LOS ESTADOS Y LA CIBERGUERRA

Gema Sánchez Medero
Profesora de Ciencias Políticas
en la Universidad Complutense de Madrid

Introducción

Aunque todavía no se ha producido un ataque cibernético de gran impacto, ya son muchos los que se aventuran a pronosticar que la guerra del siglo XXI se librará en el ciberespacio. Eso no significa que la guerra tradicional desaparezca, pero sí, que la ciberguerra irá ganando espacio en los conflictos internacionales. Dada cuenta que como señala John Arquilla es:

> «Una guerra mejor, más barata y menos sangrienta.»

Pero que además puede ser tan efectiva como una guerra convencional. Por ejemplo, imagínese que alguien bloquease virtualmente toda la actividad de Al Qaeda por Internet, pues el grupo terrorista quedaría prácticamente fuera de juego, o si un país dejará a otro sin fluido eléctrico o robase documentos secretos que garantizasen la seguridad de una nación. De ahí que tanto los grupos terroristas como los Estados se estén volcando en el ciberespacio como nuevo campo de batalla, pero no sólo desde el punto de vista ofensivo sino también defensivo.

La nueva guerra fría no se está librando en el espacio, como la anterior, sino que se está librando bajo tierra, a través de los cables de todos nuestros ordenadores. Y ya no son los misiles los que amenazan a nuestros países, sino que son los *bits* de información los que acechan. Estamos ante un nuevo paradigma que está descolocando a todos, incluido las principales potencias mundiales. Ya que paradójicamente, cuanto más avanzado es tecnológicamente un país, más dependencia tendrá de la tecnología, y por tanto, será mucho más vulnerable.

El problema es que aún no se ha valorado el verdadero alcance del problema. Y todavía son muchos los que consideran que un ataque cibernético es algo relacionado con la ciencia ficción, o reservado a las películas de acción. Pero la realidad parece ser otra muy distinta, aunque hasta el momento no se ha producido ninguna acción que haya afectado gravemente a los sistemas o instituciones de algún país.

Aunque no cabe duda que todos podemos ser víctimas en la medida en que realizamos algún tipo de actividad usual, como podría ser adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente, usamos teléfonos con tarjetas electrónicas, utilizamos Internet, etc., y lo que es más grave podemos no saberlo. Por eso, en este artículo nos hemos dedicado a analizar como se están preparando los Estados para una hipotética guerra en el ciberespacio.

La ciberguerra y los conflictos cibernéticos

La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde:

> «La infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc.» (Colle, 2000).

No obstante, para los que consideran que la *cyberwar* y la *netwar* son una misma cosa, hay que puntualizar, la ciberguerra es la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los propios (Sánchez Medero, 2008: p. 15).

En todo caso, si tuviéramos que enumerar las características de una guerra cibernética éstas serían: complejidad, asimetría, objetivos limitados, corta duración, menos daños físicos para los soldados, mayor espacio de combate y menor densidad de tropas, transparencia, lucha intensa por la superioridad de la información, aumenta la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra convencional (Thomas, 2001). Pero tal vez, de todas ellas, la más importante sea la de asimetría, porque la guerra cibernética proporciona los instrumentos necesarios para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos, sólo siendo necesario un ordenador y unos avanzados conocimientos informáticos. Más, cuando los objetivos de este tipo de guerra son:

1. Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.
2. Interrumpir o romper el flujo de la información.
3. Destruir físicamente la información del adversario.
4. Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.
5. Impedir al adversario acceder y utilizar los sistemas y servicios críticos.
6. Engañar a los adversarios.
7. Lograr acceder a los sistemas del enemigo y robarles información.
8. Proteger sus sistemas y restaurar los sistemas atacados.
9. Responder rápidamente a los ataques o invasiones del adversario.

Por eso es necesario advertir que existen tres clases de ciberguerra:

1. Clase I. *Personal Information Warfare*: área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información.
2. Clase II. *Corporate/Organizacional Level Information*: área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado).

3. Clase III, *Open/Global Scope Information Warfare*: área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; y/o la planificación logística de atentados tradicionales, biológicos o tecnológicos.

Los guerreros del ciberespacio hoy son consultores e ingenieros equipados con arsenales informáticos ajenos a la imagen convencional de los armamentos, y los encargados de combatir a los «villanos» en el escenario bélico virtual llevarán micrófonos y audífonos, computadores portátiles, sensores, etc. Sus procedimientos se asemejan bastante al de los *hackers*, aunque sus fines, casi siempre, son completamente distintos (1). Lo primero que hace cualquier *hacker* es visitar o buscar algunos de los sitios donde hay *scripts* para escanear el sitio al cual se quiere violentar, con el fin de determinar cuál es su arquitectura tecnológica básica. Esos *scripts* (2) indagan en el servidor del sitio para determinar qué sistema operativo usa y que tipo de servidor de software emplean. Luego viene la parte más difícil: encontrar «agujeros» o fallas en la versión específica del *software* de ese este sitio, ya que éste puede proporcionar las «entradas» que nos permitan romper su código. La información sobre las fallas del *software* inmediatamente pasan a ser de conocimiento público dentro de la comunidad *hacker* (3), evidentemente cuando se trata de cibersoldados la información obtenida no se publicita. Así, una vez que un *hacker* encuentra un agujero, penetrar el sistema es sólo una cuestión de persistencia, aunque la enorme mayoría de los intentos terminan en fracaso.

Los Estados se preparan la ciberguerra

En un mundo tan hiperconectado e hiperinformatizado como el actual, cualquier impacto en el corazón de los *networks* de la información y la tecnología podría generar pérdidas millonarias a cualquier país o institución, por no hablar de las fuertes consecuencias psicológicas que podría ocasionar un ataque de estas características (Sánchez Medero, 2009). Más aún si tenemos en consideración que las amenazas pueden proceder de cualquier lugar o persona, siendo relativamente baratas, difíciles de contrabandear, complicadas de asociar, etc. Ya no se trata de *hackers* que de forma deportiva tratan de descubrir los fallos en los sistemas de seguridad, o de *crackers* que con una mentalidad nihilista parecen disfrutar de la destrucción, sino de acciones dirigidas a paralizar las capacidades militares o los servicios públicos de un gobierno enemigo (Sánchez Medero, 2009). Por eso, ya son muchos los Estados, sobre todo los más desarrollados, los que han puesto en marcha programas para encontrar, y si es necesario atacar, los puntos débiles de los sistemas informáticos de sus adversarios, al mismo tiempo que

(1) La comunidad *hacker* se ha declarado más de una vez contraria a la ciberguerra, basándose en una declaración conjunta hecha por conocidos grupos norteamericanos y europeos, a finales del año 1998, donde negaron querer convertirse en «facciones paramilitares» y aseguraron que no serán ellos los que ayuden a Estados Unidos a justificar, con casos reales, los fondos asignados a la infoguerra.

(2) Los *scripts* son ficheros de comandos, que permiten agrupar órdenes que se dan a través del teclado. Los *scripts* son ampliamente utilizados en Internet y en programación atomizada de tareas.

(3) Hay sitios como *Roothell.com* que publica esa información. También hay grupos de noticias o canales de *chat* especializados donde se comparten esos conocimientos.

han aprobado medidas para proteger su ciberespacio y minimizar los efectos y daños de los ataques cibernéticos. Por ello, han creado oficinas gubernamentales, sistemas de control, o ejércitos de cibersoldados.

Oficinas gubernamentales

Cada vez son más los países que se han dotado de algún tipo de organismo u oficina con responsabilidad sobre la seguridad cibernética de la nación. Son tantos, que a lo largo de este apartado sólo vamos a especificar algún caso. En Estados Unidos, por ejemplo, se creó la CIAO *(Critical Infrastructure Assurance Office)* y NIPC *(National Infrastructure Protection Center)* para salvaguardar de los ataques cibernéticos las redes de infraestructuras y los sistemas del país; en Argentina, es la Oficina de Coordinación de Emergencias en Redes Teleinformáticas la unidad que tiene competencia en todo lo relacionado con la seguridad de los sistemas de información; en China, el Ejército de Liberación Popular ha constituido el Centro de Guerra de la Información para que dirija las acciones en relación a la ciberguerra; en Japón el Gobierno ha establecido un equipo antiterrorista compuesto por unos 30 especialistas informáticos y un responsable de la Oficina de Seguridad del Gobierno, en España es el Centro Criptológico Nacional adscrito al Centro Nacional de Inteligencia, y dentro de él, el CERT *(Computer Emergency Response Team)*, el responsable de velar por la seguridad cibernética de la nación. Su misión es estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta a las víctimas de ataques informáticos, publicar las alertas relativas a amenazas y vulnerabilidades, y ofrecer información que ayude a mejorar la seguridad de estos sistemas. Servicios que se ven completados con otros de carácter preventivo y de gestión de la seguridad.

Por tanto, su función es alertar y ayudar a las administraciones a responder de forma rápida y eficiente a los incidentes que afecten a sus sistemas de información, al mismo tiempo que apoya al Centro Nacional de Protección de Infraestructuras Críticas en la defensa de las infraestructuras vitales y los sistemas de información clasificada del país. Incluso la Organización del Tratado del Atlántico Norte (OTAN) ha creado en Tallin (Estonia) el Centro de Excelencia para la Cooperación en Ciberdefensa, cuyo objetivo es estudiar ciberataques y determinar las circunstancias en las que deben activar el principio de defensa mutua de la Alianza Atlántica. En la actualidad forman parte de él: España, Italia, Alemania, Eslovaquia, Estonia y Letonia, y se espera que otros países de la OTAN se unan a la iniciativa. Su misión será, según se manifiesta en su memorándum fundacional, proteger los Estados de los ciberataques, entrenar a militares, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad.

Sistemas de control

Existen diferentes sistemas de control, y tal vez lo más conocidos sean: Echelon, Enfopol, Carnivore y Dark Web. El primero, el Echelon o la «Gran oreja», es un sistema automatizado de intercepción global de trasmisiones operado por los Servicios de Inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Su objetivo inicial era controlar las comunicaciones militares y diplomáticas

de la Unión Soviética y sus aliados durante la guerra fría. Aunque en la actualidad se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar tramas terroristas y planes de narcotráfico, inteligencia política y diplomática. Su funcionamiento básico consiste en situar innumerables estaciones de intercepción electrónica en satélites y en otros puntos para capturar las comunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Después cada estación selecciona, mediante la aplicación de unas palabras claves, toda aquella información que guarda relación con el fin que persigue el sistema Echelon. Además, cada uno de los cinco países que componen el sistema facilitan a los demás «diccionarios de palabras claves» para que los incorporen como «filtros automáticos» a los aparatos de intercepción de las comunicaciones. Lógicamente estas «palabras claves» y «diccionarios» varían con el tiempo y de acuerdo con los intereses particulares de los países integrantes del sistema.

La idea de este proyecto es detectar determinadas palabras consideradas «peligrosas» para la Seguridad Nacional de Estados Unidos o de los países participantes en el proyecto. Tal es así, que se estima que cada media hora se interceptan cerca de 1.000 millones de mensajes que luego son filtrados mediante diversos parámetros de búsqueda para extraer los datos de interés para cada país. 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 Estados Unidos 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. Pero pese a todo, el sistema está atravesando serios problemas por el exceso de información. Hasta tal punto, que todo indica que en la actualidad, relativamente pocos son los mensajes y las llamadas telefónicas que se trascriben y registran. La mayoría son eliminados después de ser leídos por el sistema (Pachón Ovalle, 2004).

En todo caso si hoy conocemos 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 el año 1995 (Pachón Ovalle, 2004: p. 5); o la intercepción de las comunicaciones entre el Gobierno de Indonesia y representantes de la empresa japonesa NEC en relación a 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: p. 5); o la intercepción 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).

El segundo, el Enfopol (4) 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 y otros países. Así, Enfopol intenta imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tenga acceso total a las comunicaciones de sus clientes, así como a la información sobre los números marcados y los números desde los que se llama. En el caso de Internet:

> «Los proveedores deben facilitar "una puerta de atrás" para que puedan penetrar a sus anchas por los sistemas privados. Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas). 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.

El Carnivore (5) es la tercera generación de los sistemas de espionaje de redes de la Oficina Federal de Investigación (FBI) (6). Un sistema que ha sido diseñado por el FBI para capturar aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la Agencia. Se especula incluso que sea capaz de espiar el disco duro del usuario que se considere sospechoso y, todo ello, sin dejar rastro de su actividad. Para ello, se coloca un *chip* en los equipos de los proveedores de servicios de Internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos, así cuando encuentra una palabra clave, eso sí con el visto bueno de la corte, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hacen a sitios de la red y las sesiones de chat en las que participa. Esto junto con el control de las direcciones de protocolo de Internet y de los teléfonos de conexión, permite la detección de lo que consideran «movimientos sospechosos» en la red (Busón Buesa, 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

---

(4) El programa fue acordado, el 17 de enero de 1995, mediante un «procedimiento escrito» consistente en notas de télex entre los ministros comunitarios de la Unión Europea. No hubo debate público sobre el mismo, ni siquiera se realizaron consultas a los parlamentarios nacionales ni europeo. Es más, la resolución no fue publicada oficialmente en el *Diario Oficial* de las Comunidades Europeas hasta el 4 de noviembre de 1996, y no fue aprobada por el Parlamento Europeo hasta el 7 de mayo de 1999, justo un año después de que la revista *Telepolis* destapara el asunto.

(5) Después el FBI modificó el monbre, denominándolo «DCS1000».

(6) El primero fue Etherpeek, actualmente un programa comercial. El segundo, Omnivore, fue usado entre los años 1997 y 1999. Y el tercero, el Dragon Ware estaba compuesto por otros tres: Carnivore, que capturaba la información; Packeteer, que convertía los paquetes interceptados en textos coherentes, y Coolminer, que los analizabas.

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.

En esta misma línea está el Programa Dark Web, pero en este caso se centra principalmente en las actividades terroristas. Este proyecto desarrollado por el Laboratorio de Inteligencia Artificial de la Universidad de Arizona utilizan técnicas como el uso de «arañas» y análisis de enlaces, contenidos, autoría, opiniones y multimedia para poder encontrar, catalogar y analizar actividades de extremistas en la red. Una de sus herramientas es el *Writeprint*, que extrae automáticamente miles de características multilingües, estructurales y semánticas para determinar quién está creando contenido «anónimos» *on-line*. Hasta el punto que puede examinar un comentario colocado en un foro de Internet y compararlo con escritos encontrados en cualquier otro lugar de la red y, además, analizando esas características, puede determinar con más del 95% de precisión si el autor ha producido otros en el pasado. Por tanto, el sistema puede alertar a los analistas cuando el mismo autor produce nuevos contenidos, así como el lugar donde están siendo copiado, enlazado o discutido. Pero el Dark Web también utiliza un complejo *software* de seguimiento de páginas, para lo que emplea los *spiders* de los hilos de discusión de búsqueda y otros contenidos con el objetivo de encontrar las esquinas de Internet, en los que las actividades terroristas se están llevando a cabo.

Pero éstos 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 será necesario medios humanos para cotejar esa información que se genera. Sintel es otro sistema integrado de intercepción 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.

El Congreso de Estados Unidos creó el FISC *(Foreign Intelligence Surveillance Court)* como una corte *top-secret* para enterarse de las aplicaciones de vigilancia electrónica que realizaba el FBI y la Agencia Nacional de Seguridad (NSA), y para chequear las actividades domésticas de estas agencias, con el único fin de velar por los derechos constitucionales del pueblo americano (Pachón Ovalle, 2004: p. 16). Y así, podríamos continuar enumerando los distintos sistemas de control existentes, lo que nos indica lo generalizado de está práctica.

Ejércitos de cibersoldados

Sin lugar a dudas, se debe estar desarrollando sofisticadas herramientas informáticas capaces de desmantelar las defensas enemigas, de sembrar el caos en las comunicacio-

nes o de falsificar los datos sobre las posiciones de las tropas (Sánchez Medero, 2009). Por este motivo, un gran número de Estados están creando ejércitos de cibersoldados que puedan hacer frente a esta nueva amenaza y lanzar la suya propia. En Estados Unidos ha reunido un grupo de *hackers* de élite que se estaría preparado para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como JFCCNW *(Joint Functional Component Command for Network Warfare)*, una unidad que se cree que está integrada por personal de la Agencia Central de Inteligencia (CIA), la ANS, el FBI, las cuatro ramas militares, algunos civiles expertos y representantes militares de naciones aliadas, y que tiene la responsabilidad total de defender la red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información y dañar las comunicaciones rivales hasta inutilizarlas. Un comando que tiene como contraparte en el Grupo Especial de Tareas para la Libertad de la Internet Global, GIFTF *(Global Internet Freedom Task Force*, EN sus siglas en inglés), una organización multiagencias (7) subordinada al Departamento de Estado. En Alemania, la Unidad Estratégica de Reconocimiento del Ejército alemán se ha desplegado para coordinar un equipo de soldados que estén involucrados en el ensayo de nuevos métodos de infiltración, manipulación y explotación –e incluso la destrucción– de las redes informáticas.

Por ello, este equipo está aprendiendo a instalar *software* maliciosos en ordenadores sin el conocimiento de los usuarios, robar contraseñas y datos confidenciales, etc. En España, el Ejército de Ciberdefensa (ECD09) de las Fuerzas Armadas españolas está compuesto por militares especialistas en telecomunicaciones e informática, que han hecho cursos avanzados, militares y civiles, en seguridad de las tecnologías de la información y comunicaciones, así como ingenieros superiores civiles de Ingeniería de Sistemas para la Defensa de España S. A., especializados también en seguridad. Su entrenamiento consiste en asaltar los ordenadores enemigos, mientras que defienden los propios, dentro de una red creada expresamente para ello.

Pero tal vez el ejemplo por antonomasia sea China y su Ejército cibernético de reservistas. En el pasado, el papel previsto para las fuerzas de reserva era el de apoyar al Ejército de Liberación Popular (ELN) en la defensa contra cualquier intervención extranjera. En cambio, hoy en día tienen la capacidad para emplear armas electrónicas y de información para alcanzar a un adversario en otro continente (Thomas, 2001). Por ello, entre sus funciones se encuentran: interrumpir el sistema de información, sabotear la estructura para la conducción de operaciones, debilitar la capacidad para contrarrestar una ofensiva, dispersar las fuerzas, armas y fuego del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuego de las unidades propias, confundir al contrario y lanzar simultáneamente una ataque sorpresivo de información para que tome una decisión errónea o bien realizar una acción equivoca (Thomas, 2001: p. 76). Además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares y ha creado escuelas que se especializan en la guerra informática. También está contratando a graduados en informática para desarrollar sus capacidades en la guerra información y, así, crear un ejército de *hackers* civiles. Todo, tal vez porque los chinos se han dando cuenta

(7) Participan agencias del Gobierno, universidades e investigadores privados que «se mantienen operativos las 24 horas del día».

que, de momento, no pueden ganar a Estados Unidos en un guerra convencional y, por tanto, están buscando nuevos campos de batalla donde puedan ser superiores, como en el ciberespacio (Brookes, 2007).

Ataques cibernéticos que no ciberguerra

Hoy en día todavía no ha habido ningún ataque que nos permita hablar de ciberguerra propiamente dicha (8), ya que no se ha registrado ninguno que haya afectado a las instalaciones u organismos públicos, centrales nucleares, sistemas de transporte, infraestructuras nacionales, etc., de algún país causando daños y pérdidas incalculables. Es cierto, que diariamente se producen ataques a sistemas operativos de diferentes órganos o instituciones, pero se tratan más bien de acciones de *hackers*, que tienden normalmente a interrumpir servicios no esenciales, ocasionar algún desperfecto en los sistemas operativos de empresas, organismos, etc., o robar algún tipo de información secreta (Sánchez Medero, 2008: p. 15). Pero sin generar los efectos que se atribuyen a cualquier tipo de guerra, como se puede comprobar en los siguientes ejemplos que a continuación presentamos sobre algunos de los miles de ataques cibernéticos que se han producido en los últimos años:

Década de los años 1980

La NSA intercepta mensajes encriptados de Libia, Irán y de decenas de países, gracias a sus tratos con la empresa Suiza Crypto AG, que vende programas de criptología con puertas traseras sólo conocidas por la Agencia norteamericana. La NSA pone en marcha la red Echelon (con precursoras conocidas desde el año 1952), destinada a espiar las comunicaciones telefónicas, por satélite e Internet.

En plena guerra fría, cinco *hackers* alemanes robaron información de sitios militares norteamericanos y franceses y la vendieron al Comité de Seguridad del Estado (KGB). Un grupo terrorista conocido como *Middle Core Faction* atacó el sistema que controlaba los ferrocarriles de alta velocidad japoneses. Para ello, en primer lugar, cortaron el suministro eléctrico y los cables de control informatizados del ferrocarril, y posteriormente, interceptaron y perturbaron las radiocomunicaciones de la Policía para anticipar y ralentizar la capacidad de respuesta de las autoridades. Aunque nadie resultó herido con la acción, ésta afectó a 6,5 millones de usuarios del ferrocarril japonés y le costó a la compañía aproximadamente seis millones de dólares.

Década de los años 1990

Guerra del Golfo es considerada tradicionalmente como el inicio de la era de la infoguerra. En ella, aviones armados con municiones de precisión atacaron la red de telecomunicaciones y energía eléctrica de Bagdad, con especial saña contra los centros

(8) James Lewis, director del Programa de Tecnología del Centro de Estudios Estratégicos e Internacionales, no cree que hayamos asistido a una ciberguerra por el momento, aunque piensa que el riesgo de un conflicto de estas carcterísticas es cada vez mayor. En Informe sobre Criminalogía Virtual. La Era de la Ciberguerra, Casi una Realidad*,* McAfee, 2009.

informáticos de la policía secreta iraquí. Además, según el Pentágono, un grupo de *hackers* holandeses se ofreció a Sadam para romper el sistema militar norteamericano en Oriente Medio.

Según los medios de comunicación, alguien penetró en los servidores militares estadounidenses y alteró los archivos médicos de los soldados. Entre otras cosas, cambiaron los tipos de sangre, información crucial para una transfusión durante una batalla.

El grupo guerrillero tamil, *Liberation Tigers*, fue el primer grupo terrorista en atacar, a través de Internet, objetivos estadounidenses lanzandoun «mailbombing» contra ordenadores gubernamentales

La Whale and Dolphin Conservation Society, una organización británica para la preservación de los mamíferos marinos, detectó intentos de entrada en sus ordenadores provenientes de la Marina de Estados Unidos. El objetivo era robar un informe sobre delfines adiestrados para fines militares en el mar Negro

El grupo *Masters of Downloading* aseguraba haber robado programas militares para submarinos, satélites del sistema de posicionamiento *globaly* redes informáticas del Pentágono. El presunto terrorista Khalid Ibrahim, del grupo separatista indio *Harkat-ul-Ansar*, intentó contactar con uno de ellos por la conversación transmitida por Internet para cobrar una recompensa a cambio de algunos programas.

Guerra Serbia-Croacia en la red. El grupo de *hackers* serbios *Black Hand* atacó el Centro de Informática de Kosovo, universidades y la versión en línea del periódico *Vjesnik*. La respuesta croatafue entrar en el sitio *web* de la Biblioteca Serbia. La reacción del *Black* Hand fue robar el fichero de contraseñas del Rudjer Boskovic Institute, incluso se rumoreo que consiguieron entrar en el proveedor de acceso más importante de Croacia. Por el contrario, los *hackers* croatas se introdujeron en dos servidores serbios.

La guerra de Kosovo también se produjo en la Red. *Hackers* rusos, yugoslavos, norteamericanos, llenaron páginas de *graffitis* a favor y en contra de Milosevic o la OTAN. La red se utilizó para poner en contacto a los de dentro y los de fuera del territorio. Nacieron nuevos foros de discusión, la información de la guerra volaron por las listas, discutiéndose en ellos todos los sucesos acontecidos. La red se llenó de propaganda.

Década de los años 2000

La ciudad de Nueva York quedó sumida en el caos como consecuencia del mayor apagón en la historia de Estados Unidos, que afectó a casi toda la región noreste del país además de Canadá.

Un apagón de 34 minutos en el sur de Londres trastornó la red del metro de la ciudad y el sistema de trenes en el sur de Inglaterra, afectando a medio millón de personas y la mayoría de los servicios en el centro de la capital británica. El 60% de las estaciones del metro tuvo que cerrar, sobretodo en el sur de la ciudad. La Policía dijo que alrededor de 270 semáforos se apagaron, y aunque esta falla se remedió con rapidez, no dejó de añadir su dosis de estrés en las calles afectadas.

Guerra de Gaza. En el portal de *Youtube* el Ejército israelí colgó vídeos en los que se insistía que Hamás era una organización terrorista que usaba a los civiles como «escudos humanos» y a las mezquitas para esconder armas. Su vídeo más visto fue, con más de 600.000 visitas, un ataque israelí contra un centro de almacén de misiles palestinos «destinados a civiles inocentes». Los palestinos contraatacaron subiendo al portal *PalTube* vídeos donde se denunciaba la «masacre» que estaba cometiendo el Ejército israelí en Gaza.

En Estonia las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reformas quedaron paralizadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques distribuidos de denegación de servicio. Hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallín de un monumento de la época soviética. De ahí que Estonia acusará al gobierno ruso de estar detrás de estos ataques, aunque el Kremlin siempre negó su implicación en el asunto.

Una red informática del Pentágono sufrió un ataque lanzado por *hackers* desde China que se convirtió en «uno de los ciberataques de más éxito» al Departamento de Defensa de Estados Unidos. Aunque es cuestionable la cantidad de información confidencial que se robó, el incidente aumentó el nivel de preocupación, al poner de relieve cómo se podían interrumpir sistemas en momentos críticos.

El prestigioso semanario alemán *Der Spiegel* indicó que se pensaba que China había atacado sistemas informáticos de la Cancillería alemana, así como sistemas de tres ministerios, e infectaron las redes con programas espía. Los supuestos ataques se dirigieron a los ordenadores de la Cancillería y de los Ministerios de Asuntos Exteriores, Economía e Investigación.

En la India, el Centro Nacional de Informática sufrió ataques desde conexiones telefónicas a Internet en China. Destacados miembros del Servicio de Inteligencia afirmaron que los *hackers* accedieron a las cuentas de correo electrónico de 200 ministros, burócratas y funcionarios de defensa, y continuaron atacando servidores indios al ritmo de tres o cuatro al día. China ha negado todas las acusaciones de estar detrás de los ataques.

Asia Pacific News informó que unos *hackers* chinos habían intentado supuestamente acceder a las redes informáticas estatales de alto secreto de Australia y Nueva Zelanda, como parte de una operación internacional más amplia para conocer secretos militares de países occidentales.

Google denunció el 12 de enero de 2010 que había sido blanco de ciberataques, probablemente procedentes de China, para acceder a la correspondencia de disidentes y robarle a la empresa códigos y secretos comerciales.

Un experto en informática *hacker* temporalmente el sitio de microblogs *Twitter.com*, redireccionando a los usuarios a una página en Internet y señalando que representaba un grupo que se hace llamar Ejército Cibernético de Irán.

Por tanto, se puede decir que hasta el momento se está haciendo un uso pasivo de la red que se limita en la mayoría de los casos al espionaje, a dañar sistemas de comunicación, generar confusión y desinformación, bloquear páginas *web*, es decir, pequeñas acciones si las comparamos con las acciones que podría generar una verdadera guerra cibernética. Incluso el último ataque a las instalaciones nucleares de Irán no puede ser considerado, por lo menos de momento, como el inicio de una ciberguerra. Es cierto, que *Stuxnet*, ha sido el primer gusano informático que ha atacado a una planta industrial, llegado a afectar al menos a unos 30.000 ordenadores. Pero cuidado, esta acción ha supuesto el primer movimiento contra una instalación nuclear, a partir de ahora la cosa podría ir a más.

Medidas de prevención a ciberataques

No hay mejor medida para evitar un ciberataque que apagar el ordenador. Pero dado que hoy en día eso parece algo imposible se están activando otras acciones que puede ayudar a contribuir a frenar este tipo de ataques y sus consecuencias. Medidas tales, 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 que existe 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).

Otra es identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto sólo se puede conseguir con la ciberinteligencia (9). 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 puede 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 algu-

(9) El fin prioritario de la *ciberinteligencia* es el cúmulo de la información necesaria para entender el funcionamiento actual y futuro de la red, lo que lleva a que la inteligencia debe crecer continuamente con la misma velocidad que el desarrollo de las nuevas tecnologías, debe transformase con ella para mantener la capacidad de indentificar las amenazas y las contraamenazas, vulnerabilidades y respuestas frente a éstas, así como los factores descadenantes de las distintas actuaciones maliciosas (Ruiliba, 2006: p. 53).

nos países. Y otra, como algunos investigadores considera, es crear una segunda red extraordinariamente controlada y separada del Internet comercial (Waston, 2007).

Bibliografía

Añover, Julián: «Echelon y Enfopol nos espían», *Internacional,* el 16 de noviembre de 2001, en: *http://www.nodo50.org/altavoz/echelon.htm*

Brookes, Peter: «Contrarrestando el arte de la guerra informática», *Grupo de Estudios Estratégicos,* número 2.011, octubre de 2007, en: h*ttp://www.gees.org/articulo/4637/*

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

Colle, Raymond: «Internet: un cuerpo enfermo y un campo de batalla», *Revista Latina de Comunicación Social,* número 30, junio de 2000, en: *http://www.ull.es/publicaciones/latina/aa2-000qjn/91colle.htm*

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

Puime Maroto, Juan: «El ciberespionaje y la ciberseguridad», en «La violencia del siglo XXI. Nuevas dimensiones de la guerra», *Monografías* del CESEDEN, número 112, pp. 42-70, octubre, de 2009.

Rodríguez Pérez, Carlos: *Tecnologías de vigilancia e investigación: El caso Echelon. Informe: Tecnologías de vigilancia e investigación,* posgrado conocimiento, ciencia y ciudadanía en la sociedad de la información. Universitat de Barcelona, 2008, en: *http://www.ub.es/prometheus21/articulos/obsprometheus/crodr_echelon.pdf*

Ruiloba Castilla, Juan Carlos: «La actuación policial frente a los déficit de seguridad de Internet», *Revista de Internet, Derecho y Política,* número 2, pp. 52-62, 2006.

Sánchez Medero, Gema: «Ciberterrorismo: la guerra del siglo XXI», *El Viejo Topo,* número 242, pp. 15-24, marzo de 2008.

— «Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica», Amérigo Cuervo-Argango, F. y Peñaranda Algar, J. de (comp.): *Dos décadas de posguerra fría. Actas de I Jornadas de Estudios de Seguridad,* Instituto Universitario «General Gutiérrez Mellado»-Universidad Nacional de Educación a Distancia, pp. 215-241, Madrid, 2009.

— «Las dos nuevas perspectivas del siglo XXI: ciberterrorismo y ciberguerra», *Nómadas Mediterranean Perspectives,* número 1, pp. 683-700, marzo de 2009.

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

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