratas informáticos para desarrollar sus actividades. Tampoco se puede descartar la existencia de grupos terroristas que aprovechen las oportunidades que brinda el ciberespacio, contratando o formando *hackers* (1).

Internet también constituye un instrumento formidable de propaganda, que permite alcanzar fácilmente una audiencia de millones de personas. Es una infraestructura de comunicaciones fiable, favorece el reclutamiento, la colecta de fondos o incluso la coordinación de acciones a distancia de forma discreta.

Por todo lo anterior, actualmente no solamente se utilizan métodos para asegurar la información, sino que son vitales la prevención y respuesta ante violaciones de seguridad en todos los ámbitos.

---

(1) En su acepción actual, un *hacker* es una persona que por medio de sus conocimientos de programación informática, realiza actividades ilícitas.

La ciberamenaza

Originalmente, Internet surgió de investigaciones sobre comunicaciones para utilización en el ámbito militar. Sin embargo, su utilidad para otros ámbitos fue rápidamente obvia, de forma que pronto fue adoptada entre la comunidad científica, desinteresada en el abuso de la Red, para compartir información sobre sus investigaciones.

Hoy en día, sin embargo, Internet conecta millones de redes, incluidas aquellas que hacen funcionar infraestructuras y servicios esenciales. Entre las infraestructuras vitales de un país se encuentran los medios de telecomunicaciones, las redes de distribución (agua, electricidad, gas o petróleo), los servicios de emergencia, los medios de transporte, los servicios gubernamentales y las Fuerzas Armadas. Organizaciones de gran entidad como bancos y universidades también son blancos para ciberataques, ya que muchas forman parte de estas infraestructuras críticas. Estas redes también controlan instalaciones físicas, como estaciones transformadoras de electricidad, centrales hidroeléctricas, bombas de oleoductos y gasoductos, mercados de valores, etc. De modo que la economía y seguridad nacionales dependen en gran medida de las tecnologías de la información y de la infraestructura de comunicaciones.

El ciberespacio une a los países con el resto del mundo, permitiendo a los actores maliciosos en un continente actuar en sistemas a miles de kilómetros. Estos ataques cruzan las fronteras a la velocidad de la luz, haciendo muy difícil la identificación de su origen. Con estas posibilidades, un adversario podría intimidar a los líderes políticos en tiempos de crisis o enfrentamiento, atacando infraestructuras críticas y actividades económicas vitales, erosionando de esta forma la confianza de la población. Es fundamental, por tanto, la capacidad de defensa de los sistemas e infraestructuras críticas, cualquiera que sea la procedencia de los ataques.

Existen innumerables ejemplos de ataques a gran escala, muchos de ellos ya antiguos. Como ejemplos se puede citar el ataque del «gusano» (2) *Nimda* en septiembre de 2001. A pesar de que no causó una interrupción catastrófica en la infraestructura crítica, es un ejemplo de ataque automa-

(2) Un «gusano» es un programa diseñado para replicarse en gran número y distribuirse de un equipo a otro automáticamente. El resultado puede ser un intenso tráfico de red que hace más lentas las redes empresariales o Internet. También pueden permitir que otro usuario tome el control del equipo de forma remota.

tizado de gran envergadura. Se propagó a través de Estados Unidos en una hora, probando diversas formas de infectar los sistemas que invadía hasta lograr el acceso y destrucción de archivos. Su infección duró días, durante los que infectó 86.000 ordenadores. Dos meses después del ataque del *Nimda*, el ataque Código Rojo infectó 150.000 ordenadores en 14 horas.

Hechos como estos han sido el detonante de que en Estados Unidos, los especialistas en defensa e inteligencia hayan colocado a la ciberseguridad al frente de la agenda de Seguridad Nacional.

Actualmente se han generalizado los ataques en el ciberespacio. Así, India sufrió en el año 2008 problemas de infiltración en páginas *web* gubernamentales. Según sus analistas, las redes de la oficina del primer ministro, el Consejo de Seguridad Nacional y el Ministerio de Asuntos Exteriores fueron violadas por *hackers* chinos. La embajada india en Pekín también sufrió un ataque de Denegación de Servicio (DoS) (3). Además, se detectó la creación de *botnets* (4) usando ordenadores indios y de otros países.

India se siente amenazada porque la información obtenida podría ser potencialmente útil en un ataque asimétrico para corromper datos, difundir información falsa, e interferir en el desarrollo normal de las operaciones militares en el caso de que surgiese un conflicto entre los dos países. Aunque China es el país que se menciona más a menudo en este tipo de amenazas, India también identifica como potencial amenaza a Estados Unidos, lo que sugiere una creciente inquietud de que cada vez más países podrían estar interesados en la adquisición de capacidades en este terreno.

Más reciente es el caso de Kirguizistán, cuyos proveedores de servicios de Internet sufrieron ataques DoS a gran escala durante varios días en enero de 2009. El principal servidor *web* nacional y el servicio oficial de registro de dominios de Kirguizistán sólo fueron accesibles de forma intermitente desde el 18 de enero. Esto se produjo justo antes de la visita de su primer

---

(3) DoS proviene de su traducción en inglés: *Denial of Service.* Se trata de un ataque que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, debido al consumo fraudulento del ancho de banda de la red de la víctima o a la sobrecarga de sus recursos. Esta técnica es una de las más eficaces y sencillas a la hora de colapsar servidores.

(4) Una *botnet* es una red de ordenadores, denominados *zombis*, controlados por el propietario de los *bots* (programas maliciosos). Entre las órdenes que los propietarios de estas redes pueden dar a los *zombis* están la descarga de una nueva amenaza, el mostrar publicidad al usuario o el lanzar ataques DoS.

ministro a Moscú para discutir la inversión rusa en el sector energético de Kirguizistán. Además, Rusia estaba presionando a Kirguizistán para que cerrase la base norteamericana empleada para las operaciones en Afganistán. El hecho de que los sitios *web* lituanos sufrieran un ataque DoS similar en el año 2008, mientras el primer ministro lituano visitaba Estados Unidos, sugiere que Rusia podría tener un control a voluntad de las comunicaciones cibernéticas y, de esta forma, influir en sus antiguos satélites soviéticos.

Por otro lado, los ataques a Kirguizistán pueden ser vistos como parte de una campaña represiva de su primer ministro contra un intento de formar un partido político de oposición. En este caso, los ataques se podrían interpretar como una operación patrocinada por el Gobierno en la que los culpables serían *hackers* rusos. Aunque no hay evidencias de que el Gobierno ruso esté involucrado directamente, es un hecho que ejerce un control total de los servidores desde los que se producen los ataques, sin que tomase ninguna medida para evitar el acceso a ellos por los hackers en todo el tiempo que duraron los ataques. Esto refuerza la idea del control que estas capacidades podrían ofrecer a Rusia en las relaciones con sus vecinos.

Las herramientas y procedimientos para realizar ataques a redes se pueden obtener fácilmente, en Internet por ejemplo. El ciberespacio ofrece medios para realizar ataques organizados a distancia. Solamente es necesario disponer de la tecnología necesaria. Además, permite a los atacantes esconder sus identidades, localizaciones y rutas de entrada. En el ciberespacio, las fronteras nacionales pierden su significado, ya que la información fluye a través de las divisiones políticas, étnicas y religiosas. Incluso la infraestructura (tanto *software* como *hardware*) es global en su diseño e implantación. Además, cuando varias organizaciones colaboran, a menudo crean instituciones con procedimientos compartidos que, a su vez, pueden derivar en nuevas vulnerabilidades. Un ejemplo de esto son los estándares para interoperabilidad, que permiten que los problemas creados en un continente, tengan repercusiones potenciales en las redes de otro. Como consecuencia, las vulnerabilidades están abiertas en todo el mundo, disponibles para todo aquel que quiera explotarlas y tenga capacidad para hacerlo.

Conscientes de ello, las organizaciones terroristas cuentan en el ciberespacio con un arma que cada vez usan más y mejor. En este contexto, expertos norteamericanos advierten del peligro de un *cybergeddon*, en el cual una economía avanzada, donde casi todo lo importante está enlazado a ordenadores, o controlado por éstos, es atacada por *hackers*. Los resultados serían catastróficos. Como consecuencia, en Estados Unidos

existe cada vez más la certeza de que deben prepararse para un 9 de septiembre informático.

Evan Kohlmann, un investigador de *Global Terror Alert* (5), afirma que los sitios *web* y las herramientas de redes sociales actualmente ya permiten a los líderes terroristas y a sus organizaciones de militantes el reclutamiento y las comunicaciones seguras en todo el mundo.

Los terroristas emplean Internet por la sencilla razón de que es fácil y barato diseminar información de forma instantánea, por todo el mundo, y relativamente sin censura. Un ejemplo son los sitios *web* de organizaciones terroristas «populares» que, con frecuencia, tienen enlaces del tipo «Qué puedes hacer» o «Cómo puedo ayudar». Los visitantes a menudo son monitorizados e investigados, para seleccionar a posibles candidatos (6).

Otro ejemplo de las formas en que Internet puede ser usada por las organizaciones terroristas es la desfiguración de páginas *web*. En la imagen se puede ver el aspecto de una página *web* comercial israelí desfigurada durante la última invasión de Israel en Gaza. Aunque pudiese parecer que estos ataques solamente afectarían a páginas *web* árabes o israelíes, lo cierto es que también lo fueron muchas páginas *web* francesas, españolas, británicas, danesas y norteamericanas. En muchos casos solamente fue una molestia para sus programadores, pero en otros contenían enlaces a *software* malicioso, o redirigían hacia foros o *blogs* yihadistas, o incluso hacia páginas con mensajes antiisraelíes.

Esta ciberguerra no se libra en un solo bando. Desde mediados del año 2008, *hackers* pro israelíes han destruido y mantenido inaccesibles las páginas *web* de Hamas, o las relacionadas con dicha organización. Otra aproximación en este tipo de guerra es la realizada por una página *web* israelí, que ofrece una descarga (identificada como un troyano (7) ampliamente difundido y empleado en cibercrimen) con la que el ordenador pasa a formar parte de una *botnet* pro israelí de carácter mundial.

---

(5) En: *http://www.globalterroralert.com*

(6) En el artículo siguiente se ofrece una lista de páginas *web* con contenidos sobre grupos terroristas, e incluso de grupos terroristas en sí mismos, en: *http://www.infotoday.com/searcher/nov08/Piper.shtml*

(7) Los troyanos son pequeños programas que a menudo llegan disfrazados en archivos adjuntos de correo electrónico. Instalados en un sistema de forma encubierta pueden espiar, recopilar y enviar datos sin que su dueño se percate; o permitir el control remoto de un ordenador desde otro distinto.

Con el crecimiento exponencial de usuarios de Internet, 1.000 millones en el año 2008, se abre la puerta a la comisión de un mayor número de «ciberdelitos». Aún suponiendo que el 99,9% de los usuarios hiciera un uso legítimo de la Red, todavía existiría un millón de delincuentes potenciales.

La cibercriminalidad se manifiesta en todos los sectores de actividad de la sociedad, pero causa los mayores daños en el sector económico, aunque éstos no sean visibles al principio. Mientras que las víctimas del espionaje industrial, por ejemplo, invierten su capital en investigación y desarrollo, posteriormente sólo obtienen beneficios compartidos con la competencia, en el mejor de los casos.

La ciberdelincuencia se trata de un mundo interdependiente que se basa en grupos cuyas operaciones se complementan. Por ejemplo, el individuo o grupo dueño de una *botnet* capaz de lanzar ataques DoS o de distribuir mensajes no deseados *(spam)*, necesita obtener direcciones IP (8) o de correo. Alguien más, a quien el dueño de la *botnet* no necesita conocer ni mantener contacto alguno con él, roba y vende las direcciones necesarias. Los ciberdelincuentes no necesitan estar conectados organizativamente, sino sólo para su mutuo beneficio. Esto dificulta enormemente su seguimiento.

En la ciberdelincuencia el riesgo es mínimo, los delincuentes nunca ven a sus víctimas, lo que facilita mucho su labor, ya que resulta mucho más fácil atacar a alguien a quien no se ve, se toca o se siente.

En cuanto a su modo de actuar, como se ha dicho anteriormente, existen infinidad de recursos disponibles en Internet para acceder a vulnerabilidades. Las armas favoritas de los ciberdelincuentes actuales son los troyanos. Éstos se utilizan para construir *botnets* y lanzar ataques DoS, robar contraseñas, etc.

La actividad delictiva es también antigua. En el año 2000 unos intrusos accedieron a la red de Microsoft. Durante su permanencia en la red modificaron algunas partes del código de *Windows* y *Office*, así como las marcas de agua que se utilizan para evitar el copiado de sus productos. Los *hackers* utilizaron un troyano que les proporcionó las palabras clave necesarias y las envió por correo electrónico a una cuenta en Rusia.

---

(8) Una dirección IP *(Internet Protocol),* es un número que identifica de manera lógica y jerárquica a un dispositivo dentro de una red que utilice el Protocolo IP que es el empleado para las comunicaciones a través de Internet. Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.

Para lograr la distribución e implementación de estas «armas», se emplean mensajes no deseados y sitios *web* infectados. Un ordenador víctima, con una vulnerabilidad, permitirá que un programa malicioso se instale de inmediato, ya sea a través de un mensaje no deseado, o mientras se navega por Internet. La sofisticación de estos programas maliciosos es tal que a menudo eliminan códigos maliciosos instalados previamente, no para beneficiar al usuario, sino para garantizarse el control del ordenador afectado para su propio beneficio.

Los nuevos servicios disponibles a través de Internet contribuyen al éxito de la ciberdelincuencia. La *web* 2.0 y sus recursos *on-line* como las redes sociales, los *blogs*, foros, *wikis*, *MySpace*, *YouTube*, *Twitter*, y otros colocan a cada usuario de estos recursos en una situación vulnerable y propicia para infecciones de todo tipo.

Cualquier sistema de seguridad tiene una debilidad. En el caso de la seguridad en Internet, el factor humano siempre es una de ellas. En consecuencia, las técnicas de ingeniería social constituyen un elemento clave en los métodos modernos de propagación de programas maliciosos. Hoy en día, por ejemplo, los mensajes de correo pueden conectar a un usuario a sitios *web* infectados de forma automática, sin su conocimiento.

Es importante que los usuarios privados de Internet sean conscientes de que aunque sus ordenadores no formen parte de infraestructuras críticas, pueden formar parte de redes controladas de forma remota que participan en ataques a dichas infraestructuras. Los ordenadores desprotegidos conectados a Internet (por ejemplo a través de líneas ADSL), son vulnerables a ataques que los convierten en integrantes de *botnets*. Una vez realizado el ataque, pueden ser empleadas por sus controladores para lanzar sus ataques sin que el propietario sepa nada. Esto constituye una de las debilidades en la lucha por la seguridad: la amenaza es invisible y, por tanto, no siempre se toma en serio.

Los primeros ataques se centraban en la infiltración en sistemas para la interrupción de servicios. Actualmente se pueden incluir la organización y ejecución de ataques contra redes, sistemas de computación e infraestructuras de telecomunicaciones mediante la introducción de virus en redes vulnerables, la desfiguración de páginas *web* y los ataques DoS.

Hoy en día, los *hackers* ya no son adolescentes buscando emociones. Ahora existen sindicatos de crimen organizado, terroristas y ejércitos que

realizan espionaje y ataques, se introducen en redes sensibles buscando tecnología militar, secretos comerciales, etc.

Actualmente existe incluso un mercado de *hackers*. Las organizaciones que quieren penetrar en los ordenadores y redes de sus del adversarios o víctimas no se arriesgan a hacerlo por sí mismas, sino que reclutan a piratas informáticos para que hagan el trabajo sucio en su lugar.

El ciberespionaje

Hasta ahora la amenaza parece poco relacionada con el ciberespionaje. Nada más lejos de la realidad. El espionaje puro es solamente la punta del iceberg. Para poder llevar a cabo las acciones características de cada amenaza descrita en el capítulo anterior, es necesaria la recopilación previa de información. En tiempo de paz, los adversarios pueden realizar reconocimientos de los sistemas de información de gobiernos, universidades y compañías privadas, identificando los objetivos clave, buscando vulnerabilidades e introduciendo «puertas traseras» (9) para su empleo en tiempos de crisis o confrontación. Como se puede deducir, estas actividades constituyen acciones de espionaje.

Un ejemplo claro de esta forma de actuar lo constituyen las infiltraciones anteriormente citadas en sitios oficiales de India. El resultado potencial puede ser la identificación de vulnerabilidades y objetivos para su empleo futuro, aparte de las posibles fugas de información. Esta potencialidad ya es suficiente para generar desconfianzas y sentirse amenazado.

Según los expertos indios en seguridad nacional e informática, el espionaje industrial se considera una prioridad para el ciberespionaje chino. La razón es que reduciría gastos y tiempo en el esfuerzo chino para construir un ejército e industria militar modernos.

Dentro de los ataques informáticos contra empresas y redes de información, los expertos en seguridad alertaban en el año 2007 de su aumento. Éste es especialmente notable en los casos provenientes de oriente. Como ejemplo se puede citar el caso de Alemania, donde los Servicios Secretos detectaron troyanos infiltrados en los ordenadores de la cancillería y de varios ministerios en el año 2007. El vicepresidente de los

(9) Las «puertas traseras» son coloquialmente las vulnerabilidades directamente explotables en un sistema o *software.*

Servicios Secretos, Hans-Elmar Remberg, atribuyó el ataque a unidades de espionaje del Ejército chino. Se detectaron asaltos buscando, no sólo secretos políticos o diplomáticos, sino también para acceder a habilidades técnicas y científicas, principal materia prima del país. Si hasta hace unos años la industria china se limitaba a reproducir artículos en versión barata, ahora busca tecnología punta, e incluso espían la organización y construcción de plantas de producción completas.

Casos como el anteriormente citado de India y este último de Alemania coinciden en señalar la obtención de capacidades militares en el campo cibernético. Esta tendencia podría ser seguida en el futuro próximo por otros países, lo que aconseja iniciar el debate de si es necesario dotar a las Fuerzas Armadas de ellas.

Una vez más, los troyanos son los programas preferidos para estas actividades. Con ellos se pueden robar contraseñas y datos confidenciales de las víctimas. Otra herramienta especialmente útil para el espionaje son los *keyloggers* (10). Empleados contra las redes del Gobierno, son extremadamente útiles para los Servicios de Inteligencia del adversario.

Ejemplos de esto a gran escala existen desde hace tiempo. Entre los años 1999 y 2004 se robaron más de 12.000 números de la Seguridad Social y fechas de nacimiento de los visitantes del Laboratorio Nacional de Oak Ridge (ORNL) del Departamento de Energía de Estados Unidos. En diciembre de 2007 unos cibedelincuentes penetraron nuevamente en los ordenadores del ORNL. Se cree que también atacaron el Laboratorio Nacional de los Álamos y el Laboratorio Nacional Lawrence Livermore.

Más cercano todavía es el caso detectado durante la campaña electoral norteamericana. Durante el verano de 2008, un miembro del equipo del todavía candidato Obama denunció un problema con un ordenador, que él achacaba a un virus informático. Tras su revisión, se pudo comprobar que había sido descargada una gran cantidad de información de los ordenadores de la campaña. No habían sido los únicos atacados, puesto que el sistema de su rival, John McCain, también había sufrido una infiltración. Las investigaciones apuntaron a una entidad u organización extranjera

(10) Un *keylogger* es un tipo de *software* malicioso que colocado en una red permite recopilar usuarios y contraseñas. También son capaces de registrar las pulsaciones de teclado de un operador, permitiendo a un ciberespía leer el texto escrito, ya sea un programa, un correo electrónico, etc.

que quisiera reunir información confidencial de cara a una futura negociación con el nuevo presidente.

Las actividades de espionaje no se realizan sólo mediante acciones de forzamiento o programas especiales. La existencia de ordenadores desprotegidos, conectados a su vez a dispositivos ópticos, supone una fuente potencial de información y facilitan mucho las labores de espionaje.

La Asociación de Internautas de España (11) detectó, a través de un estudio de José María Luque, su responsable del área de seguridad, que el 60% de las cámaras de vigilancia conectadas a Internet están abiertas y carecen de una seguridad adecuada. Accedió a cámaras de seguridad de centros comerciales, multinacionales, e incluso a alguna instalación de las Fuerzas de Seguridad del Estado. Además, detectó otro 20% de cámaras cuyo acceso es más complicado, pero también vulnerables. Sólo el 20% de las cámaras comprobadas resultaron seguras.

La forma de acceder a estas cámaras es bastante sencilla. Basta conocer algunas marcas de cámaras y determinados puertos para que el navegador de Internet, a través de un buscador como *Google*, abra identificadores que conectan con cámaras de todo el mundo. Otra forma consiste en comprobar direcciones IP vinculadas a cámaras de vigilancia de forma aleatoria. Si la seguridad es deficiente, con pulsar en ellas con el ratón es suficiente.

Como se puede ver, resultaría relativamente fácil observar desde un ordenador particular lo que estas cámaras no seguras ven. Esto ofrece un potencial enorme para el espionaje, al poder servirse de ellas para vigilar lo que ocurre dentro de domicilios, diferentes tipos de locales e instalaciones, o cualquier otra cosa que se desee investigar.

Otra técnica con gran potencial para el ciberespionaje es la ingeniería social. Ésta se define normalmente como el procedimiento mediante en cual un *hacker* engaña a otros para que revelen datos valiosos que le benefician de alguna forma. Aunque los *hackers* empleaban inicialmente la ingeniería social para obtener códigos o claves de direcciones de correo para acceder a líneas de teléfono de larga distancia, los informes más recientes sugieren que los ataques por medio de la ingeniería social se usan para actos delictivos como la adquisición de números de tarjetas de crédito y otros datos financieros. No es muy difícil ver su utilidad para conseguir todo tipo de información procedente de personas no conscien-

(11) En: *http://www.internautas.org*

tes de los peligros de las nuevas herramientas de Internet. En un mundo donde las redes sociales, cada vez más populares, permiten que llevemos vidas paralelas, con personalidades alternativas, alguien especializado en (inteligencia humana), por ejemplo, podría conseguir la confianza de una persona que, sin saberlo, actuase de informador.

Los ejemplos anteriores son solamente una pequeña muestra de los que se pueden encontrar diariamente en los medios de comunicación. Sin embargo, permiten formar una idea de la importancia creciente que tiene este tipo de amenaza, así como de los efectos y posibilidades que ofrece a sus usuarios.

La lucha contra los ciberataques

Como se podrá ver en otros capítulos, la frontera entre el ciberataque, el ciberespionaje y el cibercrimen se diluye, ya que, en la mayoría de los casos, uno es el paso previo del otro, y además comparten las técnicas necesarias para su desarrollo. El resultado es que en la lucha para contrarrestarlos no cabe distinción. Los métodos que se desarrollen para combatirlos servirán para la lucha contra todos ellos.

Toda estrategia diseñada para la lucha contra este tipo de amenazas debe incluir la prevención de los ciberataques contra las infraestructuras críticas de la nación, un programa para la reducción de la vulnerabilidad ante este tipo de ataques, así como medidas para la reducción de daños que éstos puedan causar y del tiempo necesario para la recuperación de los sistemas e infraestructuras afectados.

Para su desarrollo, el departamento que debe liderar y coordinar los esfuerzos debería ser aquel que normalmente se dedique a la seguridad interior. En el caso de Estados Unidos, una referencia en este campo, se trata del Departamento de Seguridad Nacional (12), equivalente al Ministerio del Interior español.

Entre las responsabilidades que se le deben encomendar, se incluyen el desarrollo de un plan conjunto (13) nacional para la seguridad de los re-

(12) DHS *(Department of Homeland Security).*

(13) El empleo de la palabra «conjunto» aquí, no se limita a su acepción militar, sino que hace referencia a la implicación de todas las instituciones públicas y privadas relacionadas de alguna forma con la defensa del ciberespacio y las infraestructuras críticas.

cursos clave y las infraestructuras críticas; la dirección de la gestión de crisis en respuesta a ciberataques sobre sistemas de información críticos; y la asistencia técnica al sector privado y entidades gubernamentales sobre planes de recuperación en emergencias por fallos en sistemas de información críticos.

Esta actuación está sometida a una serie de limitaciones. En primer lugar, en países con formas de gobierno descentralizadas, este simple hecho obliga a la existencia de organizaciones más allá del Gobierno central que asuman el liderazgo de algunos esfuerzos en sus respectivas áreas de influencia. Además, como consecuencia de lo anterior, surge la necesidad de órganos de coordinación entre agencias.

Por otro lado, el ámbito de actuación gubernamental debe descender hasta un determinado límite. La implicación del Estado debe limitarse a aquellos casos en los que los beneficios de la intervención sean mayores que los costes de ésta. Dado que su actuación no será universal, el Gobierno debe impulsar la creación y participación en asociaciones público-privadas para mejorar el conocimiento sobre seguridad, identificar y arreglar vulnerabilidades, intercambiar información y planear operaciones de recuperación.

En cuanto a la regulación sobre ciberseguridad, ésta no debe ser el medio principal de asegurar el ciberespacio. Esta aproximación al problema podría llevar a estructuras de seguridad más homogéneas, y con ello a un ciberespacio menos seguro. Además, según aparecen tecnologías nuevas, se identifican vulnerabilidades nuevas, de modo que la normativa debe ser genérica y revisarse cíclicamente.

Para responder a las necesidades anteriormente citadas, es necesario desarrollar una serie de iniciativas. En primer lugar un sistema nacional de seguridad y respuesta para el ciberespacio. Este sistema debería complementarse con un programa continuo de reducción de amenazas y vulnerabilidades.

Dado que una de las mayores vulnerabilidades en el ciberespacio es el desconocimiento de la existencia de la amenaza, así como la forma de contrarrestarla, otra necesidad es la existencia de un programa de divulgación y enseñanza sobre seguridad del ciberespacio.

Finalmente, un punto clave en la lucha contra este tipo de amenazas, es la cooperación, no solamente interna, sino también internacional. El hecho de que los ataques se produzcan desde lugares lejanos, como ya se

ha mencionado, pone de manifiesto la importancia de esta colaboración. Esto se traduce también en la necesidad de un programa de cooperación internacional.

Sistema Nacional de Seguridad y respuesta para el ciberespacio

La identificación, intercambio de información y respuesta rápida, a menudo pueden mitigar los daños causados por la actividad maliciosa proveniente del ciberespacio. El sistema nacional de respuesta es necesario para detectar actividades potencialmente dañinas en el ciberespacio; analizar ataques y alertar a sus víctimas potenciales; coordinar las respuestas a los incidentes, y restaurar los servicios esenciales que hayan sido dañados. El hecho de que la gran mayoría del ciberespacio no tenga propietario ni lo controle una entidad determinada representa un reto para la creación de dicho sistema. Si no existe una visión global del ciberespacio, la información sobre un ataque se acumula en muchas organizaciones, pero sin un mecanismo para revisar todos esos indicadores, no se podrá organizar una respuesta. Para mitigar el impacto de los ciberataques es necesario que la información sobre ellos se distribuya amplia y rápidamente.

Las redes del sector privado son, cada vez más, un blanco para los ciberataques, por ello son probablemente las primeras organizaciones en detectar ataques de potencial importancia nacional. Para aprovechar esta información, el Gobierno debe impulsar la creación de órganos especializados dentro de estas organizaciones (14), que permitan el análisis e intercambio de información. Estos órganos, trabajando junto con el Gobierno, permitirían asegurar la recepción de información sobre amenazas y vulnerabilidades a tiempo, y coordinar los esfuerzos de planeamiento de contingencias.

El Sistema Nacional de Seguridad y respuesta para el ciberespacio debería ser una arquitectura mixta público-privada, coordinada por un departamento gubernamental, con la misión de analizar, alertar y gestionar incidentes de ámbito nacional, garantizar la continuidad de los sistemas del gobierno y las infraestructuras del sector privado, e incrementar el intercambio de información entre organizaciones para mejorar la seguridad del ciberespacio.

(14) En Estados Unidos estos órganos se denominan ISAC,s *(Information Sharing and Analysis Centres)*.

ANÁLISIS

El análisis es el primer paso al detectar un ataque. En esta fase se busca su naturaleza, la información que ha comprometido, la extensión del daño, la posible intención del intruso, las herramientas que ha podido usar, y las vulnerabilidades que ha explotado. Toda esta información es fundamental para identificar los indicios que permitan reconocer un ataque y generar las alertas correspondientes. Al considerar conjuntos más amplios de incidentes, se pueden identificar alertas de riesgos emergentes, como métodos nuevos de ataque.

ALERTA

En un mundo donde las comunicaciones son casi instantáneas, los minutos pueden marcar la diferencia entre una interrupción de servicios severa y un incidente gestionable. Para que la información disponible en el paso anterior se pueda distribuir a tiempo, es necesaria una infraestructura segura que proporcione comunicaciones fiables entre propietarios de infraestructura crítica, operadores y proveedores de servicios.

RESPUESTA Y RECUPERACIÓN

Una vez difundida la alerta, el Gobierno debe apoyar a la gestión de crisis en respuesta a amenazas y ataques a sistemas de información críticos para el Gobierno, gobiernos autónomos, sector público y, a petición, sector privado.

No existe ninguna tecnología capaz de hacer una red completamente segura. Una forma de reducir la exposición a pérdidas relacionadas con ciberataques es el desarrollo de planes de contingencia adecuados y probados. Además, deben establecerse planes de asistencia mutua entre los diferentes componentes de infraestructura crítica, de modo que se reduzcan los efectos en cascada debido a su interrelación. Todos estos planes deben ser coordinados por un órgano superior a nivel nacional, que debería depender directamente del Departamento Gubernamental encargado de la seguridad del ciberespacio.

Para probar la eficacia de la seguridad y los planes de contingencia se deben emplear ejercicios de simulación. De esta forma se puede evaluar el impacto potencial de los ataques y la coordinación de las capacidades públicas y privadas para la gestión, respuesta y recuperación en incidentes.

El intercambio de información sobre incidentes es fundamental. Existen dificultades para lograrlo, como el miedo a que datos confidenciales, privados o potencialmente comprometedores pudiesen llegar al dominio público si se compartiesen con el Gobierno. Preocupaciones sobre ventajas en competitividad pueden impedir que se comparta información entre empresas de un mismo sector. Una prueba de ello es que la mayoría de los ciberdelitos son abordados internamente por las mismas organizaciones afectadas, que realizan investigaciones encubiertas. Los resultados casi nunca se hacen públicos.

El gráfico mostrado a continuación proviene de un informe del *Computer Security Institute* (15) y (16) figura 1.

Para evitar éstos y otros problemas, el Gobierno debe establecer normativas para la custodia y almacenamiento de esta información, así como métodos de protección de la confidencialidad del remitente.

Las organizaciones privadas con grandes recursos informáticos, como grandes empresas, laboratorios de investigación y universidades juegan un papel importante en la detección e informe de ciberataques y vulnerabilidades. Debido a que estas instituciones poseen grandes redes que pueden ser usadas como vectores de lanzamiento de ataques, se las debe animar a establecer puntos de contacto con los proveedores de servicios de Internet y Cuerpos de Seguridad del Estado, y crear centros de análisis e intercambio de información. Esto es extensible a las grandes empresas de infraestructura.

Una iniciativa interesante para el apoyo a este sistema es el *Cyberwar Playbook* desarrollado en Estados Unidos. Este libro define las tácticas, técnicas y procedimientos que un atacante puede emplear para conseguir unos objetivos concretos. Su propósito es ayudar en la Defensa Nacional ante un ciberataque, si bien puede ampliarse su ámbito de aplicación a los sectores público y privado, en particular en la defensa de la infraestructura crítica.

Para su creación se forma un equipo de atacantes simulados, que a partir de los objetivos que deben alcanzar, y de una lista de posibles procedi-

(15) En: *http://www.gocsi.com*

(16) La figura 1, pone también de manifiesto la necesidad de mejorar las capacidades policiales y judiciales en este ámbito, que se tratarán con posterioridad.

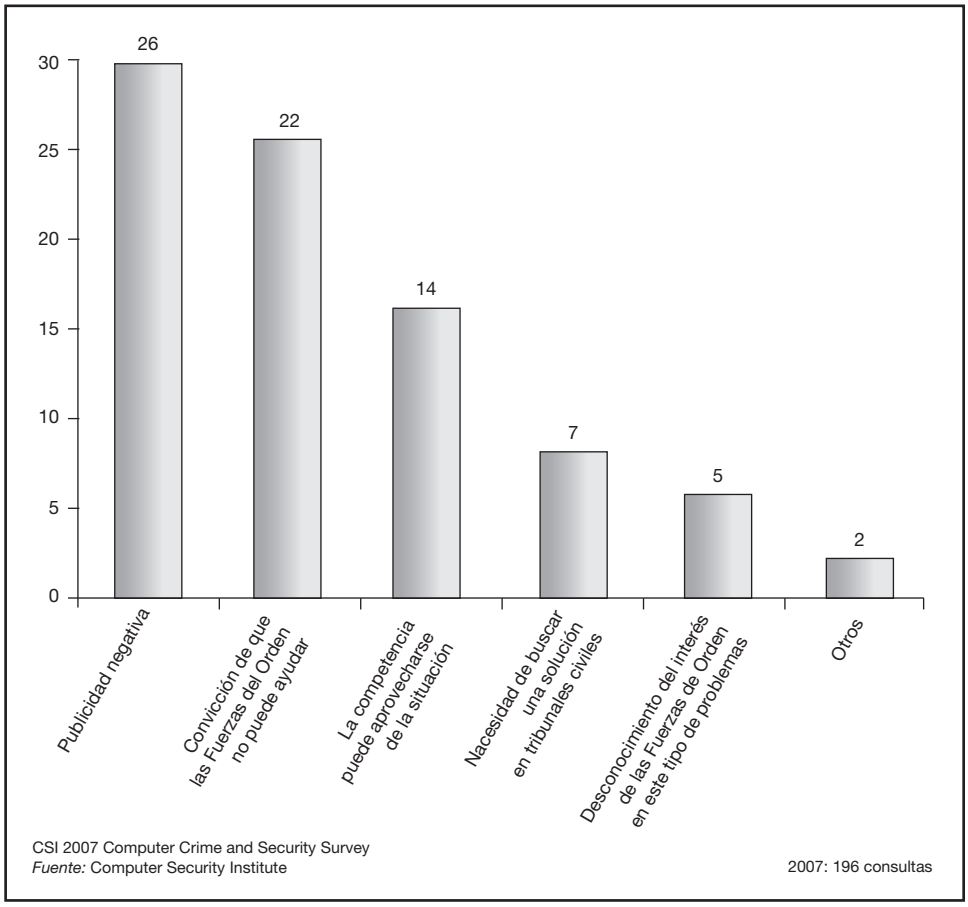

Figura 1.— *Razones por las que los organizaciones prefieren no divulgar estos incidentes, en porcentaje.*

mientos, realizan el ataque. El equipo defensivo trata de identificar el tipo de ataque, y de pararlo y mitigar sus efectos. Tras una serie de repeticiones del procedimiento, se puede identificar cuál es la estrategia defensiva más adecuada, o cuál produce resultados indeseables. El proceso se repite con diferentes objetivos del bando atacante para compilar diferentes situaciones posibles. Finalmente se plasma en el documento de apoyo para la lucha contra ciberataques.

Para la obtención de información también es importante la creación de sistemas de inteligencia. Con estos sistemas se trata de conocer qué información busca el adversario, o qué mira con más frecuencia, puesto

que antes de realizar un ataque se necesita reconocer las redes y explorar sus vulnerabilidades.

Programa Nacional de Reducción de Amenazas y Vulnerabilidades

Las vulnerabilidades que más amenazan el ciberespacio se encuentran en los sistemas de información de las empresas de la infraestructura crítica, y en sus estructuras de apoyo externo. Los atacantes buscan explotar vulnerabilidades surgidas durante el diseño e implementación del *software*, *hardware*, redes y protocolos. Incluso cuando las alertas están disponibles, el arreglo de algunas vulnerabilidades necesita días, semanas o incluso años de trabajo. Por ello, las vulnerabilidades en las redes críticas se deben identificar y corregir antes de que surjan las amenazas. No se pueden eliminar todas las vulnerabilidades o amenazas, pero se pueden minimizar realizando esfuerzos para:

– Reducir y corregir las vulnerabilidades de *software*, identificando y arreglando las vulnerabilidades existentes que, si se explotasen, podrían causar la mayor parte del daño a los sistemas críticos.
– Impulsar el empleo de sistemas seguros de supervisión, control y adquisición de datos.
– identificar interdependencias de la infraestructura y la mejorar la seguridad física de los sistemas vitales.
– Buscar vulnerabilidades en las tecnologías nuevas.
– Identificar y castigar actores maliciosos, mejorando las capacidades judiciales para la prevención y persecución de los ataques en el ciberespacio.

REDUCCIÓN Y CORRECCIÓN DE VULNERABILIDADES DE *SOFTWARE*

Cada día surgen nuevas vulnerabilidades de *software*. Las correcciones normalmente las aportan los fabricantes por medio de «parches». Sin embargo, muchos fallos conocidos, para los que existen correcciones, siguen presentes en los sistemas durante largos periodos de tiempo. El *software* no corregido en las infraestructuras críticas las hace vulnerables, ya que estos fallos pueden usarse para obtener el control sobre ellas.

La difusión de información sobre la existencia de estas vulnerabilidades y su forma de corregirlas es fundamental, sin embargo, presenta el problema de que su difusión abierta ayuda tanto al desarrollo de correcciones, como a la creación de oportunidades para los atacantes. Para solucionarlo, es necesaria la presencia de cauces seguros para la transmisión

de esta información. Una vía podría ser la red de centros de análisis e intercambio de información mencionada con anterioridad.

Una iniciativa interesante para la reducción de vulnerabilidades de *software* es el catálogo de patrones de ataque (17), patrocinado por el DHS en Estados Unidos y de dominio público. Los patrones de ataque describen las técnicas que los atacantes emplean para romper el *software*, que tienen tendencia a ser pocas y bastante específicas.

Los patrones de ataque contienen información suficiente sobre la forma en que se desarrollan los ataques, para permitir a los programadores su prevención. Al mismo tiempo, no contienen información tan detallada sobre las vulnerabilidades como para que los *hackers* con menos nivel puedan aprender de ellos. También se describen las condiciones que se tienen que cumplir para que se puedan aplicar (contexto), así como los métodos recomendados para mitigar sus efectos.

Aunque los patrones de ataque representan descripciones de cómo se explotan vulnerabilidades, no tienen necesariamente que provenir de vulnerabilidades descubiertas tras un ataque. Las organizaciones al realizar auditorias de seguridad en sus redes, pueden encontrar formas nuevas de atacar un sistema y reflejarlas en este catálogo.

La forma de emplear los patrones para desarrollar *software* más seguro es utilizar la información del contexto en el que se puede realizar un ataque determinado. De esta forma, el programador puede decidir qué debe hacer la aplicación si encuentra esa condición. También se puede emplear los patrones de ataque para identificar las mejores configuraciones y políticas de seguridad.

Una vez desarrollado el programa, los patrones de ataque se emplean a la inversa, en pruebas de seguridad basadas en los riesgos. El objetivo es tratar de romper el programa. En estas pruebas se aplican los patrones de ataque para encontrar y explotar vulnerabilidades.

EMPLEO DE SISTEMAS SEGUROS DE SUPERVISIÓN, CONTROL Y ADQUISICIÓN DE DATOS

En la actualidad existen muchas industrias e infraestructuras que emplean estos sistemas, basados en ordenadores, para controlar, de forma remota,

(17) CAPEC *(Common Attack Pattern Enumeration and Classification).*

procesos sensibles que antes se controlaban de forma manual. De forma creciente, estos sistemas usan Internet para la transmisión de órdenes, en vez de las redes aisladas que empleaban en el pasado. Debe asegurarse que existe un conocimiento amplio entre los fabricantes y los usuarios de estos sistemas, de las vulnerabilidades que crean y las consecuencias que su explotación puede tener, en contraste con las ventajas que tiene la inversión en un sistema seguro.

IDENTIFICACIÓN DE INTERDEPENDENCIAS DE LA INFRAESTRUCTURA Y MEJORA DE LA SEGURIDAD FÍSICA DE LOS SISTEMAS VITALES

Esta identificación es vital, puesto que el impacto de un ataque podría ser mayor del esperado por los efectos en cascada que podrían producirse en caso de que las infraestructuras fuesen interdependientes. A través de este conocimiento se pueden mejorar los planes de contingencia y recuperación, y se ayuda a reducir las vulnerabilidades por efectos en cascada.

En este estudio debe incluirse vulnerabilidad debida a la pérdida de infraestructura física en la que se basen estos sistemas, ya que su destrucción provocaría los mismos efectos que la caída de los servicios también por otros medios.

BÚSQUEDA DE VULNERABILIDADES EN NUEVAS TECNOLOGÍAS

Las nuevas tecnologías crean nuevas vulnerabilidades. Por ejemplo, una persona en un coche recorriendo las calles de una ciudad podría acceder a muchas redes inalámbricas sin que sus propietarios lo supiesen, a menos que estuviesen aseguradas convenientemente. Otro ejemplo son los teléfonos móviles y (asistente digital personal), que incorporan sistemas operativos cada vez más sofisticados, con tecnologías de conectividad que puede necesitar características de seguridad para evitar la explotación de vulnerabilidades por medio de ataques DoS sobre las redes de telefonía móvil, o incluso sobre Internet.

Programa de Divulgación y Enseñanza sobre Seguridad del Ciberespacio

Las organizaciones que se basan en sistemas de información conectados en red deben tomar acciones proactivas para detectar y arreglar sus vulnerabilidades, en vez de esperar a que los ataques sean detenidos, o que se les avise de un ataque inminente. Aunque la probabilidad de

sufrir un ciberataque grave es difícil de estimar, los costes asociados a uno que tenga éxito es probable que superen a los asociados a la inversión necesaria en el desarrollo de un programa de prevención. Cuando se emplee la tecnología inalámbrica, debe evaluarse cuidadosamente los riesgos asociados a su empleo en funciones críticas. Este tipo de comunicación puede ser interceptada, y sus redes asociadas pueden sufrir ataques DoS. Las auditorias de seguridad para detectar vulnerabilidades en la infraestructura pueden durar meses, por lo que el proceso debería ser repetido de forma regular.

Otra razón para la revisión regular de las condiciones de seguridad de las redes es que continuamente se crean o detectan nuevas vulnerabilidades. La mera instalación de *hardware* de seguridad de red no sustituye al mantenimiento y actualización de las defensas de la red. Como muestra de ello, El 90% de los participantes en una encuesta del *Computer Security Institute* (18) empleaba antivirus en sus redes, sin embargo, el 85% de sus sistemas había sido atacado por virus. En la misma encuesta, el 89% tenía instalados firewalls, y el 60% sistemas de detección de intrusos. Sin embargo, el 90% había sufrido brechas de seguridad, y el 40% intrusiones desde el exterior.

En muchos casos las soluciones a los problemas de seguridad ya existen, pero quienes las necesitan no lo saben, o no saben como encontrarlas. En otros casos no saben ni que lo necesitan. Por ejemplo, un pequeño negocio puede no tener en cuenta que las palabras clave por defecto que emplea su servidor de página *web* permite el acceso a todo aquel que sepa cuál es, y con ello controlarlo.

La mayoría de las vulnerabilidades de seguridad se pueden mitigar a través de buenas prácticas de seguridad. Estas buenas prácticas incluyen no sólo la instalación de *hardware* de seguridad, sino también un manejo correcto, la instalación de *firewalls* y antivirus, y la actualización regular de éstos y de sistemas operativos y programas principales.

Las grandes empresas poseen las mayores redes y sistemas de ordenadores que, si no se aseguran, pueden ser explotadas para lanzar ataques. Estos ataques, en caso de ser masivos, pueden tener grandes consecuencias económicas. El Ministerio del Interior debe sensibilizar a los propietarios de estas redes de sus vulnerabilidades y qué pueden hacer para mitigarlas.

(18) En: *http://www.gocsi.com*

Muchos ataques en empresas se producen a través de usuarios de confianza, personas con acceso legítimo a las redes y sistemas de información de las empresas. La identificación y autenticación de cada usuario es el primer eslabón en la cadena de seguridad de un sistema, sin embargo, muchas veces las palabras clave por defecto no se cambian o se renuevan raramente. Los controles de acceso débiles permiten modificar, destruir o divulgar información sensible. Nadie debería tener control total sobre ningún sistema.

Muchas redes no seguras de campus universitarios han sido empleadas por atacantes organizados para lanzar ataques DoS y de otros tipos. La razón es el gran poder de cálculo informático que poseen y el acceso abierto relativo que tienen a sus recursos. Para luchar contra estas vulnerabilidades se debería fomentar la seguridad de las redes de investigación y revisar las políticas de seguridad institucionales en la educación superior. Esto se puede lograr a través de un programa que aumente la conciencia de la necesidad de asegurar el ciberespacio.

Muchas de las infraestructuras críticas y el ciberespacio en el que se basan son propiedad y se gestionan desde el sector privado. Gran cantidad de las vulnerabilidades del ciberespacio, como las expuestas anteriormente, existen por la falta de conocimientos sobre ciberseguridad de los usuarios, administradores de sistemas, desarrolladores de tecnología, etc. La principal iniciativa gubernamental para luchar contra estos condicionantes es la creación de un programa de ámbito nacional para lograr que toda la población asegure su parte del ciberespacio.

Todo el mundo puede ayudar a la seguridad del ciberespacio, asegurando la parte de éste que puede controlar o en la que puede influir. Para hacerlo, los usuarios necesitan saber qué pueden hacer para evitar las intrusiones, ataques o brechas en la seguridad. Para lograr esta cultura de seguridad puede ser de gran utilidad la creación de un programa de conocimiento y sensibilización pública.

Los usuarios privados y las pequeñas empresas no son parte de infraestructuras críticas, sin embargo, sus sistemas son cada vez más usados por los agentes maliciosos para atacar sistemas críticos. Por lo tanto, mejorar el conocimiento sobre ciberseguridad entre los usuarios contribuye a una mayor seguridad de la infraestructura. Una forma de lograrlo es fomentar la cooperación con el Ministerio de Educación y los gobiernos locales y estatales, para introducir contenidos de ciberseguridad en la

educación obligatoria. También ayudaría la disponibilidad de páginas *web* oficiales en las que se ofreciese información a los consumidores y pequeñas empresas.

El programa de divulgación y enseñanza sobre seguridad del ciberespacio tiene como objetivo la mejora del conocimiento sobre ciberseguridad en compañías, agencias del gobierno, universidades y entre los usuarios.

Programa de Cooperación Internacional

Una Red de redes se extiende por todo el mundo, permitiendo a los actores maliciosos de un continente actuar en sistemas a miles de kilómetros. Los ciberataques cruzan fronteras, lo que hace complicada la tarea de identificar su procedencia. Encontrar el origen de esta actividad es complicado, por ello, la capacidad de protección y defensa de sistemas y redes es crítica. Para lograrla se necesita un sistema de cooperación internacional que permita el intercambio de información, reducir las vulnerabilidades y detener a los actores maliciosos.

Uno de los pilares en este sistema es la inteligencia del ciberespacio. La comunidad de inteligencia debe adoptar una postura fuerte de contrainteligencia para contrarrestar la inteligencia del adversario sobre los sistemas de información propios. Esto incluye al Gobierno y las organizaciones comerciales y de educación. El esfuerzo debe incluir un mayor conocimiento de las capacidades e intenciones del adversario en su empleo del ciberespacio como medio de espionaje. Como consecuencia, debe ser una preocupación continua la actualización de información sobre nuevas técnicas y procedimientos de ciberataque.

Otro punto importante es la creación de redes nacionales e internacionales de vigilancia y alarma. Cada nación debe desarrollar su propio sistema de observación y alerta, para capaz de informar a las agencias gubernamentales, el público y los demás países sobre ataques inminentes o virus.

La gran mayoría de los ciberataques se originan o pasan a través de sistemas en el extranjero, cruzan varias fronteras, y requieren la cooperación internacional en la investigación para pararlos. Para conseguir la seguridad global del ciberespacio se necesita la cooperación internacional en la investigación y persecución de los cibercriminales. Es necesario trabajar a través de organizaciones internacionales para conseguir la protección de la infraestructura de la información y promover una «cultura de seguridad global». Para lograrlo se debe fomentar la creación de este tipo de

organizaciones, así como la adhesión de las naciones a ellas o, al menos, asegurarse de que sus leyes y procedimientos son compatibles

Un ejemplo de este tipo de organización es la convención sobre el cibercrimen del Consejo de Europa, que obliga a sus integrantes a considerar los ciberataques como un crimen importante, y a la adopción de medidas y procedimientos de apoyo mutuo para combatir mejor el cibercrimen a través de las fronteras internacionales. Este convenio fue elaborado por el Consejo de Europa con la participación de Canadá, Estados Unidos, Japón y Suráfrica, y está en vigor desde julio de 2004. Medidas recogidas en el Convenio, como la conservación de los datos informáticos almacenados, las órdenes de presentación de los mismos, el registro, así como la confiscación y la obtención en tiempo real de datos informáticos si fuera necesario, se están convirtiendo en base jurídica para la cooperación internacional. De esta forma sirven para proporcionar una norma mundial que mejore la legislación sobre la ciberdelincuencia.

Dentro de este esfuerzo, Cybex, una empresa española, con el apoyo financiero de la Comisión Europea, ha organizado la primera Certificación Europea sobre Cibercriminalidad y Pruebas Electrónicas (ECCE, en sus siglas en inglés). Su objetivo principal es ofrecer la formación técnica necesaria para jueces, abogados y fiscales europeos y de América del Sur sobre cibercrimen y prueba electrónica, para que en el futuro, este tipo de pruebas sean presentadas y admitidas de forma habitual ante los tribunales de todo el mundo. Gracias a esta formación única en todos los países europeos, se conseguirá incrementar la compatibilidad de los sistemas judiciales existentes en materia de prueba electrónica y lucha contra el cibercrimen.

Independientemente de las medidas que se tomen con carácter internacional, cada nación debe retener la capacidad de ejercer la respuesta que considere conveniente. Cuando se produce el ataque de una nación, grupo terrorista u otro adversario a través del ciberespacio, la respuesta no tiene por qué limitarse a la persecución criminal. De este planteamiento se deriva la posibilidad de responder través del propio ciberespacio. Para ello se necesita estudiar las capacidades necesarias, y a quién dotar de ellas dependiendo del reparto de responsabilidades. En el caso de Estados Unidos y otros países, aparte de las competencias otorgadas a sus cuerpos de policía, sus ejércitos están comenzando a dotarse de capacidades para el enfrentamiento a través del ciberespacio.

Situación en España

En España, las competencias en materia de defensa contra ciberataques le corresponden al Centro Criptológico Nacional (CCN). Dicho Centro se creó por la Ley 11/2002, de 6 de mayo, que regula el Centro Nacional de Inteligencia, e incluye al CCN. Posteriormente, por Real Decreto 421/2004, de 12 de marzo, se regula y define el ámbito y funciones del CCN.

Dentro de las competencias del CCN, una de las más importantes es la certificación de las redes seguras de las instituciones gubernamentales, entre ellas las de Defensa. Este cometido viene regulado por la Orden Ministerial PRE/2740/2007 de 19 de septiembre, que establece el *Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información*.

Dentro del CCN, existe un órgano especializado en la ciberdefensa denominado CERT (19). Esta Organización estudia la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publica las alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas. Complementa los servicios de carácter reactivo anteriores con otros de carácter preventivo y de gestión de la seguridad. La misión del CERT es desarrollar la función de centro de alerta y respuesta ante incidentes de seguridad, ayudando a las Administraciones Públicas (20) a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información.

El objetivo del CCN-CERT es contribuir a la mejora del nivel de seguridad de los sistemas de información de las Administraciones Públicas. En el desarrollo de su actividad tiene autoridad para:

– Realizar todas las acciones necesarias para la resolución de incidentes en Sistemas Clasificados (Real Decreto 421/2004).
– Colaborar y asesorar en la resolución de los incidentes en sistemas no clasificados. En este caso, las acciones necesarias para cumplir con la misión del CCN-CERT deben tomarse en consenso con las Administraciones Públicas.

(19) CERT *(Computer Emergency Response Team)* (equipo de respuesta para emergencias informáticas).
(20) Las Administraciones Públicas incluyen la Administración Central, las autonómicas y locales.

Los incidentes prioritarios para el CCN-CERT son:

– Incidentes que afecten a información clasificada.
– Ataques contra infraestructuras de Internet de las Administraciones Públicas.
– Ataques distribuidos y automáticos contra sitios de Internet.
– Nuevos tipos de ataques o nuevas vulnerabilidades.
– Ataque con código dañino.
– Análisis forense de equipos comprometidos.
– Ataque a sistemas CIS de infraestructuras críticas.

Una de las funciones que desarrolla el CCN-CERT es la promoción de otros CERT,s. Para ello proporciona la información, formación y herramientas necesarias para que la comunidad pueda desarrollar sus propios CERT,s, actuando el CCN-CERT como coordinador de CERT,s a nivel gubernamental. Además, realiza el diseño de guías y herramientas de implantación y operación.

En cuanto a la Protección de Infraestructuras Críticas, el CCN-CERT apoya al Centro Nacional de Protección de Infraestructuras Críticas. En particular proporciona:

– Coordinación a nivel nacional.
– Información sobre incidentes.
– Apoyo a las Fuerzas y Cuerpos de Seguridad del Estado.
– Apoyo en análisis y gestión de riesgos.

Además del CCN-CERT, desarrollan funciones en la defensa del ciberespacio las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado. Dentro de ellas, merece especial mención El Grupo de Delitos Telemáticos de la Guardia Civil y la Brigada de Investigación Tecnológica de la Policía Nacional.

Conclusiones

En el mundo actual pocos son ya los ámbitos de la sociedad donde no están presentes los sistemas de información, y este empleo parece que continuará aumentando en el futuro. En muchas organizaciones, entre las que se encuentran infraestructuras críticas para las naciones, estas tecnologías desempeñan ya funciones insustituibles y primordiales. Como consecuencia, las redes de estas infraestructuras se presentan como una de las mayores vulnerabilidades actuales, a la vez que provocan que el ciberespacio sea uno de los campos de mayor esfuerzo y desarrollo actual en la seguridad y defensa.

En la nueva Directiva de Defensa Nacional ya se considera la amenaza cibernética como un riesgo. Sin embargo, este reconocimiento no es suficiente. Es necesaria una estrategia para la defensa del ciberespacio, que permita sentar los objetivos estratégicos para el posterior proceso de planeamiento de capacidades. Esta estrategia debería desarrollarse de forma individual, como ya sucede en países líderes en este campo, como Estados Unidos, o, por lo menos, ser un capítulo importante en la futura Estrategia de Seguridad y Defensa Nacional.

Muchas de las acciones necesarias para la lucha contra las ciberamenazas descritas anteriormente ya se han tomado en España. Entre las instituciones con responsabilidades en este campo se encuentran el CCN-CERT y unidades específicas de las Fuerzas y Cuerpos de Seguridad del Estado. Sin embargo, quedan sin cubrir algunos puntos importantes. Uno de ellos es el de la información sobre ciberseguridad a los usuarios domésticos. El CCN-CERT se ocupa de la difusión de información a grandes entidades, pero no desciende al público en general. Dado que como se ha mencionado varias veces, la seguridad del ciberespacio atañe a todos, debería hacerse un esfuerzo gubernamental en este sentido. Algunos ejemplos de acciones útiles son campañas en los medios de comunicación, o la existencia de una página *web* específica.

También se echa en falta un órgano asesor y coordinador al más alto nivel gubernamental. Este órgano no solamente serviría como único punto de contacto presidencial para los asuntos relacionados con el ciberespacio, sino que se comportaría como coordinador de todos los esfuerzos realizados por los diferentes actores con competencias en su defensa.

Como ya se ha expuesto, la procedencia de los ataques es dispar. Estos pueden ser acciones de terroristas, criminales o naciones. Esto tiene como consecuencia la necesidad de un esfuerzo multidisciplinario. Es la razón de que existan unidades diferenciadas en la lucha contra las diferentes procedencias de las amenazas. En este contexto, cabe la duda sobre el posible papel de las Fuerzas Armadas en la defensa del ciberespacio, o en su empleo como medio ofensivo. En cualquier caso, las Fuerzas Armadas son una parte importante en la ciberdefensa, porque su infraestructura es una de las denominadas críticas, y a su vez depende de otras infraestructuras críticas, además de hacer un uso extensivo de las tecnologías de la información.

En el caso de que, a semejanza de lo que se está produciendo en otros países, se decida la participación de las Fuerzas Armadas como actor en

el ciberespacio, debe acotarse de forma detallada sus responsabilidades, pues de ello depende el planeamiento adecuado de las capacidades necesarias, tanto defensivas como, en su caso, ofensivas.

Todos estos esfuerzos no alcanzarán el nivel de seguridad buscado si no se prueban los diferentes planes y medidas puestas en práctica. Para ello, el Gobierno debe diseñar medidas de rendimiento y evaluar la efectividad de los programas de ciberseguridad. Para este fin son útiles los ejercicios de simulación y las iniciativas ya descritas del CAPEC y *Cyberwar Playbook*.

Las tecnologías de la información siguen sufriendo un continuo desarrollo, lo que supone que el esfuerzo en la obtención de su seguridad debe ser un proceso también continuo. España no puede quedarse atrás, pues como la realidad nos ha mostrado en varias ocasiones, la amenaza también nos tiene en su punto de mira.

Bibliografía

Libros y monografías:

VERTON, Dan: *Black Ice. La amenaza invisible del ciberterrorismo,* editorial McGraw-Hill, 2004.

VIGILANT, Jean-Marc: *Ciberterrorismo,* Escuela Superior de las Fuerzas Armadas, 20 de marzo de 2002.

Publicaciones y artículos disponibles en páginas web:

ALANDETE, David: «Cómo Obama puede salvar la Red», *El País.com,* 9 de diciembre de 2008, consultado el 24 de enero de 2009, en: *http://www.elpais.com/articulo/Pantallas/Obama/puede/salvar/Red/elpepurtv/20081209elpepirtv_3/Tes*

ARMIN, Jart and WALTON, Greg: «The Kyrgyzstan DoS Attacks of January, 2009: Assessment and Análisis», *IntelFusion.net,* consultado el 30 de enero de 2009, en:*http://intelfusion.net/wordpress/?p=516*

BARNUM, Sean: *Attack Patterns: Knowing Your Enemy in Order to Defeat Them,* Cigital Inc., 1 de marzo de 2007, consultado el 10 de enero de 2009, en: *http://capec.mitre.org/documents/Attack_Patterns-Knowing_Your_Enemies_in_Order_to_Defeat_Them-Slides.pdf*

— CAPEC *(Common Attack Pattern Enumeration and Classification) Schema Description),* Cigital Inc., 15 de enero de 2008, consultado el 10 de enero de 2009, en: *http://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf*

BARNUM, Sean y SEIT, Amit: *Attack Patterns as a Knowledge Resource for Building Secure Software,* Cigital, Inc., 2007, consultado el 10 de enero de 2009, en:*http://capec.mitre.org/documents/Attack_Patterns-Knowing_Your_Enemies_in_Order_to_Defeat_Them-Paper.pdf*

BRODIE, Cindy: *The Importance of Security Awareness Training,* SANS Institute Infosec Reading Room, 30 de junio de 2008, consultado el 28 de enero de 2009, en: *http://www.sans.org/reading_room/whitepapers/awareness/rss/the_importance_of_security_awareness_training_33013*

CCN-CERT: El *CERT Gubernamental Español, Servicio de Respuesta a Incidentes de Seguridad para la Administración,* Centro Criptológico Nacional (CCN), octubre de 2008, onsultado el 18 de enero de 2009, en: *https://www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_2008.10_Castilla_y_Leon.pdf*

CSIS: *Securing Cyberspace for the 44th Presidency, d*iciembre 2008, consultado el 10 de enero de 2009, en: *http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf*

Cyberwar-The Battle for Gaza on the Internet, Hostexploit.com, consultado el 6 de enero de 2009, en: *http://hostexploit.com/index.php?view=article&catid=1%3Aarticles%E2%80%A6&tmpl=component&print=1&layout=default&page=&option=com_content*

Cyberwar-The Cyber Iron Curtain: Now Kyrgyzstan, Hostexpliot, 26 de enero de 2009, consultado el 18 de febrero de 2009, en: *http://hostexploit.blogspot.com/2009/01/cyberwar-cyber-iron-curtain-now.html*

«El "cibercrimen", un desafío para el sistema judicial que exige la colaboración entre Estados y empresas», en *Cibersur.com,* 7 de octubre de 2008, consultado el 24 de enero de 2009, en: *http://www.cibersur.com/modules.php?name=News&file=article&sid=11479&theme=Cibersur&ref=64*

El CSIC prueba un sistema que ayudará a luchar contra el espionaje informático. La web del programador, 4 de junio del 2008, consultado el 24 de enero de 2009, en: *http://www.lawebdelprogramador.com/noticias/mostrar.php?id=1983*

GÓMEZ, Juan: «Los troyanos espían en Alemania», *El País.com,* 2 de septiembre de 2007, consultado el 24 de enero de 2009, en: *http://www.elpais.com/articulo/reportajes/troyanos/espian/Alemania/elpeputec/20070902elpdmgrep_5/Tes*

HERNÁNDEZ, José: «¡Cuidado! Miran a través de tu cámara», *El País,* 28 de septiembre de 2008, consultado el 12 de noviembre de 2009, en: *http://www.elpais.com/articulo/sociedad/Cuidado/Miran/traves/camara/elpepisoc/20080928elpepisoc_1/Tes*

Indias Sino cyber concerns, Janes Intelligence Digest, 23 de septiembre de 2008. Base de datos IRIS (necesaria suscripción), en: *http://www.janes.com*

KASPERSKY, Eugene: *Cybercrime arms race,* Kaspersky lab, 17 de septiembre de 2008, versión traducida al español, consultado el 24 de enero de 2009, en:*http://www.viruslist.com/sp/analysis?pubid=207271000#1*

LANGEVIN, Jim and MCCAUL, Michael: *US must update laws defending against foreign hackers,* Houston Chronicle, 20 de diciembre de 2008, consultado el 6 de enero de 2009, en: *http://www.chron.com/disp/story.mpl/editorial/outlook/6174987.html* (necesario darse de alta).

«Lanzan certificación europea sobre cibercriminalidad y pruebas electrónicas», *DiarioTI.com,* 3 de diciembre de 2008, consultado el 24 de enero de 2009, en:*http://www.diarioti.com/gate/n.php?id=20545*

«Microsoft, víctima del "ciberespionaje" industrial», *El Mundo.es,* 27 de octubre de 2000, consultado el 20 de enero de 2009, en: *http://www.elmundo.es/navegante/2000/10/27/microsoft.html*

MIKKELSEN, Randall: *Estados Unidos no está listo para ciberataque, demuestra juego,* Reuters, 19 de diciembre de 2008, consultado el 24 de enero de 2009, en: *http://lta.reuters.com/article/internetNews/idLTASIE4BI02D20081219?pageNumber=3&virtualBrandChannel=0&sp=true*

PIPER, Paul: *«Nets of Terror, Terrorist Activity on the Internet», Information Today, Inc.,* volume 16, número 10 de noviembre/diciembre 2008, consultado el 30 de enero de 2009, en: *http://www.infotoday.com/searcher/nov08/Piper.shtml*

REYNA, Luis: «El bien jurídico en el delito informático», *Alfa-Redi:* Revista de Derecho Informático, número 33, abril de 2001, consultado el 24 de enero de 2009, en: *http://www.alfa-redi.org/rdi-articulo.shtml?x=667*

RIVEIRO, Aitor: «Piratas informáticos robaron información confidencial de los ordenadores de Obama y McCain», *El País.com*. 6 de noviembre de 2008, consultado el 6 de enero de 2009, en: *http://www.elpais.com/articulo/internet/Piratas/informaticos/robaron/informacion/confidencial/ordenadores/Obama/McCain/elpeputec/20081106elpepunet_2/Tes*

RUSCH, Jonathan: The «Social Engineering» of Internet Fraud, ISOC *(Internet Society),* 1999, consultado el 24 de enero de 2009, en: *http://www.isoc.org/inet99/proceedings/3g/3g_2.htm*

SMITH, Sebastian: «"Cybergeddon" strikes fear». *Iafrica.com,* a division of Primedia Online, consultado el 10 de enero de 2009, en: *http://lifestyle.iafrica.com/content_feed/telkom/1425520.htm*

THE WHITE HOUSE: *The National Strategy to Secure Cyberspace,* febrero de 2003, consultado el 10 de enero de 2009, en: *http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf*

TINNEL, Laura; SAYDJARI, Sami and FARRELL, Dave: *Cyberwar Strategy and Tactics,* Proceedings of the 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, junio de 2002, consultado el 24 de enero de 2009, en: *http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf*