ISSN: 1988-2629. No. 13. Nueva Época. Marzo-Mayo, 2013

El ciberespionaje

Gema Sánchez Medero[1]
gsmedero@cps.ucm.es

Resumen

Hoy en día Internet conecta a millones de redes, incluidas aquellas que hacen funcionar infraestructuras y servicios esenciales. De modo que la economía y la seguridad nacional dependen en gran medida de las tecnologías de la información y de la infraestructura de comunicaciones. De ahí que el tema de la ciberdefensa y el ciberataque hayan emergido con fuerza en la agenda política de los gobiernos, siendo éstos los que se están lanzando a la red para vigilar cualquier posible acción delictiva contra sus intereses. Es por este motivo que en este artículo se ha analizado una de esas actividades delictivas: el ciberespionaje.

Palabras clave

Ciberespionaje, internet, TIC, infraestructuras críticas, ciberataque y ciberdefensa.

Abstract

Today the Internet connects millions of networks, including those that run critical infrastructure and services. Thus the national economy and security largely depend on information technology and communications infrastructure. Hence, the issue of cyber defense and cyberattacks have emerged strongly in the political agenda of governments, those being the ones who enter the network quickly and deeply to monitor any possible criminal action against their interests. This is the reason why such a crime has been chosen as topic here.

Keywords

Cyberespionage, internet, TIC, critical infrastructure, cyberattack and cyberdefense.

1. Introducción

Las TIC (Tecnologías de la Información y el Conocimiento) han ocasionado una revolución sin precedentes cuyo alcance todavía es insospechado. La globalización ha 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, y a que su repercusión para la sociedad sea extraordinaria, llegándose incluso a hablar de 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 interconectadod: los sistemas de seguridad, defensa, comerciales,

[1] Prof. de Ciencia Política y de la Administración en la Universidad Complutense de Madrid. Doctora en Ciencias Políticas y de la Administración por la Universidad Complutense de Madrid.

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 haya 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 hallar noticias sobre algún hecho ilícito que se ha producido a través de la red. De ahí que a lo largo de este trabajo nos hayamos marcado como objetivo estudiar las actividades de ciberespionaje más celebres que se han producido en los últimos años, y qué soluciones se están dando y buscando para intentar contrarrestar la presencia y actividades delictivas en Internet.

2. Ciberespionaje

El ciberespionaje no es comparable al espionaje tradicional. Con anterioridad, el espionaje consistía en pichar un teléfono del adversario o en interceptar comunicaciones, o bien enviar un espía para que se infiltrara en las instituciones de otro país con el fin de apoderase de información clave y secreta. En cualquier caso, el objetivo de estas acciones era conseguir información, pero en ningún caso se trataba de manipularla ni destruirla. En cambio, con el ciberespionaje es muy normal que, después de hacerse con la información, se la manipule, se la borre o se la destruya, etc. Así, dentro del ciberespionaje se pueden incluir acciones como, por ejemplo, reconocer los sistemas (obtener información previa sobre las organizaciones y sus sistemas informáticos, para poder escanear sus puertos con el objetivo de determinar qué servicios se encuentran activos, etc), detectar las vulnerabilidades de los sistemas (para después desarrollar alguna herramienta que permita explotarlas fácilmente, como el *"exploits"*), robar información mediante la interceptación de mensajes, modificar el contenido y la secuencia de los mensajes transmitidos, analizar el tráfico (observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los *"sniffers"* o *"switches"*), realizar ataques de suplantación de la identidad IP *Soofing*, capturar contraseñas y cuentas de usuarios, conectarse de forma no autorizada a equipos, servidores y sistemas informáticos, enviar malware, ataques a sistemas criptográficos, engañar y extorsionar, o denegar servicios.

3. El ataque cibernético y las medidas a adoptar

Todo ataque contra una red de ordenadores o de sistemas informáticos suele seguir las siguientes etapas:

- Descubrimiento y exploración del sistema informático.
- Búsqueda de las vulnerabilidades en el sistema.
- Explotación de las vulnerabilidades.
- Modificación de programas y ficheros para dejar instaladas las puertas traseras, y creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema.
- Eliminación de las pruebas que puedan revelar el ataque, incluso, se puede llegar a parchear las vulnerabilidades descubiertas en el sistema.

No obstante, para poder llevar a cabo este tipo de ataques es necesario que los intrusos dispongan de los conocimientos y medios técnicos necesarios. Además deben tener una

determinada motivación o finalidad y una oportunidad que facilite el desarrollo del ataque, como podría ser un fallo en la seguridad del sistema informático elegido.

En cambio, las medidas a adoptar pasan por detectar el ataque. En esta primera fase es necesario buscar la naturaleza del mismo, la información que se ha comprometido, la extensión del daño, el objetivo del intruso, las herramientas empleadas y las vulnerabilidades que se han podido detectar. Después hay que lanzar la alerta y, a continuación, propiciar la respuesta e iniciar la recuperación. Para ello, es necesario que, previamente, los gobiernos y los actores gubernamentales se hayan decantado por desarrollar planes de contingencia que sean adecuados y probados y planes de asistencia mutua entre los diferentes componentes de la infraestructura crítica. No obstante, todos estos planes deben estar coordinados por un órgano superior a nivel nacional, que debe depender directamente del departamento encargado de la seguridad cibernética. Por último, ante todo ataque cibernético se debe facilitar el intercambio de información. Esta última fase es esencial, pero existen grandes dificultades para conseguirlo dado que primaría el miedo a que los datos confidenciales se hicieran públicos si se compartieran con otros Estados. De ahí que la mayoría de los ciberdelitos sean abordados internamente por las mismas organizaciones afectadas. Incluso, en la mayoría de los casos, no se llegan hacer públicos ni siquiera lo incidentes acontecidos. Un grave error, dado que de las experiencias de unos podrían aprender los otros y viceversa.

4. Los sistemas de espionaje y de control

Existen numerosos sistemas de espionaje, pero tal vez los más relevantes son los que vamos a analizar en este apartado, principalmente, porque son creados y puestos en marcha por los Estados.

4.1. El sistema "Echelon"

El "Echelon" o la "Gran Oreja" es un sistema automatizado de interceptación 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 interceptación 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 clave, 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 facilita a los demás "diccionarios de palabras clave" para que los incorporen como "filtros automáticos" a los aparatos de interceptación de las comunicaciones. Lógicamente estas "palabras clave" y "diccionarios" varían con el tiempo y de acuerdo con los intereses particulares de los países integrantes del sistema. Aunque, este sistema no sólo intercepta, sino que desencripta, filtra, examina y codifica esta información (Pachón, 2004: 13).

La idea de este proyecto es detectar determinadas palabras consideradas "peligrosas" para la seguridad nacional de los Estados Unidos o de los países participantes en el proyecto. Hasta tal punto es así que se estima que cada media hora se interceptan cerca de mil millones de mensajes que luego son filtrados mediante diversos parámetros de búsqueda para extraer los datos de interés para cada país. Así, una vez detectada la comunicación, el sistema informático pasa a monitorearla y grabarla. Entonces esta grabación es etiquetada y enviada a distintos centros de análisis. Dependiendo del origen y fecha de la comunicación, será marcada con un número clave. Se transcribe, descifra, traduce y se guarda entonces como un informe más o menos extenso.

Estos informes recibirán un código dependiendo del grado de secretismo otorgado al mismo: "Morai" equivale a secreto. Después le siguen los códigos "Spoke" (más secreto), "Umbra" (alto secreto), "Gamma" (comunicaciones rusas) o "Druid" (destinado a países no miembros de la red). Después se asignará otro código más relacionado con cada una de las agencias de seguridad. Si se considera que es una transmisión peligrosa para los intereses de los Estados que componen la red Echelon, los participantes de esa comunicación pasarán a formar parte de una lista negra y, a partir de entonces, sus comunicaciones y acciones serán espiadas, en mayor o menor medida, dependiendo de las distintas consideraciones que los responsables crean oportunas. El problema al que se está enfrentando el programa es la saturación de información, y eso que a cada Estado participante se le asigna un área de control determinada. Por ejemplo, a Canadá le corresponde el control del área meridional de la antigua Unión Soviética; a los EE. UU., gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China; a Gran Bretaña, Europa, Rusia y África; a Australia, Indochina, Indonesia y el sur de China; y a Nueva Zelanda, la zona del Pacífico Occidental. Hasta tal punto que todo indica que, en la actualidad, relativamente pocos son los mensajes y las llamadas telefónicas que se transcriben y registran. La mayoría son eliminados después de ser leídos por el sistema (Pachón Ovalle, 2004).

En todo caso, los componentes de este sistema son (Pachón Ovalle, 2004: 6-7):

1º. Los satélites militares, que se encuentran situados en:

- MILSTAR. (USA). Gestiona 6 satélites geoestacionarios para comunicación militar a nivel mundial con navíos, bases terrestres, aviones, barcos y submarinos.

- DSCS. (USA). Compuesto por 5 satélites para comunicación global.

- SKUNET. (UK). Sistema de cobertura mundial.

- SYRACUSE. Francés, de alcance regional.

- SICRAL. Italiano, de alcance regional.

- SISTEMA ESPAÑOL. De alcance regional que utiliza la banda X de los satélites civiles, como es el caso del francés y del italiano.

- MOLNYIA. Ruso, que utiliza también la banda X.

- OTAN. Las series de satélites NATO IIID, NATO IVA y NATO IVB.

2º. Los satélites espía:

- Según MSNBC y NBC News10, la red Echelon tiene un sistema especial adicional de satélites espía de uso permanente.

3º. Los nodos de conexión:

- Nodo de College Park, localizado en Maryland-USA.

- Nodo de Mountain View, localizado en California-USA.

- Nodo de Westminster, en Inglaterra.

4º. Las estaciones de escucha:

- Morwenstow (Inglaterra), encargada de coordinar las escuchas de satélites INTELSAT en Europa, Océano Atlántico y Océano Pacífico.

- Menwith Hill (Inglaterra), para coordinación con satélites diferentes de INTELSAT. Maneja el núcleo central del programa informático.

- Bad Aibling (Alemania), para coordinación con satélites diferentes de INTELSAT.
- Submarino USS Match, para "pinchar" comunicaciones en cable submarino.

- Sugar Grove, en Virginia USA.

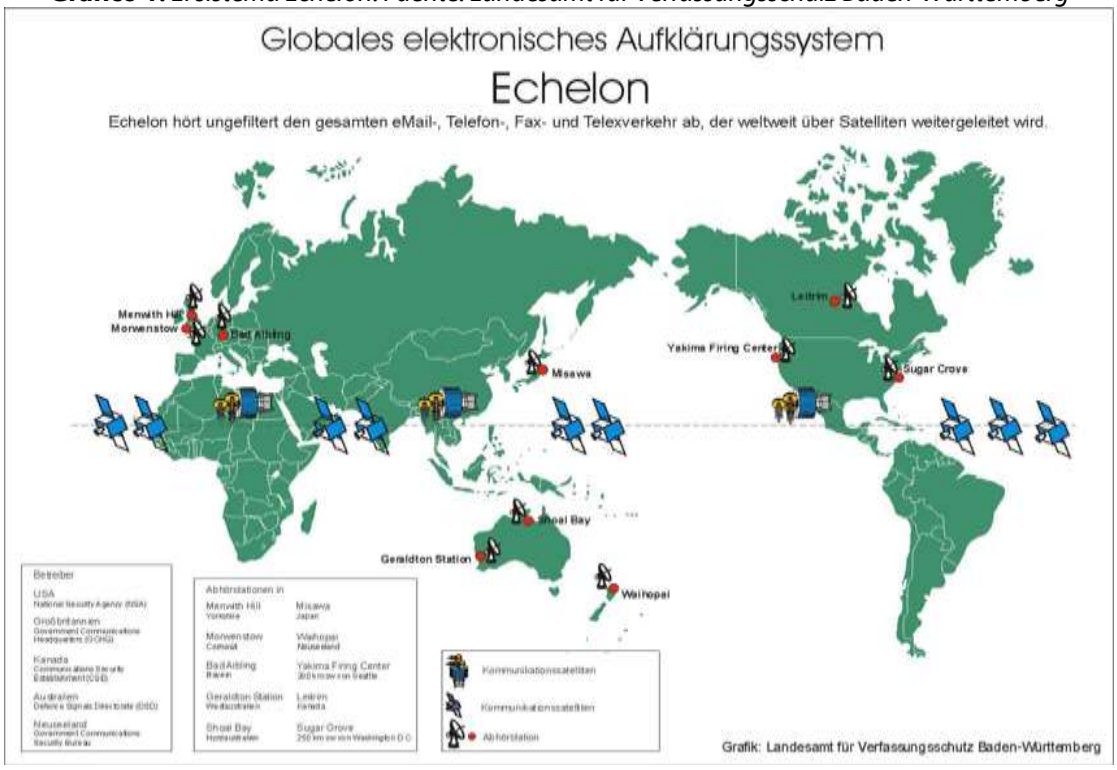
- Leitrim, Canadá.

- Sabana Seca, en Puerto Rico.

- Waihopai, Nueva Zelanda.

- Shoal Bay, Australia.

Gráfico 1: *El sistema Echelon. Fuente: Landesamt für Verfassungsschulz Baden-Württemberg*



En todo caso, si hoy se conoce lo que es el sistema Echelon ha sido gracias al espionaje industrial. Los intereses económicos de los países implicados y de las multinacionales han sido la causa que ha llevado a este sistema al debate público (Rodríguez Pérez, 2008). Téngase en cuenta que, por ejemplo, la interceptación de los faxes y las llamadas telefónicas entre Airbus y el Gobierno de Arabia Saudí con los detalles de las comisiones ofrecidas a los funcionarios permitió a Estados Unidos presionar para que el contrato de un billón de pesetas fuera concedido a Boeing-McDonnell Douglas en 1995 (Pachón Ovalle, 2004: 5); o la interceptación de las comunicaciones entre el Gobierno de Indonesia y representantes de la empresa japonesa NEC, en relación con un contrato de 200 millones de dólares en equipamiento de telecomunicaciones, permitió a George Bush intervenir personalmente para obligar a Indonesia a dividir el contrato

entre la NEC y la firma estadounidense AT&T (Pachón Ovalle, 2004: 5); o la interceptación de las comunicaciones entre Thomson-CSF y el Gobierno brasileño para la negociación de un contrato de 220.000 millones de pesetas para un sistema de supervisión por satélite de la selva amazónica permitió la concesión del proyecto a la empresa estadounidense Raytheon, vinculada con la red Echelon (Rodríguez Pérez, 2008).

4. 2. El sistema "Enfopol"

"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, Australia, pero también en otros países. De esta manera, 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 en los sistemas privados. Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas). 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.

No obstante, Enfopol sólo funcionaba dentro de los límites de la Unión Europea, a diferencia de otros sistemas de control, que actúan sobre todo el planeta. Eso sí, según este sistema, las agencias de la ley y el orden pueden interceptar todo tipo de comunicaciones. Es más, pueden requerir: acceso a toda la comunicación transmitida, a todos los sujetos interceptados y a todos los datos asociados a la comunicación, así como a la señal de "listo para acceso", número (de teléfono, IP, etc) del sujeto que llama y del que recibe la llamada, con una identificación de tales personas, duración, comienzo y fin de la conexión, destino real y destinos intermedios en el caso de llamadas derivadas; información sobre la ubicación geográfica del sujeto, con la máxima exactitud posible; datos sobre los servicios específicos usados por los interlocutores, y sus parámetros técnicos; capacidad de monitorización de las comunicaciones en tiempo real, o lo antes posible; cooperación de los operadores/servidores de redes para proporcionar "interfaces" para transmitir la comunicación interceptada a la oficina policial correspondiente, y para facilitar dicha comunicación: datos asociados a una llamada y que permitan una correlación de dichos datos con la llamada; cooperación de los operadores/servidores para que proporcionen las comunicaciones "en claro", cuando haya de por medio codificación, compresión o cifrado de la misma; una interceptación tal que el sujeto investigado no esté al corriente de dicha interceptación; un diseño de interceptación que evite el uso autorizado de la información; y la posibilidad de efectuar interceptaciones simultáneas (de modo que, por ejemplo, las policías de cinco países puedan todas escuchar una conversación al mismo tiempo) [2].

4.3. El sistema "Carnivore"

El "Carnivore"[3] es la tercera generación de los sistemas de espionaje de redes del FBI[4]. Un sistema que ha sido diseñado por la Oficina Federal de Investigaciones (FBI) para capturar

[2] Taller de Criptografía-Informe 11: Enfopol: El Gran Hermano Europeo, 17 mayo de 1999. En: http://www.ugr.es/~aquiran/cripto/informes/info011.htm (fecha de consulta: 3/10/2012)

[3] Después, el FBI modificó el nombre, denominándole "DCS1000".

[4] El primero fue Etherpeek, actualmente, un programa comercial. El segundo, Omnivore, fue usado entre 1997 y 1999. Y el tercero, el DragonWare estaba compuesto por otros tres: Carnivore, que capturaba la información; Packeteer, que convertía los paquetes interceptados en textos coherentes, y Coolminer, que los analizaba.

aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la agencia. Se especula, incluso, con 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).

No obstante, esta aplicación forma parte de un programa más complejo y amplio de vigilancia, llamado Cyber Knight (Caballero cibernético), el cual incluye diversas bases de datos que permiten al FBI cruzar información proveniente de e-mails, salas de chat, messenger y las llamadas telefónicas realizadas a través de Internet (Añover, 2001), y un sistema llamado "Magic Lantern" que permite acceder y apropiarse de las contraseñas de los sospechosos que usen correo electrónico encriptado en sus comunicaciones. Aunque, el Carnivore ha sido abandonado por el FBI para pasar a emplear un software comercial que revise el tráfico informático en el marco de sus investigaciones.

4.4. Otros sistemas de control

Pero estos no son los únicos sistemas de control. Además existen otros. Por ejemplo, el Ministerio de Defensa español, junto con Italia y Francia, han puesto en marcha el proyecto Infraestructura Semántica Operacional (OSEMINTI). Se trata de que los Servicios de Inteligencia, por medio de ordenadores, no sólo puedan identificar frases o palabras concretas en cintas de grabación o en textos escritos, sino que sean capaces de entenderlas. Es un sistema inteligente programado para aprender a medida que interactúa con las personas, de modo que no serán necesarios medios humanos para cotejar esa información que se genera. Sintel es otro sistema integrado de interceptación legal de telecomunicaciones que también gestiona el Ministerio de Interior español. Un sistema informático que permite interceptar las comunicaciones y otra serie de datos como la localización geográfica de los interlocutores, el tráfico de llamadas, los mensajes SMS, los accesos a Internet, etc, es decir, un sistema capaz de rastrear, interceptar y almacenar cualquier conversación llevaba a cabo vía electrónica.

Por otra parte, el Congreso de EEUU creó el Foreign Intelligence Surveillance Court (FISC) como una corte "top-secret" para enterarse de las aplicaciones de vigilancia electrónica que realizaba el FBI y la NSA, y chequear las actividades domésticas de estas agencias, con el único fin de velar por los derechos constitucionales del pueblo americano (Pachón, 2004, 16). Otro es el proyecto "Shamrock", que comenzó a caminar en 1945, con el objetivo de obtener copias de la información telegráfica existente en EE.UU. Para tal cometido, el Gobierno estadounidense contó con la colaboración de la Global Communications (RCA), la World Communications, Incl (ITT) y la Western Union. El sistema inicial de microfilmación cambió radicalmente con el uso de cintas magnéticas de computador, a través del famoso HARVEST que tenía la capacidad de gravar las comunicaciones y espiarlas mediante el empleo de palabras claves. El proyecto MINARET vino a ser un sistema gemelo del SHAMROCK. Paralelamente a estos dos proyectos, la CIA creó por orden del Presidente Lyndon Johnson, la Domestic Operation Division (DOD), cuyo propósito era dirigir, apoyar y coordinar operaciones clandestinas contra activistas dentro de los Estados Unidos. Así, frente a las constantes protestas estudiantiles por la guerra de Vietnam, la DOD instauró dos unidades de acción contra las organizaciones y los activistas antiguerra: el proyecto RESISTANCE y el proyecto MERRIMAC. El primero se desarrolló en coordinación con los directores de los Colleges y las Universidades, la seguridad de los campus y las policías locales. El segundo monitoreaba cualquier demostración antiguerra en

Washington. Pero fue el Presidente Nixon el que oficializó todas estas actividades de vigilancia mediante la Operación CHAOS, aunque el proyecto dejó de tener vigencia tras el escándalo Watergate.

5. Un estudio de caso: Estonia

A finales de abril de 2007, las principales páginas web de Estonia (bancos, sitios gubernamentales, partidos políticos, etc) fueron atacadas y bloqueadas durante varios días. Estos ataques coincidieron con la decisión, por parte del Gobierno de Estonia, de trasladar una estatua del memorial ruso de la II Guerra Mundial a otro lugar de ubicación, el Soldado de Bronce de Tallín. El soldado de bronce era considerado por la comunidad rusa como un símbolo de sus caídos en la Segunda Guerra Mundial y era costumbre depositar flores a sus pies en señaladas fechas conmemorativas de la victoria rusa, mientras que, para los estonios, el soldado es considerado como un símbolo de la era soviética que no trae buenos recuerdos a muchos estonios.

Ante la decisión adoptada por el Gobierno de Estonia, las web del Congreso, del Presidente y del Primer Ministro quedaron bloqueadas por la cantidad de consultas realizadas. Además, se produjo una fuerte protesta del Gobierno de Rusia y de las minorías étnicas rusas en Estonia. Incluso, en determinados foros rusos, se difundieron mensajes patrióticos y se explicaba la forma de realizar ataques cibernéticos sencillos. Para estos ataques se usaban "botnets" y "defacements" con propaganda rusa, modificando ciertas páginas web sin autorización de sus dueños. Esto llevó a que no sólo se vieran afectadas las webs anteriormente mencionadas, sino también las de la policía, el Ministerio de Economía, Agricultura, Medio Ambiente, Asuntos Exteriores y el Departamento de Comunicaciones. Ante tal caos, fue necesaria la intervención y la coordinación de varios CERTs a nivel internacional, además de desconectar todo el país de internet, con el objetivo de poder seguir usando los servicios online internos. Además, desde entonces, varios países (EEUU, Reino Unido, Francia, Alemania, etc.) han comunicado haber sido objeto de ataques de este tipo tratando de introducirse en los sistemas de información gubernamental.

Este ataque marcó un hito y un reto histórico para la OTAN, ya que fue la primera vez que un país miembro solicitó apoyo a la organización por un sistema de información y comunicación. En aquel momento, la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro, lo que obligó a adoptar medidas conjuntas para mejorar la protección ante ciberataques, y por ello, el Consejo de la OTAN firmó la política de ciberdefensa en enero de 2008. Incluso la Alianza Atlántica creó en Tallín (Estonia) el Centro de Excelencia para la Cooperación en Ciberdefensa, cuyo objetivo es estudiar ciberataques y determinar las circunstancias en las que deben activar el principio de defensa mutua de la Alianza Atlántica. En la actualidad forman parte de él: España, Italia, Alemania, Eslovaquia, Estonia, Letonia, EE.UU, 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 personal experto en ciberseguridad y especializado en tres ramas fundamentalmente: 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 miembros y de la OTAN y tiene el estatus legal de Organización Militar Internacional.

6. Conclusiones

Hoy en día, Internet conecta a millones de redes, incluidas aquellas que hacen funcionar infraestructuras y servicios esenciales. De modo que la economía y la seguridad nacional dependen, en gran medida, de las tecnologías de la información y de la infraestructura de comunicaciones. De ahí que el tema de la ciberdefensa y el ciberataque hayan emergido con fuerza en la agenda política de los gobiernos, dada cuenta que, como sostiene William Crowell, exsubdirector de la Agencia para la Seguridad Nacional, "en el curso de los próximos veinte o treinta años, el papel de los ciberataques en caso de guerra cobrará cada vez más importancia".

Y para garantizar la seguridad de los ordenadores no hay nada mejor que apagar el ordenador. El problema es que hoy en día eso parece imposible y, por eso, se están activando otras acciones que puede contribuir a frenar este tipo de ataques y sus consecuencias, como dotarse de medios de seguridad especializados en ciberdefensa para reducir las amenazas y las vulnerabilidades de los mismos, aunque siempre considerando que existe la posibilidad de que sean vulnerados. En este sentido, el intercambio de información entre los actores víctimas de ataques puede ser fundamental, aunque eso siempre es difícil por el miedo a que se filtren datos confidenciales, se conozcan las vulnerabilidades, etc. Otra posible operación es establecer planes de asistencia mutua entre los diferentes componentes de las infraestructuras críticas, de modo que se reduzcan los efectos en cascada debido a su interrelación. Eso sí, todos estos planes deben ser coordinados por un órgano superior a nivel nacional, que debe depender directamente del Departamento Gubernamental encargado de la seguridad del ciberespacio (Puime, 2009: 57). Otra es 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, centros educativos, máquinas populares de acceso a Internet y otras donde, de forma anónima, las personas pueden conectarse y realizar actividades ilícitas (Sánchez Medero, 2009). 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). Otra posible solución es empezar a endurecer la legislación que hace referencia a los delitos informáticos para paliar las posibles deficiencias jurídicas que existen en algunos países. Y otra, como algunos investigadores consideran, es crear una segunda red extraordinariamente controlada y separada del Internet comercial (Waston, 2007).

Bibliografía

Añover, Julián. (2001). "Echelon y Enfopol nos espían", en *Internacional*, el 16 de noviembre. En http://www.nodo50.org/altavoz/echelon.htm (fecha de consulta: 3/10/2012).

Brookes, Peter. (2007) "Contrarrestando el arte de la guerra informática", en *Grupo de Estudios Estratégicos*, nº 2011, octubre. En: http://www.gees.org/articulo/4637/ (fecha de consulta: 3/10/2012).

Busón Buesa, Carlos. (2009). *Control en el Ciberespacio*. Conferencia en el Programa Modular en Tecnologías Digitales y Sociedad del Conocimiento, celebrada el 22 de agosto. En http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm (fecha de consulta: 3/10/2012).

Candau Romero, Javier. (2011). "Estrategias Nacionales de Ciberseguridad. Ciberterrorismo", en Joyanes Aguilar, Luis (coord.) *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Madrid: Cuadernos de Estrategia.

Caro Bejarano, M. J. (2011). *Nuevo Concepto de Ciberdefensa de la OTAN*. Documento Informativo del IEEE, nº 9, marzo. En:

http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09_2011ConceptoCiberdefensaOTAN.pdf (fecha de consulta: 3/10/2012).
Colle, R. (2000). "Internet: un cuerpo enfermo y un campo de batalla", en *Revista Latina de Comunicación Social*, nº 30, junio. En: http://www.ull.es/publicaciones/latina/aa2000qjn/91colle.htm (fecha de consulta: 3/10/2012).
Fojón Chamorro, Enrique y Sanz Villalba, Ángel F. (2010). "Ciberseguridad en España: una propuesta para su gestión", en *ARI*, nº 101, junio.
Joyanes Aguilar, L. (2010). "Introducción. Estado de la cuestión de la Ciberseguridad", en *Cuadernos de Estrategia, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, 149, 13-49.
Pachón Ovalle, G. (2004). "La red Echelon: Privacidad, Libertad y Criptografía", *Virtualidad Real*. Programa de Doctorado en SIC. Universitat Oberta de Catalunya. En: http://www.virtualidadreal.com/Red%20Echelon.pdf (fecha de consulta: 3/10/2012).
Puime Maroto, J. (2009). "El ciberespionaje y la ciberseguridad", en CESEDEN, *La violencia del Siglo XXI. Nuevas dimensiones de la guerra*. Madrid: Monografías del CESEDEN, octubre, 112, 42/70.
Rodríguez Pérez, Carlos. (2008). *Tecnologías de vigilancia e investigación: El caso Echelon. Informe: Tecnologías de vigilancia e investigación*. Postgrado conocimiento, ciencia y ciudadanía en la sociedad de la información. Barcelona: Universitat de Barcelona. En: http://www.ub.es/prometheus21/articulos/obsprometheus/crodr_echelon.pdf (fecha de consulta: 3/10/2012).
Sánchez Medero, G. (2009). "Ciberguerra y Ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica", en Amérigo Cuervo-Argango, F. y De Peñaranda Algar, J. (Comp.) *Dos décadas de Posguerra Fría. Actas de I Jornadas de Estudios de Seguridad*. Madrid: Instituto Universitario General Gutiérrez Mellado-UNED, 215/241.
Sánchez Medero, G. (2010) "Los Estados y la ciberguerra", *Boletín de Información del CESEDEN*, diciembre, 317, 63/75.
Sánchez Medero, G. (2011a) "Ciberespacio y el Crimen Organizado", en *Revista Enfoques: Ciencia Política y Administración Pública*, septiembre, 11 (15).
Sánchez Medero, G. (2011b) "El futuro de la ciberseguridad en Europa: hacia una estrategia de gestión unificada", en *Revista de Seguridad Global*, mayo, 1, 25-37.
Sánchez Medero, G. (2012) "Cibercrimen, cibeterrorismo y ciberguerra: los nuevos desafíos del S. XXI", en *CENIPEC*, enero-diciembre, 31.
Thomas, T. L. (2001). "Las estrategias electrónicas de China", en *Military Review*, julio-agosto, 72-79.
Waston, S. (2007), "Científicos usamericanos quieren desembarazarse de la red de Internet", en *Rebelión*. En http://www.rebelion.org/noticia.php?id=49932 (fecha de consulta: 3/10/2012).