3. Ciberguerra y Ciberterrorismo

*Gema Sánchez Medero**

3.1 Introducción

Hoy en día, el uso de la red se ha generalizado, hasta tal punto, que Internet conecta en la actualidad a millones de redes, incluidas aquellas que hacen funcionar las infraestructuras vitales y los servicios sociales. 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, entre otros. Pero ¿qué sucedería si se produjese un ciberataque sobre cualquiera de estas infraestructuras o servicios? Téngase en cuenta que diariamente se producen ataques a sistemas operativos de diferentes órganos o instituciones, que tienden normalmente a interrumpir servicios no esenciales u ocasionar algún desperfecto en los sistemas operativos de empresas, organismos, etc. Aunque también es cierto, que el único gran ataque cibernético a escala mundial que ha habido hasta el momento es el del virus WannaCry. Pero solo este ha supuesto ya un gran impacto en el corazón de los *networks* de información y tecnología que ha generado pérdidas millonarias.

* Profesora de Ciencias Políticas y de la Adminstración de la Universidad Complutense de Madrid.

Actualmente, vivimos en un mundo digital hiperconectado e hiperinformatizado, donde las amenazas pueden proceder de cualquier lugar o persona, siendo relativamente baratas, fáciles de contrabandear, virtualmente indetectables y complicadas de asociar. Además, la vulnerabilidad de las redes está haciendo que no solo los terroristas, sino también los gobiernos empiecen a tomarse muy en serio la posibilidad de lo que se ha denominado *"ciberguerra"*. Hasta el punto que unos 120 países están desarrollando modos de utilizar Internet como un arma para atacar a los mercados financieros, los sistemas informáticos gubernamentales y las empresas de sus potenciales enemigos. Situación que puede desencadenar en las próximas décadas, como sostiene el informe anual de la compañía de seguridad McAfee, en una *"guerra fría cibernética"* dominada por los *"ciberespías"* y los *"cibersoldados"*.

No obstante, todavía son muchos los que consideran que este tipo de prácticas se enmarcan dentro de la ciencia ficción, y se preguntan ¿cómo podría afectarnos un ataque ciberterrorista o la ciberguerra? Sin ánimo de ser alarmista habría que plantearse qué sucedería si 4B/Mastercard/Servired fueran atacadas, cuando nuestros pagos con tarjeta fueran imposibles; si el centro de control de Metro sufriera un ataque; si los periódicos online, cadenas de TV y radio, así como las agencias de noticias, se hicieran eco de una noticia falsa; si se accediera ilegalmente al tablero de control de una presa hidroeléctrica, realizando una apertura descontrolada de sus compuertas, generando así una inundación en una región; si se hiciera un *blinds* de radar, generando un bloqueo de tráfico aéreo por 12 horas, etc. Además, sabiendo que los sistemas militares de ataque y de defensa, los de información públicos y muchos otros de control de sistemas de sanidad, energía y servicios públicos, etc. dependen casi en su totalidad de la informática, podemos decir sin ánimo a equivocarnos que un ciberataque bien organizado puede ocasionar grandes perjuicios a la población de cualquier Estado. Por tanto, no nos encontramos tan lejos del ciberterrorismo y la ciberguerra como algunos piensan (Sánchez, 2009a).

3.2 La ciberguerra y el ciberterrorismo

> 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 se ha 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" (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 propios (Sánchez, 2008[a], p. 15).

En todo caso, si se tuvieran 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, ya que sólo es 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 enemigo 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; 8) 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), y 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 (Sánchez, 2010c).

Los guerreros del ciberespacio hoy son consultores e ingenieros que equipados con arsenales informáticos ajenos a la imagen convencional de los armamentos son los encargados de combatir a los "villanos" en el escenario bélico virtual. Sus procedimientos se asemejan bastante al de los hackers, aunque sus fines, casi siempre, son completamente distintos, dado que la comunidad se ha declarado en más de una ocasión contraria a la ciberguerra. Como en la declaración conjunta hecha por conocidos grupos norteamericanos y europeos, a finales de 1998, donde negaron querer convertirse en "facciones paramilitares" y aseguraron que no serían ellos los que ayúdese a los EE.UU a justificar, con casos reales, los fondos asignados a la infoguerra (Sánchez, 2010c).

En cualquier caso, lo primero que hace cualquier hacker es visitar o buscar algunos de los sitios donde hay *scripts* (son ficheros de comandos, que permiten agrupar órdenes que se dan a través del teclado) para escanear el sitio al cual se quiere violentar, con el fin de determinar cuál es su arquitectura tecnológica básica. Esos *scripts* 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 sitio, ya que éste puede proporcionar las "entradas" que permitan romper su código. La información sobre las fallas del software inmediatamente pasan a ser de

conocimiento público dentro de la comunidad hacker, evidentemente cuando se trata de cibersoldados la información obtenida no se publicita. Así, una vez que un hacker encuentra un agujero, penetrar en el sistema es sólo una cuestión de persistencia, aunque la mayoría de los intentos terminen en fracaso (Sánchez, 2010c).

El ciberterrorismo es la convergencia del ciberespacio y el terrorismo (Orta Martínez, 2005). No obstante, no existe acuerdo entre la doctrina acerca de una definición única. Muchos se centran en la noción del elemento cibernético, y otros dan especial relevancia al elemento de terror (González Amado, 2007, p. 28). Por ejemplo, el Centro de Protección de la Infraestructura Nacional nos indica que el ciberterrorismo es "un acto criminal perpetrado a través de computadores que resulta en violencia, muerte o/y destrucción y crea terror con el propósito de coaccionar a un gobierno a cambiar sus políticas" (González Amado, 2007, p. 30). Para Dan Verton (2004, p. 32) "el ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo terrorista extranjero subnacional con uno objetivo político y que utilizan la tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de un nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos". Para Jeffrey F. Addicott (2004, p. 32) el ciberterrorismo es "el empleo de varios recursos de computación para intimidar o coaccionar a otro para alcanzar objetivos específicos".

En todo caso, los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en la categoría ciberterrorismo. Dentro de este concepto, se puede hablar de tres niveles de capacidad *cyberterror*, tal como se define en la Escuela de Postgrado Naval de Monterey, Ca:Monterey: 1) 1.Simple-Unstructured: the capability to conduct basic hacks against individual systems usSimple-no estructurado: la capacidad de realizar cortes de base contra los sistemas individuales usando tools created by someone else.herramientas creadas por otra persona; 2) 2.Advanced-Structured: the capability to conduct more sophisticated attacks against multAvanzado-estructuradas: la capacidad para llevar a cabo sofisticados ataques contra múltiples systems

and possibly to modify or create basic tools.sistemas y, posiblemente, para modificar o crear herramientas básicas; y 3) 3.Complejo Coordinado por: la capacidad de ataques coordinados que pueda provocar perturbaciones en masa (Jachowicz, 2003 (Sánchez, 2010c).

De esta manera, el ciberterrorismo representa una alternativa para los terroristas contemporáneos por varios motivos (Carlini, 2016, p. 6):

- Un ataque cibernético es más barato que un ataque tradicional.
- Anonimato y la posibilidad de atacar desde cualquier punto del planeta.
- Un elevado número de objetivos gubernamentales, privados, multinacionales, etc.
- Una cobertura mediática muy elevada.
- Un ataque simultáneo en el espacio físico así como en el ciberespacio podría llevar la amenaza terrorista a un nivel mucho más avanzado y difícil de contener.

3.3 La ciberseguridad

El término "ciberseguridad" se define normalmente como la protección de datos, información y sistemas conectados a Internet. No es fácil englobar una materia tan compleja en una definición tan sencilla, pues el concepto extiende el de seguridad clásica a otras nociones más propias del ciberespacio, como integridad, disponibilidad, autenticidad, confidencialidad o la mencionada denegación del servicio. Tal es así, que en un primer momento, la ciberseguridad obedecía a un enfoque de protección de la información (*Information Security*) donde solamente había que proteger la información a los accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas (Fojón y Sanz, 2010: 2). Mientras que ahora, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (*Information Assurance*) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en

los estándares internacionalmente aceptados (Fojón y Sanz, 2010, p. 2). Por tanto, es importante para los Estados disponer de estructuras organizacionales nacionales, regionales e internacionales, para fortalecer su ciberseguridad y luchar contra la ciberdelincuencia. Pero teniendo en cuenta, que existen soluciones pero que pueden ser falibles y posibles de burlar, por tanto, nunca son universales ni definitivas.

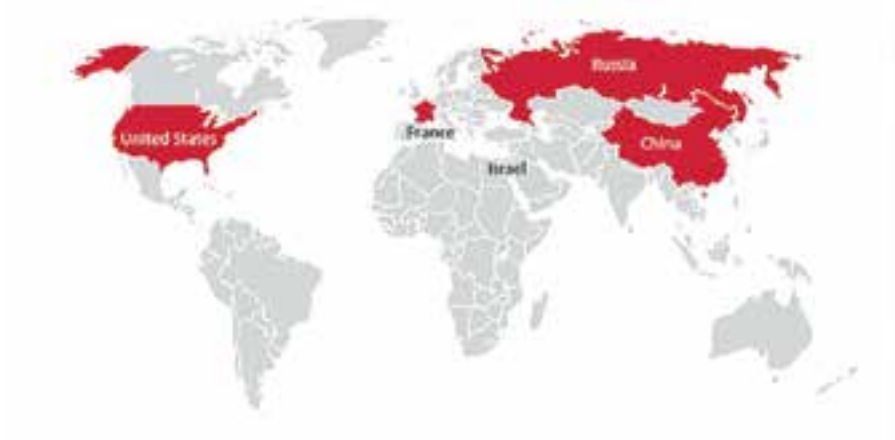
Así, ante el temor de las posibles consecuencias de un hipotético ataque cibernético, países como EE.UU., Francia, el Reino Unido, Israel y Corea del Sur, así como la ONU y la OTAN entre otras organizaciones internacionales, están tomando conciencia de la importancia y la necesidad de un ciberespacio seguro y, por ello, se están desarrollando marcos normativos, planes y estrategias específicas para la defensa del ciberespacio (Fojón y Sanz, 2010: 2), es decir, medidas y acciones dirigidas a:

- Educar, formar y concienciar a todos los agentes de la ciberseguridad;
- Establecer estructuras que puedan funcionar como centro de alerta y de gestión de crisis a nivel nacional;
- Agrupar los medios a implementar para utilizarlos y compartirlos para un conjunto de países o para una región; imponer sistemas de vigilancia y control;
- Desarrollar las competencias de un equipo de ciberpolicía que pueda contribuir a la persecución e investigación de los delitos informáticos en el ámbito de la cooperación internacional;
- Proponer soluciones tecnológicas en lo que se refiere a la gestión de identidades, el control de acceso, la utilización de plataformas materiales y de aplicaciones informáticas seguras, las infraestructuras de respaldo, los protocolos criptográficos y la gestión operacional, etc.

Y todo con el fin de establecer una línea de defensa común y homogénea, mejorar las capacidades de detección y reacción, concienciar y proporcionar apoyo a los ciudadanos para hacer más segura su actividad en línea (on-line), así como reforzar la capacidad de las fuerzas y cuerpos

de seguridad del Estado para combatir el cibercrimen, y fortalecer el entorno futuro de la ciberseguridad (Sánchez, 2012).

Figura 1. Los países que más gastan en ciberdefensa



Fuente: McAfee.

Por otro lado, países como China, Irán, Corea del Norte, Rusia y Pakistán han reconocido su interés estratégico en el ciberespacio como vehículo para alcanzar posiciones de liderazgo económico y político en sus áreas geográficas de influencia, y lo están concretando en la definición de políticas, en la ejecución de grandes inversiones económicas destinadas a recursos TIC y en la formación de recursos humanos, con el objetivo de establecer "una defensa beligerante" de su ciberespacio (Fojón y Sanz, 2010, p. 2). Para ello, se están dedicando a incrementar el número de especialistas en seguridad de las TIC, impulsar y coordinar los esfuerzos de investigación y desarrollo de productos de seguridad y ataque nacionales, y definir estrategias que disuadan la actividad hostil o dañina en el ciberespacio.

En todo caso, el ciberespacio se está convirtiendo en un lugar ideal para la usurpación de la identidad, la burla de los sistemas, la intrusión, el secuestro de recursos, la infección, el deterioro, la destrucción, la manipulación, la violación de la confidencialidad, la denegación del servicio, el robo, la extorsión, etc. Toda una serie de actividades delictivas que llevan a cabo todo tipo de actores, como:

- *Las unidades cibernéticas de las Fuerzas Armadas* (FFAA)*:* En muchas naciones las FFAA disponen de unidades que tienen asignadas misiones de ataque a los sistemas de información de los adversarios (Candau, 2011, 263). En los últimos años se han detectado ciberataques contra objetivos concretos. El ejemplo más conocido es el ataque que sufrió Estonia en 2007, y que supuso el bloque temporal de muchas de las infraestructuras críticas del país báltico.

- *Servicios de inteligencia y contrainteligencia:* Empleados por los Estados para realizar operaciones de información sensible o clasificada manejada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos, incluso para el espionaje industrial (Candau, 2011, p. 263). Por ejemplo, entre los servicios de inteligencia es habitual la intercepción de teléfonos móviles, es más cualquier estudiante de telecomunicaciones con un radio multibanda puede captar las comunicaciones entre teléfonos analógicos, estaciones de policía, radiotaxi y un sinfín de bandas teóricamente privadas.

- *Espionaje industrial***:** Son compañías o gobiernos que tienen interés en disponer de información crítica de desarrollos tecnológicos e industriales de industrias de la competencia (Candau, 2011, p. 263). Por ejemplo, el ataque ha sufrido el G-20, en marzo de 2011. Según reconoció el gobierno francés más de 150 computadoras del Ministerio de Finanzas resultaron afectadas. El objetivo era conseguir documentos relacionados con asuntos económicos internacionales.

- *Crimen Organizado:* Este tipo de organizaciones han comenzado a trasladar sus acciones al ciberespacio, gracias al anonimato que éste les ofrece. De ahí, que empleen el ciberespacio para realizar actividades relacionadas con el robo de información de tarjetas de crédito o de los certificados digitales asociados, con el fraude telemático asociado a operaciones bancarias o a cualquier transacción desde Internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal (Candau, 2011, p. 263).

- *Hacking Político/Patriótico:* Este tipo de actividad recogida abundantemente en prensa es el reflejo de un conflicto regional, étnico, religioso o cultural en el ciberespacio (Candau, 2011, p. 264). Así, son frecuentes los ataques de denegación de servicio entre China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiítas y sunitas, o el conflicto entre árabes e israelíes (Candau, 2011, p. 263). En todo caso, 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* indagan en el servidor del sitio para determinar qué sistema operativo usa y que tipo de servidor de software emplean.

- *Terrorismo:* Los grupos terroristas y extremistas emplean el ciberespacio para planificar sus acciones, publicitarlas, reclutar adeptos, financiarse, entrenarse, buscar información, comunicarse, etc. Por ejemplo, los terroristas están empleando sus webs para solicitar donaciones, pero también para extorsionar a grupos financieros, transferir, lavar y robar dinero, usar el dinero electrónico, etc., como una manera de buscar financiación económica. Pero también utilizan Internet para publicitar sus puntos de vistas y justificar sus actividades, así cuelgan en distintas webs videos de torturas, las súplicas y el asesinato de rehenes como Nicholas Berg, Eugene Armstrong y Jack Hensley. O recabar información de sus objetivos y ofrecer manuales de operativos, así en Internet se puede encontrar "El arte del secuestro", "Manual del terrorista", "La guerra dentro de la ciudades", aunque estos manuales no sustituyen al adiestramiento real si pueden ser de gran utilidad, como sucedido en los atentados de Londres del 7-J, etc.

3.4 Los Estados se preparan para 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, 2009b). 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, 2009a). 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 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 (Sánchez, 2010c)

3.4.1 Las oficinas gubernamentales y organismos internacionales de seguridad cibernética

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. Es más, muchos incluso han llegado a crear todo un entramado organizativo que destina sus esfuerzos a la defensa del ciberespacio. Aunque son tantos, que a lo largo de este apartado sólo vamos a especificar alguno de los casos.

3.4.1.1. Oficinas gubernamentales

En EE.UU., por ejemplo, se creó la "Critical Infrastructure Assurance Office" (CIAO), National Infrastructure Protection Center (NIPC) y el United States-Computer Emergency Readiness Team (US-CERT) para salvaguardar las redes de infraestructuras y los sistemas del país de los ataques cibernéticos, identificar las vulnerabilidades, difundir información sobre alertas de amenazas de seguridad, y coordinar las actividades de respuesta antes de incidentes cibernéticos. Además, en el Departamento de Defensa existen muchas iniciativas tanto de los tres

ejércitos como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas como la Agencia de Seguridad Nacional (NSA). Esta agencia, por ejemplo, tiene un departamento encargado del aseguramiento de la información, NSAIDA, que se centra en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad. Además, el Departamento de Defensa financia el CERT-CC que tiene como misión principal establecer un foro de coordinación entre los CERT nacionales. Asimismo, con la llegada de Obama se reforzó todo este tipo de iniciativas relacionadas con la ciberseguridad. Por ejemplo, elaboró un informe sobre la seguridad cibernética que sirviera para luchar contra los delitos informáticos y el robo de información confidencial, anunció el nombramiento de un responsable de ciberseguridad para que formara parte del Consejo de Seguridad Nacional en la Casa Blanca, y ordenó al Pentágono que prepara la creación de un nuevo mando especializado en la ciberguerra.

Además, después del 11-S Estados Unidos cambió su estrategia de seguridad, centrándola en el establecimiento y reordenación relativos a la seguridad del territorio, el desarrollo de la legislación en cuanto a seguridad nacional y la ciberdefensa, la implantación de planes y estrategias referidos a la seguridad nacional, la creación de un Comando Ciberespacial en la Fuerza Área y la ejecución de ejercicios periódicos en ciberseguridad. Además, se ha apostado por la colaboración con otros Estados, tal es así, que EE.UU. ya está enlazando algunos ordenadores de defensa con los de sus aliados, incluso se ha llegado a acuerdos de intercambio de información, tecnología e inteligencia con sus aliados. Por ejemplo, ha establecido un acuerdo de cooperación en materia de ciberseguridad con Israel o Cuba.

También, durante la Presidencia de Obama se inauguró una nueva agencia de seguridad informática denominada "Integración de Inteligencia contra la Amenaza Cibernética (CTIIC)", que tiene como principal tarea evitar que terceros accedan a información confidencial del Gobierno y detectar a los atacantes. Pero además entre sus funciones se encuentra analizar la información recopilada por otras agencias guber-

namentales, con el fin de detectar amenazas cibernéticas. En este mismo sentido, el Departamento de Defensa elaboró el Plan de Cybersecurity Discipline Implementation, con el fin de reforzar de manera más estricta los requisitos de acceso y reducir el anonimato en sus redes.

Francia ha creado la Autoridad Nacional de Seguridad de los Sistemas de Información (ANSSI), que depende del Ministerio de Seguridad Nacional, para vigilar las redes informáticas gubernamentales y privadas con el objetivo de defenderlas de ataques cibernéticos. Sus funciones son: la detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes, el desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos, el asesoramiento de seguridad a organismos gubernamentales y operadores de infraestructuras críticas, la difusión de información a empresas y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación. Este organismo dependen la Subdirección de Estrategia y Reglamentación, el Centro de Formación y el Centro Operacional de la Seguridad de los Sistemas de Información (COSSI), que son los responsables de la realización de las inspecciones y auditorías de seguridad a sistemas gubernamentales, las misiones de desarrollo de productos de cifra, los ejercicios que evalúen la seguridad, el despliegue de los sistemas de detección, y la coordinación de la respuesta gubernamental. En el COSSI se encuentra además el Centro de Expertos del Gobierno en el Tratamiento de Ataques Informáticos (CERTA), creado en 1999 y que facilitan la aplicación de buenas prácticas y mejora la atención a los usuarios en todo el territorio (Sánchez, 2011).

Además, el Gobierno francés elaboró el Libro Blanco de la Seguridad y Defensa Nacional y la Seguridad Nacional, donde se contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar como son: el conocimiento y la previsión (con la necesidad de mejora de las capacidades técnicas de las Agencias de Inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

El Reino Unido ha decidido crear el Centro de Operaciones de Ciberseguridad, para supervisar la protección de importantes sistemas de tecnológicos de información usados por el gobierno británico y el sector privado y la Oficina de Ciberseguridad, para coordinar las medidas de ciberseguridad de todos los departamentos gubernamentales. EL primero es una entidad multidepartamental con sede en Cheltenham y ligado al "Government Communications Headquarters (GCHQ), desde el que se proporciona protección coordinada a los sistemas de infraestructuras críticas del país. La segunda, coordina las políticas y supervisa el programa de trabajo entre las distintas agencias gubernamentales. Estos dos centros forman parte del Primer Plan Estratégico de Ciberseguridad del Reino Unido, donde también se contempla la creación de un grupo de asesores técnicos, y el establecimiento de las líneas estratégicas de seguridad cibernética del país: reducción del riesgo del uso del Ciberespacio por el Reino Unido actuando sobre la amenaza, las vulnerabilidades y el impacto; aprovechamiento de las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y actué contra los adversarios, y el impulso de una doctrina sobre el ciberespacio.

En Alemania se ha creado la Oficina Federal de Seguridad de la Información (BSI), dependiente del Ministerio Federal de Interior. Las funciones del BSI son la protección de las redes del Gobierno federal, el desarrollo de productos de cifra, el análisis de nuevas tecnologías, la seguridad de los productos *software*, la protección de infraestructuras críticas, y el soporte del CERT para ciudadanos y pequeñas y medianas empresas. Además se ha aprobado un Plan Nacional de Protección de Infraestructuras de la Información del Ministerio de Interior, en el que se establece como objetivos la prevención (las actividades críticas son divulgar información sobre riesgos y posibilidades de protección o empleo de productos y sistemas confiables), la preparación (las actividades son recolectar y analizar la información para proporcionar alertas y avisos) y la reacción (mejorar las capacidades técnicas propias y desarrollar productos con tecnología nacional). Además, a partir de abril de 2011, el Gobierno alemán ha abierto un Centro Nacional de Ciberseguridad (NCA) para defenderse de los ataques cibernéticos externos a sus in-

fraestructuras críticas, y también ha puesto en marcha un "Consejo de Ciberseguridad Nacional", para mejorar la cooperación entre el Estado y los representantes del sector financiero y económico.

En China todas las ciberoperaciones están a cargo del Departamento General de Personal del Ejército Popular de Liberación, que se ha convertido en el departamento más importante del mencionado ejército. Bajo las órdenes de este departamento se encuentran tres departamentos que trabajan en campañas para guerras no convencionales:

- Departamento enfocado en el espionaje e inteligencia (HUMINIT).
- Departamento enfocado en el ciberespionaje y señales de inteligencia (SIGINT).
- Departamento enfocado en la guerra electrónica, interceptación de datos satélites y en inteligencia electrónica (ELINT).

Además, el Departamento General de Personal también supervisa las regiones militares de China, la Armada, la Marina, las Fuerzas Áreas y la Segunda Artillería. Las estimaciones sobre la cantidad de soldados que hay en cada uno de estos departamentos varía, solo algunas apuntan a que el segundo departamento lo componen 130.000 trabajadores, el primer departamento contaría entre 30.000 y 50.000 trabajadores, pero no existe ningún dato sobre el tercer departamento. Sus órdenes provienen de los Planes Quinquenales del Partido Comunista Chino, lo que induce a pensar que normalmente sus objetivos se dirigen a cuestiones industriales y metas económicas.

En España, a lo largo de los últimos años, también se están tomando medidas que contribuyan a incrementar la seguridad del ciberespacio. Se creó en diciembre de 2013 el Departamento de Seguridad Nacional, dando lugar a la primera "Estrategia de Ciberseguridad Nacional", cuyo objetivo es fortalecer las capacidades de prevención, defensa, detección y respuesta a los ciberataques. Asimismo, se ha constituido el Consejo Nacional de Ciberseguridad, que se encarga de asegurar el funcionamiento coordinado y eficaz de la ciberseguridad en España. Entre los organismos de coordinación se hallan: el Mando Conjunto de

Ciberdefensa de las Fuerzas Armadas (creado también en el 2013) y los centros de respuesta anteciberataques del Centro Criptológico Nacional, de Seguridad e Industria, de las comunidades autónomas, así como los de las entidades privadas y otros servicios de seguridad relevantes. En este momento, España cuenta con un Plan Nacional de Ciberseguridad, que fue aprobado el 31 de octubre de 2014 por el Consejo de Seguridad Nacional.

El Centro Criptológico Nacional (CNN), dependiente del Centro Nacional de Inteligencia (CNI) tiene entre sus funciones: elaborar y difundir normas, instrucciones y recomendaciones para garantizar la seguridad de las TIC en la administración; formar el personal de la administración especialista en el campo de la seguridad de las TIC; constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito; valorar y acreditar la capacidad de productos de cifras y Sistemas de las TIC; coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de sistemas antes mencionados; velar por el cumplimiento de la normativa, y establecer las relaciones necesarias con otros actores e instituciones.

A nivel nacional, también existen otros organismos con competencias en la materia:

- La Capacidad de Respuesta ante Incidentes de Seguridad (CCN-CERT) es el centro de alerta nacional que coopera con todas las administraciones públicas para responder rápidamente a los incidentes de seguridad en su parte del ciberespacio.
- El Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio, es el responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las PYMES españolas y los ciudadanos en su ámbito doméstico.
- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), dependiente del Ministerio de Interior, procura la ciberseguridad relacionada con las infraestructuras.

- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio de Interior, son responsables de combatir la delincuencia que se produce en el ciberespacio.
- La Agencia Española de Protección de Datos (AGPD), dependiente del Ministerio de Justicia, hace cumplir la normativa en materia de protección de datos personales, y
- El Centro de Ciberseguridad Industrial, que trata de mejorar la seguridad cibernética industrial en España y Latinoamérica.

A nivel autonómico, existen centros homólogos a los referidos a nivel nacional, que igualmente tienen obligaciones en la gestión de la ciberseguridad en su ámbito territorial. Además, a nivel internacional, España forma parte de las organizaciones que promueven la defensa del ciberespacio, como el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN y en organismos como ENISA, Antiphising Working Group (AWG) y Data Protection Working Party.

3.4.1.2 Organismos internacionales de ciberseguridad

La Unión Europea ha creado la Agencia Europea de Seguridad de las Redes y la Información (ENISA), con sede en Heraklion (Grecia), para ayudar a los Estados miembros a obtener unos niveles altos de seguridad, asesorar técnicamente y prestar asistencia a los Estados miembros, así como a las instituciones de la UE sobre las cuestiones vinculadas a la seguridad de las redes y de la información, y fomentar la cooperación entre el sector público y privado. Así, para garantizar estos objetivos, las tareas de la Agencia consisten principalmente en: acopio y análisis de datos relativos a aspectos vinculados a la seguridad y a los riesgos emergentes; cooperación con los distintos protagonistas, creando asociaciones entre el sector público y el privado con empresas que ejercen sus actividades en la UE o a nivel mundial; sensibilizar a los usuarios en la problemática de la seguridad de las redes y de la información, y promover métodos de evaluación de riesgos y mejores prácticas con el fin de encontrar soluciones interoperativas de gestión de los riesgos; el

seguimiento del desarrollo de las normas sobre productos y servicios en la sociedad de la información y en las redes; asistir a la Comisión y a los países de la Unión en el diálogo que mantienen con las empresas para gestionar los problemas de seguridad; y presentar sugerencias.

Su estructura gira en torno al Consejo de Administración, el Director Ejecutivo y el grupo permanente. La primera está compuesta por representantes de los Estados miembros y de la Comisión, así como de las empresas y expertos universitarios en la materia, y consumidores sin derecho al voto. A través de esta institución, los Estados miembros pueden formular sus necesidades en relación con esta materia. El segundo es nombrado por el Consejo de Administración a partir de una lista de candidatos propuestos por la Comisión. El tercero lo forman las partes interesadas, y es creado por el Director Ejecutivo y está compuesto por representantes de las empresas, los consumidores y expertos universitarios. Así, viendo esta organización se podría concluir que ENISA es un centro neurálgico para fomentar el intercambio de información y cooperación entre todas las partes interesadas (organismos de la UE, miembros de la UE Estados, la industria, el mundo académico y las organizaciones de consumidores de interés) en el campo de la seguridad en el ciberespacio. Además, en diciembre de 2002 la Unión Europea aprobó la Estrategia Europea de Seguridad (EES), pero fue en su revisión, en diciembre de 2008, cuando se recogió un apartado dedicado a las nuevas amenazas y riesgos, la seguridad de los sistemas de información.

Por otra parte, el primer ejercicio de ciberseguridad realizado por ENISA es CyberEurope 2010. En dicho ensayo, los expertos que participaban en la prueba debían hacer frente a los piratas informáticos en su intento simulado de paralizar las infraestructuras críticas de varios Estados miembros. El escenario del simulacro contemplaba que la conectividad de Internet se fuera perdiendo gradualmente de forma significativa en todos los países participantes, reduciendo el acceso a servicios en líneas básicas. Entonces, los diferentes Estados implicados tuvieron que cooperar para evitar el colapso total de la red europea. El resultado del primer ejercicio paneuropeo se cerró con éxito, ya que sirvió para fortalecer la ciberdefensa europea y revelar una serie de puntos donde debían mejorar los canales y procedimientos de comunicación.

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

Incluso la OTAN ha creado en Tallin (Estonia) el Centro de Excelencia para la Cooperación en Ciberdefensa, cuyo objetivo es estudiar ciberataques y determinar las circunstancias en las que 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 consiste, según se manifiesta en su memorándum fundacional, en proteger 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 componentes y de la OTAN y tiene el estatus legal de Organización Militar Internacional (Sánchez, 2010c).

Además, la OTAN ha aprobado un nuevo concepto de ciberdefensa de la Alianza, en el que se hace mención a que la protección de las redes corresponde fundamentalmente a los países aliados. No obstante, se define que la gestión del ciberespacio recae en la Cyber Defence Ma-

nagement Authority (CDMA) que tiene encomendada la misión de la coordinación de este ámbito dentro de la Alianza, centrándose particularmente en la amenaza cibernética; la gestión del riesgo de seguridad; la valoración de las vulnerabilidades; y la continuidad de negocio de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza (Caro, 2011a) (Sánchez, 2011).

Asimismo, la OTAN está impulsando una cooperación práctica en ciberdefensa con sus socios y organizaciones internacionales, y para ello, la CDMA cuenta con el apoyo del Comité de Planificación de Comunicación Civil, los Centros de Excelencia de Ciberdefensa de Tallinn y de Defensa contra el Terrorismo de Ankara, y el Programa de Ciencia por la Paz y la Seguridad, del Consejo de Gestión de Ciberdefensa (CDMB) del que forman parte representantes de todas las autoridades de la OTAN, incluyendo el Consejo del Atlántico Norte (NAC), el Comité Militar (MC), las autoridades de Emergencia Política y Civil, la autoridad de Gestión de la Política (NATO Policy Management Authority, NPMA) y el Comité de Seguridad (NATO Security Committee, NSC), y es supervisado por el Consejo de Gestión de Consulta, Mando y Control (NATO Consultation, Command and Control, NC3B). En todo caso, el Consejo de Gestión es el principal órgano de consulta de la OTAN en materia de ciberdefensa. Téngase en consideración que si antes de los ataques cibernéticos de Estonia en 2007, los esfuerzos de la OTAN se dirigían hacia la protección de los sistemas de comunicación propios y los que eran operados por la Alianza, ahora los destina hacia la ciberseguridad de los países aliados.

Por otra parte, está la Unión Internacional de Telecomunicaciones (UIT) que juega un papel esencial en la seguridad y las tecnologías de la información y la comunicación (TIC), y es el organismo más importante en esta materia en Naciones Unidas. La UIT tiene su sede en Ginebra (Suiza) y está formada por Estados miembros y más de 700 miembros del sector y asociados. Está compuesta por tres sectores: sector de Normalización de las Telecomunicaciones (UIT-T), que estudia los aspectos técnicos; sector de Normalización de las Radiocomunicaciones (UIT-R), que regula la mayor parte del espectro radioeléctrico; y sector de Desarrollo de las Telecomunicaciones (UIT-D), que se encarga de difundir

un acceso equitativo, sostenible y asequible a las telecomunicaciones. La UIT es la responsable de la regulación, normalización y desarrollo de las telecomunicaciones a nivel mundial, intentando cerrar la brecha digital y fortaleciendo las comunicaciones de emergencia, al tiempo que vela por la armonización de las políticas nacionales de telecomunicaciones de los Estados miembros.

Otro organismo internacional que se está centrando en el tema de la ciberseguridad es la Organización de Estados Americanos (OEA), que es la alternativa interamericana para combatir las amenazas a la seguridad cibernética. Será mediante la resolución AG/RES, 2004 (XXXIV-O/04) cuando se adoptó la estrategia interamericana para combatir las amenazas a la seguridad cibernética. La estrategia tomó en cuenta el trabajo de la Comisión Interamericana de Telecomunicaciones (CITEL) sobre la creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones y aumentar la conciencia en el riesgo que afrontan los sistemas y redes de información, y en la necesidad de implementar medidas para hacer frente a los riesgos de seguridad. Consideró también las recomendaciones de la Reunión de Ministros de Justicia, fiscales y procuradores de la Organización de los Estados Americanos (REMJA) en materia de delito cibernético y de seguridad cibernética, y los planes de la Conferencia de Terrorismo y Ciberseguridad (CICTE) para la creación de una Red Hemisférica de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT).

3.4.2 Los sistemas de control como garante de la ciberseguridad de los Estados

Los avances tecnológicos aplicados a los sistemas de vigilancia y control están revolucionando la noble profesión de "espía". Ahora las personas están siendo sustituidas por sofisticados sistemas capaces de interceptar una llamada, o de seguir los movimientos de un individuo por todo el planeta sin apartar los ojos de la pantalla de un ordenador, o de adentrarse en un disco duro sin que el usuario ni siquiera lo detecte. La excusa más utilizada para legitimar el uso de este tipo de sistemas por parte de los Estados es la lucha contra el terrorismo y la delincuencia, es decir, la seguridad nacional e internacional. Aunque como se sabe,

no siempre ha sido así, ya que por ejemplo, gracias al sistema Echelon y 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, 2004, p. 5); o la intercepción 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, 2004, p. 5). En todo caso, son muchos los sistemas que controlan las comunicaciones en el mundo, pero tal vez los más conocidos sean, Echelon, Enfopol, Carnivore y Dark Web.

3.4.2.1 Echelon

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 (Sánchez, 2010c). 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. Aunque, este sistema no sólo intercepta, sino que desencripta, filtra, examina y codifica esta información (Pachón, 2004, p. 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. Tal 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 monitorearlo 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 sus comunicaciones y acciones serán espiadas a partir entonces, en mayor o menor medida, dependiendo de las distintas consideraciones que los responsables consideren 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 trascriben y registran. La mayoría son eliminados después de ser leídos por el sistema (Pachón Ovalle, 2004) (Sánchez, 2009b).

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

1. Los satélites militares 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.

2. Los satélites espías:

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

3. Los nodos de conexión:

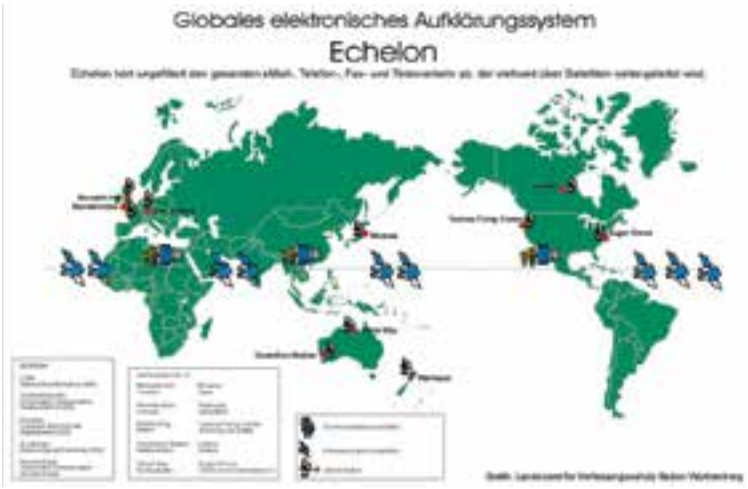
- Nodo de College Park, localizado en Maryland-USA.
- Nodo de Mountain View, localizado en California-USA.
- Nodo de Westminster, en Inglaterra.

4. 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 la coordinación con satélites diferentes de INTELSAT. Maneja el núcleo central del programa informático.

- Bad Aibling (Alemania) para la 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 (Sánchez, 2013).

Figura 2. *El sistema Echelon*



Fuente: http://www.complotsymisterios.com.ar/complots-y-fabulaciones/el-sistema-echelon.html

- 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 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: 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) (Sánchez, 2013).

3.4.2.2. Enfopol

En la Unión Europea estableció su propio sistema de espionaje, Enfopol. Todo comenzó con la Resolución de 17 de enero de 1995, sobre la Interceptación Legal de Comunicaciones, un texto no vinculante, pero tan secreto que el Consejo de la U.E decidió no sacarlo a la luz hasta dos años después. Tal es así, que el programa fue acordado 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 parlamentos 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. Luego con la justificación de "actualizarlo", se compiló ENFOPOL 98, un documento de unas cuarenta páginas. Algunas de esas páginas (relativas a requisitos sobre criptografía y seguridad en los proveedores) desaparecieron, y fueron incluidas en otros documentos; lo que quedó pasó a denominarse ENFOPOL 19. Y el 7 de Mayo de 1.999, contra la opinión de las comisiones de Libertades Públicas y

Asuntos Interiores, y de Asuntos Jurídicos y Derechos de los Ciudadano del Parlamento Europeo, fue aprobado por esta misma cámara.

- El "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 y otros países. Enfopol intentaba imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tuviera 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 debían facilitar <<una puerta de atrás>> para que pudieran penetrar a sus anchas por los sistemas privados. Además, estaban obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas). Todo sin que fuera necesaria una orden judicial" (Añover, 2001). Pero todavía era más exigente para la criptografía. Se pedía que sólo se permitiera este tipo de servicios siempre que estuvieran regulados desde un "tercero de confianza", que deberían entregar automáticamente cuando le fuera 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 (Sánchez, 2013).

- No obstante, Enfopol solo 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 podía interceptar todo tipo de comunicaciones, es más podía 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 llamaba y del que recibía 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 posi-

ble; 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 permitían una correlación de dichos datos con la llamada; cooperación de los operadores/servidores para que proporcionase las comunicaciones "en claro", cuando hubiera de por medio codificación, compresión o cifrado de la misma; una interceptación tal que el sujeto investigado no estuviese al corriente de dicha interceptación; un diseño de interceptación que evitase el uso un 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) (Sánchez, 2013).

3.4.2.3 Carnivore

El "Carnivore", también denominado "DCS 1000", es la tercera generación de los sistemas de espionaje de redes del FBI. 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.

El "Carnivore" es un sistema que ha sido diseñado por la Oficina Federal de Investigación (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. Pero este sistema sólo se dedica a revisar los casilleros del email del "para" y "de", y siempre en relación a un sujeto específico. 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 Buesa, 2009) (Sánchez, 2013).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 (Sánchez, 2013).

3.4.2.4 El "Dark Web"

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 (Sánchez, 2009b).

3.4.2.5 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 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.

Por otra parte, el Congreso de EE.UU. 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 Commnications, 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. Pero con este sistema, entre 1967 y 1973, el FBI sindico de

"subversivas" de muchas actividades domésticas de hombres relevantes como Martin Luther King, Malcolm X, Jane Fonda, Joan Baez y el Dr. Benjamín Spock, etc, pero también de 5.925 extranjeros y 1.690 organizaciones y ciudadanos norteamericanos (Sánchez, 2013).

Paralelamente a estos dos proyectos, la CIA creó por orden del Presidente Lyndon Johnson, la Domestic Operation Division (DOD), cuyo propósito era dirigir, soportar 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 College 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.

El último caso relevante del espionaje estadounidense podemos encontrarlo en el caso "Snowden". Todo comienza cuando Edward Snowden filtra un documento donde se revela que Agencia de Seguridad Nacional estadounidense (sus siglas en inglés NSA) ha espiado las conversaciones telefónicas, a través de Verizon, de 35 líderes mundiales después de obtener los números por medio de un miembro del Departamento de Estado. Entre los espiados se encuentran Angela Merkel, François Hollande, etc. Es más, EE.UU han espiado a la misión de la UE en Nueva York y a 38 embajadas, entre ellas la de Francia, Italia, Grecia y países de Oriente Medio, lo que les permitió, por ejemplo, saber el sentido del voto en la Asamblea de la ONU en temas clave como el reconocimiento de Palestina como Estado observador no miembro. Esta acción de espionaje se enmarca del plan denominado "Prism", un programa de vigilancia cibernética desarrollado por el gobierno estadounidense. Gracias a este programa, el gobierno tenía acceso a los emails, registros de chat y datos de redes sociales a través de nueve empresas de internet (Gmail, Facebook, Hotmail, Yahoo, Google, Skype, PalTalk, Aol, y YouTube) que colaboraron activamente en este espionaje ofreciendo servicios de

puerta trasera. Además, la NSA es capaz de procesar la inmensa cantidad de datos que circula cada segundo por las redes globales. Gracias a un sistema llamado "Xkeyscore" se puede averiguar quién, cuándo y dónde accede alguien a una cuenta o a quién envía un mensaje, para ello extrae, filtra y clasifica la información que cualquier usuario ponga en correos electrónicos y conversaciones digitales, así como historiales de navegadores de Internet.

3.4.3 Los cibersoldados: Elementos de defensa y ataque en el ciberespacio

Sin lugar a dudas, se debe estar desarrollando sofisticadas herramientas informáticas capaces de desmantelar las defensas enemigas, de sembrar el caos en las comunicaciones o de falsificar los datos sobre las posiciones de las tropas (Sánchez Medero, 2009c). 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. Por ejemplo, EE.UU. ha reunido un grupo de hackers de elite que se están preparado para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como "Joint Functional Component Command for Network Warfare" (JFCCNW), una unidad que se cree que está integrada por personal de la CIA, la agencia nacional de seguridad, el FBI, las cuatro ramas militares, algunos civiles expertos y representantes militares de naciones aliadas. Tiene la responsabilidad total de defender la red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información, dañar las comunicaciones rivales hasta inutilizarlas y trabajar con una variedad de socios fuera y dentro del gobierno de los Estados Unidos. Un comando que tiene como contraparte el Grupo Especial de Tareas para la Libertad de la Internet Global (Global Internet Freedom Task Force, GIFTF, por sus siglas en inglés), una organización multiagencias (agencias del gobierno, universidades, investigadores privados, etc) subordinada al Departamento de Estado. Además, con vista a la implantación de un sistema planetario de guerra ciberespacial y el lanzamiento del primer mando militar múltiple del mundo, el mando del Equipo Operativo Conjunto de la Red Global de Operaciones del

Departamento de Defensa de USA fue disuelto oficialmente para pasar a integrarse en el nuevo Cibermando de USA (en inglés, CYBERCOM). Este servirá para fusionar el abanico de operaciones que lleva a cabo el Departamento de Defensa en el ciberespacio, y sus funciones serán liderar la defensa diaria, proteger las redes de información, coordinar las operaciones del departamento de apoyo a las misiones militares, dirigir las acciones y defensa de redes de información especificadas por el Departamento de Defensa, etc. Así, el USCYBERCOM centraliza el comando de operaciones ciberespaciales y fortalece las capacidades ciberespaciales del Departamento de Defensa. Además, el Cibercomando de la Fuerza Área (AFCYBER) ha creado también programas específicos de ciberguerra, entre los que se incluye: adversario, un sistema de objetivo de guerra de la información de la Fuerza Aérea; y arena, un programa de simulación "basado en objeto" para crear estudios por país; como casi tres docenas de otros programas y/o ejercicios de ciberguerra (Sánchez, 2010c).

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. (Sánchez, 2010c).

En España, el Ejército de Ciberdefensa (ECD09) de las Fuerzas Armadas está compuesto por militares especialistas en telecomunicaciones e informática, que han hecho cursos avanzados, militares y civiles, en seguridad de las TIC, así como ingenieros superiores civiles de ISDEFE, 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. Además, existe el Centro de Respuesta a Incidentes de Seguridad Computacionales (CSIRT), que se trata de un equipo de técnicos especialmente entrenados para resolver y gestionar incidentes informáticos de alto impacto.

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, 76). Además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares y ha creado escuelas donde 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 dado cuenta que, de momento, no pueden ganar a EE.UU en un guerra convencional y, por tanto, están buscando nuevos campos de batalla donde puedan ser superiores, como en el ciberespacio (Brookes, 2007) (Sánchez, 2010c).

Comprender el funcionamiento de la unidad militar del ejército chino en cuanto a ciberespionaje y operaciones cibernéticas ayuda a entender el entramado de dicha estructura. Como se ha mencionado anteriormente, en China es el Departamento General de Personal el que se encarga de este tipo de cuestiones, y los tres departamentos que se encuentran bajo su supervisión trabajan conjuntamente. Así, por ejemplo, los hackers del segundo departamento pueden violar los sistemas de seguridad de los satélites y proporcionar datos útiles al tercer departamento, que es el responsable de inteligencia electrónica. Los espías físicos del primer departamento pueden infectar internamente un malware en las redes de una empresa, el cual luego facilita el acceso a los hackers del segundo departamento. Es más hay empresas estatales que operan directamente bajo la dirección de cada uno de los tres departamentos, al

igual que bajo otras ramas militares del ejército. Pero además el ejército chino también puede superponerse con los departamentos de seguridad nacional, y participar directamente en algunas acciones.

3.5 Los grupos armados se lanzan a la red

Internet se ha convertido en la mayor plataforma de expresión disponible en todo el mundo. Hoy en día, se puede encontrar todo tipo de material en Internet, y resulta casi imposible para los diversos servidores y los gobiernos controlar todo el contenido que se vierte sobre el ciberespacio. De ahí, que las nuevas tecnologías, y en concreto Internet, ofrezca a los grupos armados vías alternativas (o más bien complementarias) para difundir libremente, sin prácticamente censuras, sus mensajes. Por tanto, no es de extrañar que se hayan inclinado hacia ella, y el ciberespacio se haya transformado por las ventajas que ofrece en el marco ideal de sus operaciones ideal (Merlos García, 2006a). Hasta el punto que en 1998 se identificaron por lo menos unas 30 organizaciones terroristas que tenían un espacio en Internet y justo dos años después se pudieron encontrar cientos de estas páginas en la red. Actualmente, existen alrededor de 10.000 sitios web dedicados a la divulgación de material violento y terrorista, lo que indica un crecimiento de la presencia de estos grupos en el ciberespacio. Es más, en estudio llevado a cabo por la Oficina Europea de Policía (EUROPOL) en 2008 se advertía, al analizar las tendencias del terrorismo en suelo europeo, que el uso que hacía los grupos armados de Internet seguía siendo muy preocupante, pues las direcciones en la red, weblogs y foros eran utilizados para la propaganda y las comunicaciones de grupos y redes terroristas, destacándose en particular el incremento en las direcciones de carácter islamista elaboradas en lenguas occidentales en un intento de ampliar lo más posible su espacio de actuación (Echevarría, 2009) (Sánchez, 2010c).

Así, no cabe duda que los grupos armados se han volcado en la red. Uno de los primeros fue el "Movimiento Sendero Luminoso", después lo harían otros como Al Qaeda, Ejército Republicano Irlandés (IRA), Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Euskadi Ta Askatasuna (ETA), el Hezbollah, etc (tabla 1). Se podría decir que, prácticamente,

todos los grupos armados disponen de algún tipo de espacio (web, foro, site, etc) en la red. Bien sea para divulgar la historia de la organización y de sus actividades, la información sobre sus objetivos políticos e ideológicos, las críticas de sus enemigos, o simplemente, para verter amenazas o abrir foros de debate e interactuar con sus seguidores y simpatizantes. Aunque eso sí, no siempre son fáciles de encontrar ni de acceder, ya que como cabe de suponer suelen ser perseguidos por los servicios policiales y de inteligencia de los distintos gobiernos. De ahí, que normalmente se mantengan poco tiempo en una misma dirección, cambiando constantemente de ubicación, o bien, porque su acceso se encuentra limitado por un administrador.

Cuadro 3.1. *Grupos Armados 2002: Websites.*

Grupos Armados	Sitios web	Idioma
Abu Nidal Organisation (ANO)		
Abu Sayyaf Group (ASG)		
Al-Aqsa Martyrs Brigade		
Armed Islamic Group (GIA)		
Asbat al-Ansar		
Aum Supreme Truth (Aum)	http://www.aleph.to/index_e.html http://www.aleph.to	Inglés, Japonés
Basque Homeland and Liberty (ETA)	http://www.contrast.org/mirrors/ehj/index.html http://www.batasuna.org/	Inglés, Vasco
Al-Gama'a al-Islamiyya (Islamic Group)	http://www.azzam.com	Inglés
Hamas	http://www.palestine-info.com/hamas	Árabe, Inglés

Grupos Armados	Sitios web	Idioma
Harakat ul-Mujahidin (HUM)	http://www.ummah.net.pk/harkat/	Árabe, Inglés
Hizbollah	http://www.hizbollah.org	Árabe, Inglés
Islamic Movement of Uzbekistan		
Jaish-e-Mohammed		
Al-Jihad (Egyptian Islamic Jihad)		
Kahane Chai (Kach)	http://www.kahane.org	Inglés
Kurdistan Workers Party (PKK)	http://www.pkk.org/index.html	Kurdo
Lashkar-e-Tayyiba	http://www.markazdawa.org.pk/	Árabe, Inglés
Liberation Tigers of Tamil Eelam	http://www.eelamweb.com/	Inglés
Mujahedin-e Khalq Organization	http://www.iran-e-azad.org/english/index.html	Inglés
National Liberation Army (ELN), Colombia	http://www.eln-voces.com/	España
Palestine Islamic Jihad (PIJ)	http://www.entifada.net/	Árabe
Palestine Liberation Front (PLF)		
Popular Front for the Liberation of Palestine (PFLP)	http://www.pflp-pal.org/main.html	Inglés
Popular Front for the Liberation of Palestine- General Command (PFLP-GC)		

Grupos Armados	Sitios web	Idioma
al-Qaida	http://www.alneda.com	Árabe
Real IRA		
Revolutionary Armed Forces of Colombia (FARC)	http://www.farc-ep.org/	Inglés, España, Portugués, Italia, Alemania, Rusia
Revolutinary Nuclei (formerly ELA)		
Revolutionary Organization 17 November (17 November)		
Revolutionary People's Liberation Party/Front (DHKP/C, Dev Sol)	http://www.ozgurluk.org	Inglés
Salafist Group for Call and Combat	N/A	N/A
Sendero Luminoso	http://www.csrp.org/	Español, Inglés.
United Self-Defense Forces of Colombia (AUC)	http://colombia-libre.org/colombialibre/pp.asp	Español

Fuente: (Conway, 2002).

Otra cuestión a tener en consideración son los destinatarios de las webs. Téngase en cuenta, que, por ejemplo, el 78% de las visitas a las webs yihadistas proceden de Oriente Medio y el Norte de África, mientras que el restante 22% provenían del resto del mundo. Pero eso no significa que los grupos renuncien a buscar apoyo fuera de sus propias fronteras, ya que es normal encontrar páginas dirigidas exclusivamente a simpatizantes que residen en su territorio y otras destinadas para aquellos que viven en otros lugares del planeta. Práctica, por cierto, muy habitual entre los grupos yihadistas. Dado que desde la óptica del yihadismo, los musulmanes afincados en Occidente son los perfectos muyahidínes,

ya que conocen el idioma del enemigo, están habituados a sus usos y costumbres, y poseen un estatus jurídico que les facilita la movilidad y la confidencialidad de sus operaciones, pero también tienen una situación económica inferior al resto de la población de las sociedades en las que habitan, lo que les vuelven más permeables a la sensibilización psicológica que pueda proyectar este tipo de organizaciones (Sánchez, 2010b).

3.5.1 Las tipologías de los sitios web de los grupos armados

La tipología de los sitios web de los grupos armados sería la siguiente:

1. *Sites oficiales o webs* creadas y administradas directamente por miembros de la organización: Es el grupo menos numeroso pero el más importante y el más cuidado estética y técnicamente, ya que este tipo de páginas son las principales fuentes para acceder a la difusión de nuevos vídeos, grabaciones sonoras, libros y cualquier otro material original (Torres Soriano, 2009a: 300). En la red podemos encontrar webs del Ejército Republicano Irlandés (IRA), Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Sendero Luminoso, ETA) el Hezbollah, etc. Por ejemplo, las FARC colgaron una página que funcionaban en seis idiomas (español, inglés, francés, italiano, alemán y portugués) para facilitar el intercambio de informaciones. En dicha página web se podía leer los partes de guerra desde 1997, poemas escritos por guerrilleros, una revista on-line, un programa de radio, y mensajes dirigidos a captar la atención de los jóvenes colombianos. El grupo Hizbollah, por ejemplo, ha tenido una importante presencia institucional a través de un sitio propio, que poseía tres réplicas a fin de que si una era clausurada, se pudiera acceder a las demás (www.hizbollah.org, www.hizballah.org, y www.hizbollah.tv). Estos sitios estaban escritos en árabe pero con una versión en inglés, y en ellos se ofrecían una amplia garantía de fotos, archivos de audio y video con discursos propagandísticos. En el sitio oficial de Hamas (http://www.palestine-info.com) se ofrece comunicados, biografías de los líderes y mártires del movimiento, y relatos de

momentos importantes de su historia. Además esta organización ha contado con seis sitios subsidiarios en distintos idiomas: inglés (www.palestine-info.co.uk), francés (www.palestine-info.cc), ruso (www.palestine-info.ru), malayo (www.infopalestina.com), urdu (www.palestine-info-urdu.com), y farsi (www.palestine.persian.info).

El problema de estas webs es que suelen estar muy perseguidas, lo que hace que su presencia sea bastante breve, hasta que pasado un tiempo son capaces de reubicarse en nuevo dominio (Conway, 2002). Para solventar esta dificultad, más que recurrir a la puesta en marcha de nuevas y efímeras "webs oficiales", que son rápidamente hackeadas, la solución ha sido recurrir a una serie de plataformas completamente virtuales, cuyo cometido es recibir los materiales procedentes de los grupos que combaten la yihad, editarlos y distribuirlos a través de una red de webs y foros de confianza (Torres Soriano, 2009a: 307).

No obstante, este tipo de web no son fáciles de localizar. Como casi siempre, se parte de las búsquedas de Google, aunque también se puede realizar mediante la localización de blog o los enlaces que aparecen en las páginas de Wikipedia, o supervisando Whois [http://www.whois.com] o el portal islámico [http://www.worldofislam.info] o el blog del antropólogo denominado Gerad [http://warintel.blogspot.com] o el Southern Poverty Law Center [http://www.splcenter.org]. Además, mucho de los enlaces que encontramos pueden llegar a ser altamente cuestionables, o no están traducidas al inglés.

Otra cuestión, es que guerras como la de Irak también han trasladado su campo de batalla a la red. Tal es así, que hay muchos sitios web terroristas con fuerte lazos con simpatizantes de la resistencia islámica en su conjunto. Por ejemplo, Al-Zarqaqi [http://www.alamer.biz/ameer/home.html] está dedicado a los seguidores de Abu Musab Al-Zarqawi un terrorista de origen jordano que formó el grupo Al-Qaeda de Irak y que fue asesinado en 2006; o la página web Ansar [http://www.al-ansar.biz] repre-

senta Ansar al Sunna, un conglomerado de facciones terroristas formado en 2003, que inauguró su web con un video de la decapitación del ciudadano americano Nicholas Berg; o el Ejército Islámico en Irak [http://iasite-eng.org] que se dedica a trasmitir las operaciones militares realizadas sobre el terreno.

2. *Foros*: Es un página web donde se coloca alguna pregunta sobre un tema en especial, esperando abrir un debate. Su diseño, gestión y estructura les vuelve especialmente atractivo para los grupos armados. Así, en estos foros suelen registrarse destacados miembros del grupo, que con el objeto de evitar los inconvenientes asociados a la "inestabilidad" de sus webs oficiales, utilizan estas plataformas para colgar nuevos comunicados y enlaces hacia nuevo materiales (Torres Soriano, 2007: 260). Por este motivo estos foros suelen estar sometidos a varias medidas de "seguridad". Por ejemplo, es frecuente encontrar contraseñas de entrada para prevenir la sobrecarga de las mismas, o que estén sometidos a la censura interna de sus administradores para evitar envíos que contradigan el mensaje yihadista, o que los administradores delimiten los contenidos en función de la categoría que les otorgan a los diferentes miembros en función de sus méritos dentro del foro, etc. (Sánchez, 2010b).

3. *Blogs*: Son utilizados para expresar opiniones y distribuir contenidos y enlaces con otras páginas. Gracias a los blogs se puede crear un verdadero *"feed back"* de la comunicación, ya que atraviesa un modelo bidireccional (uno a uno) para acabar en un modelo multidireccional (muchos a muchos). Los blogs se convierten así en un espacio de discusión sobre la información relacionada expuesta, que permite no sólo el debate entre el lector y bloggero sino que también entre los lectores. Los blogs son, por tanto, un medio democrático para difundir ideas, en el sentido que cualquier persona con acceso a un ordenador con Internet y unos conocimientos básicos puede establecer uno. Pero ahí está también su mayor peligro, cualquiera puede crear una identidad falsa y divulgar información falsa o contradictoria, confundiendo a los lectores (Sánchez, 2010b).

4. *Sites de distribución*: Tienen como objetivo el sustento de la infraestructura del grupo, de manera que los miembros del mismo no queden desenganchados de la *umma* virtual, como consecuencia de los *hackeos* por parte de los servicios de inteligencia y ciberactivistas individuales (Torres Soriano, 2007: 261). Además muchas de ellas son auténticos directorios actualizados donde es posible encontrar reubicadas las más importantes webs yihadistas, lo que las han convertido en un valioso recurso para aquellos individuos que se inician en el consumo de estos materiales, ofreciendo de manera sencilla y accesible toda una serie de recursos de información a través de los cuales pueden llevar a cabo una profundización en la ideología de los grupos (Torres Soriano, 2007: 261) (Sánchez, 2010b).

5. *Los grupos mediáticos*: El grupo mediático más representativo es, sin duda, el llamado Global Islamic Media (GIM), transformado posteriormente en Global Islamic Media Front (GIMF). Originalmente constituía uno de los grupos o espacios virtuales que la compañía Yahoo ofrece a los usuarios de sus cuentas gratuitas de correo electrónico. Dicho grupo atesoraba las direcciones de e-mail de casi 7.500 usuarios afiliados, los cuales recibían regularmente información sobre nuevos materiales, vídeos, enlaces, etc (Torres Soriano, 2009a: 303) (Sánchez, 2010b).

6. *Las redes* sociales: Una red social que permite comunicar al instante a cientos de miles de sus componentes, simplemente publicando un *"post"* que no puede superar los 140 caracteres. Los mensajes para cualquiera de estos *"microblogs"* pueden enviarse desde la web, un móvil vía SMS o los sistemas de mensajería instantánea (en el caso de Twitter, Aol, GTalk, .Mac, LiveJournal y Jabber), con una facilidad asombrosa, como un chasquido de dedos. En ellas, además, los usuarios pueden intercambiar de manera abierta fotografías, textos y opiniones, sino también informaciones de interés como las nuevas direcciones webs de grupos terroristas. De ahí, que algunos grupos armados, como por ejemplo, Sendero Luminoso, haya creado redes sociales en Facebook y Hi5, o Hizbullah creó la suya en 2012 (Facebook.com/Hezb.alaah).

Además, actualmente, distintos grupos terroristas están lanzando sus propias aplicaciones para IPhone, IPad, Android, BlackBerry, Nokia o Google Play (Sánchez, 2010b).

Desde su creación el poder de las redes sociales no ha dejado de crecer, válganos simplemente de ejemplo la capacidad de movilización y de repercusión que han mostrado durante la guerra de Irak. Tal es así, que se han utilizado Twitter para enviar y recibir a tiempo casi real los movimientos de las tropas extranjeras, fotografías de su ubicación y mensajes entre los soldados. No obstante, cada vez más Twitter o Facebook da de baja aquellas cuentas en las que se produce amenazas directas, una cosa que suele suceder con demasiada frecuencia en las cuentas vinculadas a los grupos terroristas, pero éstos pronto abren otra para continuar su actividad. Por tal motivo, los gobiernos están intentando poner freno a esta actividad de los terroristas en las redes sociales solicitando una mayor transparencia en las reglas y regulaciones de las empresas que regulan las mismas. Tal es así, que en los informes que publicó Twitter en el 2012 advirtió de un aumento constante de las peticiones de los gobiernos para eliminar contenido y avisos de copyright, aunque también señala que en la mayoría de las ocasiones no ha cumplido con tales requerimientos (Sánchez, 2010b).

En todo caso, las redes sociales se han convertido en un sitio ideal para que los grupos terroristas puedan llegar a unos grupos de edad imprescindible que podría identificarse con la causa y, posiblemente, se muestren de acuerdo a unirse a la organización. De esta manera, los grupos terroristas a través de estas plataformas consiguen una lista de reclutas y de simpatizantes predispuestos. No obstante, estás prácticas también tienen sus peligros porque las fuerzas de seguridad pueden rastrear a los miembros y seguidores de toda una cuenta. Pero al mismo tiempo, los grupos terroristas también pueden utilizar estos sitios webs para supervisar y obtener información del personal militar enemigo. Tal es así, que en el Departamento de Defensa de Canadá y EE.UU y el servicio secreto británico MI5 ha llegado a solicitar a sus

miembros eliminar de las redes sociales todos sus datos personales ante la vigilancia de estos espacios por los grupos terroristas (Weimann, 2011: 8). El motivo es que muchos soldados publican información detallada sobre ellos mismos, sus carreras y familias, fotografías de amigos, etc, y pueden estar poniendo en peligro a su círculo más cercano y su seguridad.

7. *Páginas de alojamientos de vídeos y archivos*: YouTube, Internet. Archive, World TV; Megaupload o similares, esconden miles de archivos y videos de grupos armados. Además, en ellas grupos de música hip-hop y rap cuelgan sus videoclip, donde se enfatiza sobre la opresión mundial contra el Islam o la necesidad de reinstaurar un califato islámico regido por la sharia. Pero ahí no queda la cosa, sino que la guerra cibernética también se ha trasladado a este tipo de portales. La guerra entre Israel y Hamas es un buen ejemplo de ello. En un conflicto donde los corresponsales de prensa no pueden acceder a la Franja de Gaza por el bloque israelí, el control de los mensajes difundidos por la red cobran tanta importancia como las propias operaciones militares. Así, el ejército israelí se ha dedicado hacer alarde de su lucha contra los terroristas de Hamas en el portal de YouTube. Uno de sus videos más vistos es un ataque israelí contra un centro de almacén de misiles palestinos destinados a civiles inocentes. Por el contrario, los palestinos han contraatacado en el portal de vídeos PalTube, colgando imágenes de mujeres llorando, alrededor de cadáveres de niños ensangrentados, como una forma de mostrar al mundo la barbarie del ejército israelí contra su pueblo, o emitiendo en directo la programación de la cadena Al-Quds, vinculada a Hamás (Sánchez, 2010b).

   Pero además los grupos armados se están valiendo de las webs de empresas que se dedican a ofrecer a sus clientes la posibilidad de alojar en sus servidores archivos que pueden ser descargados por cualquier usuario simplemente con copiar en la barra de direcciones de su navegador. Un link que está disponible en una serie de foros que actúan como bibliotecas virtuales de enlaces. Aunque es muy probable que esta estrategia de comunicación

sea remplazada por otro tipo de páginas que como *Megavideo* y *InternetArchive.org* permiten no sólo alojar y descargar estos archivos de gran tamaño sino también poder visionarlos *on-line*, lo que acelera el proceso de su "consumo" al tiempo que se reducen los "rastros digitales" que supone descargar y alojar estos contenidos en una computadora (Torres Soriano, 2009b) (Sánchez, 2010b).

3.5.2 La construcción de los sitios web de los grupos armados

Está claro que no todos los grupos armados han otorgado la misma importancia a su estrategia comunicativa. Para algunos supone un frente esencial hacia la victoria, mientras que para otros es una cuestión secundaria (Torres Soriano, 2009a: 32). Pero pese a ello, en una primera etapa, muchas organizaciones pusieron en marcha sus propias webs oficiales para difundir sus comunicados, videos, documentos, etc. Dado que Internet se ha convertido en lugar ideal para que los grupos difundan sus mensajes y para comunicarse con otros y con sus simpatizantes. Aunque normalmente los grupos armados, en especial los yihadistas, suelen externalizar su acción propagandística, al dejar que sean los activistas más cualificados los que se dediquen a estos menesteres. Aunque eso sí, las plataformas suelen tener un contacto directo con los grupos, por lo menos mantienen algún tipo de lazo de conocimiento y confianza con individuos concretos y con autoridad suficiente para actuar en nombre de sus respectivas organizaciones, lo que explica que los grupos estén dispuestos a ceder una importante parcela de esta actividad (Torres Soriano, 2009a: 320). Así, por ejemplo, el sitio no oficial más oficial del Zapatismo, www.ezln.org, fue creado por Justin Paulson, -estudiante en literatura inglesa en la Universidad de Pensilvania-, y tiene su origen en Estados Unidos. Paulson empezó a subir información en inglés del movimiento en 1994, en un sitio con la siguiente dirección: http://www.peak.org/~justin/ezln/. Cuando la organización se enteró de su labor, le autorizó, a través de Javier Elorriaga, para colgar materiales zapatistas en la página www.ezln.org. Por lo tanto, los llamados "ciberzapatistas" no son miembros del EZLN, sino por el contrario, son simpatizantes de la sociedad civil, sin ningún vínculo oficial con el zapatismo (Sánchez, 2010b).

Prácticamente lo mismo sucede con la yihad. Su mayor ciberactivista ha sido Younis Tsouli, hijo de un diplomático marroquí destinado en el Reino Unido, que pasó de ser un simple hacker a productor y distribuidor de *warez*, para después centrarse en labores de mayor compromiso ideológico como podían ser: facilitar enlaces de utilidad, reubicar sus páginas, plasmar su pericia informática en los foros para que otros pudieran hacer lo mismo, colaborar con la plataforma propagandística como Global Islamic Media Front, Tibyan Publications o Yihad Media Battalion, robar números de tarjeta de crédito, traducir textos, etc. Se puede decir que Tsouli ha llegado a ser el máximo exponente de una nueva generación de partidarios de la yihad dispuestos a volcar su habilidad técnica en nuevos e imaginativos usos de la red (Gunaratna, 2003). Además, se puede decir que existen cientos de sitios web administrados por individuos que apoyan a la yihad sin, probablemente, haber conocido a ningún insurgente o haber mantenido ningún tipo de vinculación con el grupo terroristas. De ahí, que por ejemplo el número de sitios web dedicados a hacer apología del terrorismo islamista de Al Qaeda aumente en aproximadamente 900 cada año (Sánchez, 2010b).

En el caso de Al Qaeda fue un estudiante de ingeniería en el Imperial College de Londres, Babar Ahmad, el responsable de poner en marcha en 1996 la primera web de la organización, www.azzam.com, y fue su administrador hasta que fue detenido en 2003. Aunque la primera web con vocación de ser la plataforma oficial de Al Qaeda fue www.maalemajihad.com ("hitos de la yihad"), que fue lanzada por un simpatizante de la Yihad. El problema fue que justo un año después de su creación desapareció de la red, debido a que su administrador olvidó renovar la suscripción con el servidor chino donde se encontraba alojada. Luego aparecerían otras webs vinculadas a la organización. Tal vez, la más importante haya sido www.alneda.com ("la llamada"), donde era posible encontrar bajo un formato atractivo y colorista, una amplia gama de recursos: comunicados oficiales, "noticias" sobre la marcha de la yihad, archivos de audio y video, fotografías especialmente significativas, logotipos, recomendaciones de seguridad a los activistas, instrucciones de carácter técnico para llevar a cabo "ciberyihad" y, sobre todo, foros donde eran posible interactuar con la comunidad yihadista directa a través del inter-

cambio de opiniones, sugerencias y opiniones (Torres Soriano, 2004: 227). Aunque Al Qaeda jamás ha reivindicado su dominio, pero eso sí, Abu al Laith al Libi, comandante de Al Qaeda, recomendaba este sitio web a los lectores de Islamic Jihad Online, afirmando que era una "web gestionada por hermanos de confianza […]" (Anoymous, 2002). La cuestión es que de nuevo, a mediados de 2002, Al Qaeda perdió su dominio a manos de un ciudadano estadounidense, aunque siempre ha tratado de resucitar una y otra vez la emblemática web, gracias a la inestimable colaboración de su administrador, Yousef Al Ayiri (Sánchez, 2010b).

En todo caso, la participación de activistas voluntarios de nuevo es importante. Tal es así que, por ejemplo, Al Qaeda está organizado, periódicamente, concursos *"on-line"* para rapsodas o recitadores de Corán[1]. Incluso, en los últimos tiempos han puesto anuncios de empleo en Internet pidiendo partidarios que les ayuden en sus montajes de vídeo y sus comunicados en la web sobre los extremistas en Irak, en los territorios palestinos, en Chechenia y en otras zonas conflictivas donde los combatientes están activos[2]. Pero la importancia que concede Al Qaeda a su estrategia comunicativa es tal, que pese a contar con colaboradores, nunca se ha desligado ella, siendo siempre controlada por la organización. Por ello, creó As-Sahab Institute for Media Production, un ente que centralizó toda la actividad propagandística, y el Frente Mediático Islámico Global (FMIG), que se ha dedicado hacer de Internet una especie de nuevo "cuartel general" para desarrollar "la guerra santa mediática" (Torres Soriano, 2009a). Pero no es el único grupo terrorista que deja su estrategia comunicativa al azar, por ejemplo, el IRA cuenta con un "Director de Publicidad", lo que muestra la importancia que también atribuye a este tema (Sánchez, 2010b).

3.6 El uso pasivo de los grupos armados

Pese a las actividades que tanto los grupos terroristas como los propios Estados están realizando en Internet, todavía no se ha producido

1. El País, 11 de enero de 2008.
2. Ryhno Zeros Web, del 4 de marzo de 2005.

ningún ataque que nos pueda inducir a proclamar el inicio de una verdadera ciberguerra o ataque ciberterrorista, con la única salvedad por el que en el 2017 afecto a 150 países. No obstante, hasta el momento solo se han encontrado rastros de visitas o intentos de acceso a infraestructuras estratégicas norteamericanas en ordenadores capturados a yihadistas, pero sin mayores consecuencias. Los ataques informáticos se han limitado, en la mayoría de los casos, a colapsar los servicios de sitios web de instituciones o empresas (Ej. Estonia, 2007), inutilizar los sistemas de comunicación (Ej. Guerra del Golfo, 1991), contrainformar (Ej. Guerra Kosovo, 1999), o robar información (Ej. EE.UU., 2009). Por eso, podemos decir que hasta el momento unos y otros están haciendo un uso pasivo de la red. Pero también es cierto que ya no solo utilizan internet para buscar medios de financiación, reclutar nuevos militares o hacer propaganda sino también para tener mayor presencia pública. Es más ahora, emplean internet para amenazar abiertamente unos a otros o para reclamar la autoría de un atentado (Sánchez, 2010b).

3.6.1 La financiación

Los grupos terroristas están empleando la red, como otras organizaciones, para financiarse, es decir, como un medio para recaudar fondos para la causa. Por tal motivo, los terroristas están utilizando sus páginas webs para solicitar donaciones a sus simpatizantes. Por ejemplo, Al Qaeda depende en gran medida de los donativos, y su red global de recaudación se apoya en sociedades benéficas, organizaciones no gubernamentales y otras instituciones financieras que disponen de sedes y foros de Internet. El sitio web del IRA contenía una página en la que los visitantes podían hacer donaciones con sus tarjetas de crédito, Hamas ha recaudado dinero a través de la página web de una organización benéfica con sede en Texas, la Fundación Tierra Santa para la Ayuda. Los terroristas chechenios han divulgado por la red el número de cuentas bancarias en las que sus simpatizantes podían hacer sus aportaciones. La organización sunita Hizo al-Tahir pide contribuciones económicas a sus simpatizantes, que son identificados gracias a las visitas que éstos realizan a determinados sitios web. Babar Ahmad desde el sur de Londres puso en funcionamiento "Azzam Publications" y un número de webs asociados que se centraron principalmente en el

apoyo de los talibanes en Afganistán y los muyahidin en Chechenia (Jacobson, 2009: 17). En estos sitios incluso se proporcionan instrucciones para que las personas puedan mover dinero, aludiendo para ello, que el apoyo de la yihad en cierto modo era una obligación para todo musulmán (Jacobson, 2009: 17). No olvidemos que Internet ofrece cierto grado de autoanonimato y seguridad, tanto para los donantes y los receptores (Jacobson, 2009: 17) (Sánchez, 2009d).

Pero también se están valiendo de Internet para extorsionar a grupos financieros, transferir dinero, realizar transferencias financieras a través de bancos offshore, lavar y robar dinero, usar el dinero electrónico (*cybercash*) y las tarjetas inteligentes (smart cards), efectuar ventas falsas de productos, o perpetuar diferentes timos mediante correos spam, etc. Su financiación procede principalmente de dos fuentes, la primera es la que les proporcionan las organizaciones con infraestructuras suficientes para obtener y suministrar fondos a las organizaciones terroristas, o una persona que posea medios suficientes que le permita financiar al grupo, y la segunda es la ganancia que obtienen dichos grupos con el desarrollo de actividades relacionadas con el secuestro y la extorsión. Pero además, a diferencia de otras organizaciones delictivas, las organizaciones terroristas pueden incluir ingresos derivados de fuentes legítimas (por ejemplo, Instituciones Benéficas) o de una combinación de fuentes legales e ilegales (Sánchez, 2009b).

3.6.2 La guerra psicológica

También están usando el ciberespacio para librar la llamada "guerra psicológica". Existen incontables ejemplos sobre cómo se sirven de este medio sin censura para propagar informaciones equívocas, amenazar o divulgar las imágenes de sus atentados. Al Qaeda, por ejemplo, combina propaganda multimedia y los avances de la tecnología de la comunicación para crear una sofisticada forma de guerra psicológica. Desde el 11 de septiembre de 2001, la organización ha llenado sus sitios web con una serie de anuncios de un inminente ataque a EE.UU. Estas advertencias han recibido una considerable cobertura en los medios de comunicación, lo que ha contribuido a generar un sentimiento generalizado de temor e inseguridad entre los ciudadanos de todo el mundo, especialmente los

estadounidenses. A través de esta estudiada estrategia, los grupos han conseguido trasmitir una imagen interna de vigor, fortaleza y pujanza, y sus mensajes han alcanzado un impacto global (Sánchez, 2009b).

Los videos de las torturas, las súplicas y/o el asesinato de rehenes como los estadounidenses Nicholas Berg, Eugene Armstrong y Jack Hensley, los británicos Kenneth Bigley y Margaret Hassan o el surcoreano Kim Sun-Il que han circulado descontroladamente por numerosos servidores y portales de Internet no han hecho más que reforzar la sensación de indefensión de la sociedad occidental, pero además han cuestionado la legitimidad y los efectos de la "Operación Libertad Iraquí". De esta manera, los grupos están consiguiendo transmitir una imagen interna de vigor, fortaleza y pujanza, y sus mensajes están alcanzando un impacto global. Todo para intentar minar la moral de EE.UU y sus aliados, y fomentar la percepción de vulnerabilidad de esas sociedades. Al mismo tiempo, se han dedicado a divulgar imágenes, textos y videos sobre los ataques que están soportando los musulmanes con el objetivo de incitar a la rebelión y a la lucha armada, tratando de conseguir lo que el sociólogo francés Farhad Josrojavar denomina "frustración delegada", es decir, la rebelión ante la injusticia que sufren otras personas, pero también para levantar la moral de los combatientes (Sánchez, 2009d).

3.6.3. El reclutamiento

Asimismo, la red está sirviendo para reclutar a miembros de la misma manera que algunas personas la usan para ofrecer sus servicios. En primer lugar, porque al igual que las sedes comerciales rastrean a los visitantes de su web para elaborar perfiles de consumo, las organizaciones terroristas reúnen información sobre los usuarios que navegan por sus sedes. Luego contactan con aquellos que parecen más interesados en la organización o más apropiados para trabajar en ella. En segundo lugar, porque los grupos terroristas cuentan con páginas webs en las que se explican cómo servir a la Yihad. En tercer lugar, porque los encargados de reclutar miembros suelen acudir a los cibercafés y a las salas de los chats para buscar a jóvenes que deseen incorporarse a la causa. Y en cuarto lugar, la red abre la posibilidad a muchos para ofrecerse a las organizaciones terroristas por su propia iniciativa. Así, por

ejemplo, un cibernauta que estaba deseoso de participar en la Yihad de Iraq estableció, con el seudónimo de "La redención está cerca", un diálogo virtual con un tal "Terrorista sin piedad". Al cabo de unos días este último le mandó un vídeo propagandístico y un programa de comunicación encriptado para afinar los últimos detalles de su participación en el conflicto (Sánchez, 2009d).

Los blogs también han desempeñado un papel importante en el reclutamiento de nuevos miembros. En un foro, un participante apodado Wali al-Haq publicó los pasos que debe tomar un candidato a unirse a Al-Qaeda: 1) entender y respetar la identidad, la ideología y los objetivos de Al-Qaeda, 2) preparación física, científica y espiritual, y 3) o bien directamente unirse a una facción de jihadistas o seguir un camino solitario en la toma de la causa yihadista. Según al-Haq, cualquier musulmán que apoya a Al-Qaeda en cualquier forma, ya sea económica, física o simplemente mostrando el deseo de la intención de unirse, es considerado como un yihadista en al-Qaeda (Bakier, 2008).

3.6.4 La interconexión y la comunicación

Además, Internet les está proporcionando medios baratos y eficaces de interconexión. A través de la red, los líderes terroristas son capaces de mantener relaciones con los miembros de la organización u otra sin necesidad de tener que reunirse físicamente, tal es así que los mensajes vía correo electrónico se han convertido en la principal herramienta de comunicación entre las facciones que están dispersas por todo el mundo. No obstante, habría que mencionar que los grupos terrorista, utilizan técnicas muy diversas para evitar la intercepción de sus mensajes, entre las que cabe destacar la estenografía, la encriptación y los semáforos rojos (Sánchez, 2010a).

Pero también pueden colgar mensajes en el servidor corporativo privado de una empresa predeterminada para que operativos/receptores recuperen y, a continuación, eliminen el comunicado sin dejar rastro alguno; o manipular páginas electrónicas de empresas privadas u organismos internacionales para crear en ellas ficheros adjuntos con propaganda; u ocultar datos o imágenes en website de contenido pornográfico. Por ejemplo, el video del rehén Paul Johnson apareció en primicia

mundial en la página electrónica de la empresa "Silicon Valley Land Surveying", con sede en San José (California), lo que constituyó una auténtica revolución mundial en las técnicas de propaganda y una emulación de las "formas de trabajo" empleadas casi exclusivamente hasta ese momento por cibercriminales o piratas informáticos. Aunque existe otra técnica más simple para transmitir órdenes y comunicados, es la llamada "semáforos electrónicos" (o "semáforos on line"). Ésta consiste en que un cambio de color de una imagen o del fondo de una fotografía en una página preestablecida se convierte en un signo, en una señal que esconde un significado (una orden de ataque, la fecha y el lugar para una reunión) entre los terroristas involucrados en ese proceso de comunicación interna (Sánchez, 2009d).

Aunque entre todos los métodos que emplean el más creativo sea establecer comunicaciones a través de cuentas de correo electrónico con nombres de usuarios y claves compartidas. Así, una vez acordadas las claves, los terroristas se las comunican por medio de draft, messages o borradores. La forma de comunicación es sencilla, el emisor escribe un mensaje en esa cuenta y no lo manda sino que lo archiva en el borrador, y el destinatario, que puede estar en otra parte del mundo, abre el mensaje, lo lee y lo destruye, evitando que pueda ser interceptado. El acceso a los buzones se hace desde cibercafés públicos, con lo que es imposible saber quién en un momento dado ha accedido desde un ordenador concreto.

Otro método que se está viendo utilizando es la tecnología conocida como Voz IP. Lejos quedaron los primeros programas utilizados como "Internet Phone" y "PGPFone", los cuales requerían de un ordenador personal, de acceso a una línea telefónica analógica o digital, así como de un micrófono y unos auriculares. No obstante, y a medida que Internet se fue extendiendo y aumentando exponencialmente el número de usuarios, el uso de los nuevos programas que aparecerían durante los siguientes años tales como Messenger, Skype o Paltalk, supondría la apertura y desarrollo de una "nueva forma o modo de comunicación" más discreto y seguro para poder mantener comunicaciones a nivel internacional –global– (Sánchez, 2009d).

3.6.5 La coordinación y ejecución de acciones

Pero los terroristas no solo emplean la red para comunicarse, sino también para coordinarse y llevar a cabo sus acciones. La coordinación la consiguen mediante una comunicación fluida a través de Internet, y la ejecución puede implicar desde un ataque lo suficientemente destructivo como para generar un temor comparable al de los actos físicos de terrorismo como cualquier otro tipo de actividades que repercuten de manera diferente en la población, pero que son igual de efectivas, como pueden ser el envío masivo de email o la difusión de un virus por toda la red. Para ello, por ejemplo, utilizan una red de ordenadores controlados como zombies. Esto consiste, para explicarlo de forma sencilla, en que los *botnets* están compuestos por ordenadores convencionales sobre los que la gente ha perdido parcialmente el control. Los usuarios nos saben que hay un software malicioso ejecutándose en su ordenador, y al estar conectados a Internet pueden recibir y enviar información de quienes operan en la *botnet*. El procedimiento es fácil: primero, el operador de la *botnet* manda un virus o un gusano a los usuarios; segundo, los PC entran en el IRC o se usa otro medio de comunicación; tercero, el *spammer* le compra acceso al operador de la *botnet*; cuarto, el *spammer* manda instrucciones vía servidor de IRC u otro canal de los PC infectados; quinto, causando que éstos envíen spam al servidor de los correos. En todo caso, tal es el atractivo que presenta para los terroristas, que incluso se ha llegado a hablar que Al Qaeda poseía en Pakistán un campo de entrenamiento destinado únicamente a la formación de miembros operativos en cuestiones de penetración de sistemas informáticos y técnicas de guerra cibernética (Sánchez, 2010a).

3.6.6 Las fuentes de información y entrenamiento

Otro papel que juega Internet para el terrorismo es el ser una fuente inagotable de documentación. La red ofrece por sí sola cerca de mil millones de páginas de información, gran parte de ellas libres y de sumo interés para los grupos terroristas, ya que éstos pueden aprender una variedad de detalles acerca de sus posibles objetivos (mapas, horarios, detalles precisos sobre su funcionamiento, fotografías, visitas virtuales, etc.), la creación de armas y bombas, las estrategias de acción, etc. Los

terroristas, al igual que muchos otros usuarios de Internet, no sólo tienen acceso a mapas y esquemas de los posibles objetivos, sino también a los datos e imágenes de los mismos, a los horarios de apertura y de cierre, e incluso en algunos casos pueden realizar visitas virtuales (Sánchez, 2009d).

Pero, además, en la World Wide Web hay decenas de sitios en los que se distribuyen manuales operativos donde se explica cómo construir armas químicas y bombas, cómo huir, qué hacer en caso de detención policial, cómo realizar secuestros, o documentos críticos en los que se intenta extraer lecciones para el futuro de conflictos pasados. Evidentemente, este tipo de documentos no sustituyen el adiestramiento en la vida real, pero en casos concretos pueden ser de gran utilidad. Por ejemplo, los terroristas de los atentados de Londres, el 7 de julio de 2005, fabricaron los explosivos con fórmulas obtenidas a través de Internet (Sánchez, 2009d).

3.6.7. La propaganda y adoctrinamiento

Internet abre enormemente el abanico para que los grupos puedan publicitar todo lo que deseen, ya que antes de la llegada de esta herramienta, las esperanzas de conseguir publicidad para sus causas y acciones dependían de lograr la atención de la televisión, la radio y la prensa. Además, el hecho de que muchos terroristas tengan un control directo sobre el contenido de sus mensajes ofrece nuevas oportunidades para dar forma a la manera en que sean percibidos por distintos tipos de destinatarios, además de poder manipular su propia imagen y la de sus enemigos (Sánchez, 2009d).

De esta manera, la propaganda de los grupos catalogados como "terroristas" se ha hecho común en Internet. En la red se puede encontrar webs del Ejército Republicano Irlandés (IRA), Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Sendero Luminoso, ETA, el Hezbollah, y hasta del Ku Klux Klan, etc. Por ejemplo, el uso que hacía el IRA de Internet solía ser discreto, evitando cualquier manifiesto que hiciera referencia a la lucha directa. Es más, no han tenido sitios ni publicaciones oficiales, su

presencia en Internet ha sido básicamente a través de su brazo político, el Sinn Fein. Otro ejemplo es el de las FARC que colgaron una página que funcionaban en seis idiomas (español, inglés, francés, italiano, alemán y portugués) para facilitar el intercambio de informaciones. En dicha página web se podía leer los partes de guerra desde 1997, poemas escritos por guerrilleros, una revista online, un programa de radio y mensajes dirigidos a captar la atención de los jóvenes colombianos. El grupo Hizbollah, por ejemplo, ha disfrutado de tres réplicas a fin de que si una era clausurada, se pudiera acceder a las demás (www.hizbollah.org; www.hizballah.org; y www.hizbollah.tv). Estos sitios estaban escritos en árabe pero con una versión en inglés, y en ellos se ofrecían una amplia garantía de fotos, archivos de audio y video con discursos propagandísticos.

Así, las nuevas tecnologías, y en particular Internet, han abierto un nuevo panorama en la estrategia comunicativa de los grupos terroristas e yihadistas, ya que gracias a ellas pueden burlar las restricciones que les imponían los tradicionales medios de comunicación y así llegar a un mayor público objetivo. Téngase en cuenta que antes de Internet la única información que nos llegaba sobre las actividades terroristas era la que nos facilitaban los medios de comunicación, y ésta siempre estaba condicionada por la propia política que a este respecto mantenían los grupos mediáticos. Así, en muchos de los casos, los videos y documentos que los grupos terroristas facilitaban a los medios para su difusión eran ignorados o cuando eran publicados eran recortados y retocados. Por no mencionar el riesgo que suponía para los propios terroristas hacer llegar sus misivas a los medios de comunicación. Recuérdese que, por ejemplo, Al Qaeda empleaba una complicada red de mensajería para distribuir sus comunicados. Normalmente, antes del que el medio en concreto recibiera el material, está había recorrido cientos de kilómetros, utilizándose para ello una multitud de portadores para evitar su localización e intercepción. Pero pese a todo, y aún a sabiendas que los medios distorsionan sus noticias, existe una relación de dependencia dado que los grupos terroristas son conscientes del enorme poder de los medios a la hora de concitar la atención de la sociedad en sus mensajes. Más, cuando hasta ese momento era la única forma de garantizar una elevada cuota de intimidación y potenciación de sus convicciones

ideológicas y la fidelidad de los miembros del grupo. No obviemos que la publicidad del acto terrorista es uno de los componentes capitales, eficientes e irrenunciables de la guerra psicológica, pero sobre todo para promover su longevidad y asegurar su propia supervivencia. Téngase en cuenta, que sin una estrategia de comunicación efectiva, un movimiento terrorista sería incapaz de motivar e inspirar a los miembros existentes, o de atraer a nuevos partidarios o simpatizantes (Hoffman, 2007, p. 4) (Sánchez, 2010a).

Pero con la irrupción de las nuevas tecnologías e Internet, las cosas han cambiado de forma sustancial, ya que los grupos terroristas no sólo han podido incrementar la calidad de sus materiales, sino que además les ha permitido evadir la intermediación de todos aquellos actores que ejercían de filtradores de sus mensajes. Los medios de comunicación de masas han perdido así su posición de preeminencia a la hora de seleccionar el tipo de materiales que serían conocidos por la sociedad. Todo porque la red permite establecer un contacto directo y sin censuras entre el difusor y un público potencialmente ilimitado. Además, el abaratamiento, fácil manejo y disponibilidad de los modernos medios de filmación y distribución *on line* de imágenes hace posible que cualquiera pueda realizar su particular contribución al relato del conflicto. De esta manera, la red está contribuyendo a eliminar la asimetría informativa, ya que cualquier grupo armado, por débil que sea, tiene la capacidad de generar la información que quiere ofrecer en cada momento, casi de manera inmediata (Sánchez, 2010a).

Ahora son ellos mismos, los que elaboran, editan y difunden sus materiales sin restricciones y en el momento que quieren. Para ello, han desarrollado toda una red de ciberactivistas que colaboran con la organización en tales menesteres, pero además han creado toda una infraestructura al servicio de la propagada del grupo como, por ejemplo, "Frente Mediático Islámico Global" de Al Qaeda o "Al Hayat Mediacenter" del Estado Islámico. Detrás de dichas siglas encontramos a personas que han concebido su aportación a la yihad como la puesta a disposición del movimiento de sus conocimientos informáticos, habilidades lingüísticas o su creatividad. Se trata de una nueva generación de terroristas a "tiempo parcial", capaces de conjugar un intenso compromiso con la yihad

global, con una actividad profesional y una vida social perfectamente "normal" (Torres Soriano, 2009c). Esto les está permitiendo cuidar su imagen y elaborar más detalladamente su mensaje según la finalidad que se pretende alcanzar. Pero también algunos de los archivos audiovisuales de sus operaciones son grabados por teléfonos móviles de última generación y enviados instantáneamente a través de un mensaje multimedia a la persona encargada de distribuir material en la red. Así, en las células es tan importante la persona que aprieta el gatillo como el de cámara que trata de obtener una imagen nítida del evento. La difusión de este tipo de grabaciones les ha permitido crear en la opinión pública una imagen de sus capacidades muy por encima de la real (Johnson, 2007) (Sánchez, 2010a).

No olvidemos, que los mensajes de los grupos terroristas no solo están destinados a sus partidarios y simpatizantes, sino que en ocasiones también pretenden minar la moral de sus enemigos, deslegitimar a los gobiernos que emprenden acciones contra ellos, transferir la culpabilidad, explotar las divisiones internas del enemigo, y romper con la unidad de acción de los países occidentales. Ya que de todos es conocido que hoy en día la información convertida en propaganda, tanto defensiva como ofensiva, resulta ser un recurso esencial para lograr erosionar la moral de combate del oponente. Además, la red está colaborando a que los grupos terroristas puedan llevar su mensaje más allá de sus propias fronteras y de sus seguidores y simpatizantes, y por tanto, contribuyendo a consolidar y potenciar el poder del grupo y su causa (Sánchez, 2010a).

Los grupos terroristas difunden una multitud de información por la red, que va desde videos, comunicados, fotografías, archivos de audio, logotipos, biografías de sus líderes y mártires, relatos de momentos importantes de su historia, recomendaciones de seguridad, hasta todo tipo de links. Por tanto, se puede hablar de tres tipos de materiales: los destinados a los seguidores o miembros del grupo y a la causa, a los simpatizantes y seguidores que no mantienen ningún tipo de vínculo directo con la organización, y a los adversarios. No obviemos, que la guerra psicológica siempre ha sido un elemento crucial en las cruzadas de los grupos terroristas. Por eso, la propaganda de guerra se dirige, en primer lugar, a la propia vanguardia para sostener la moral combatiente; luego,

a la propia retaguardia que nutre de hombres y pertrechos a la vanguardia; también a los neutrales para impedir que se alíen con el enemigo, para mantenerlos en su posición equidistante o para atraerlos hacia la causa; se dirige asimismo hacia al enemigo, tanto a su vanguardia como a su retaguardia (Pizarroso, 2008: 51). De ahí, que la finalidad de los mensajes de los grupos terroristas, más en concreto de los yihadistas, sea:

a. Trasmitir la idea de que la victoria del enemigo es inalcanzable. Así, los mensajes de los grupos yihadistas tratan de lograr que la población enemiga interiorice la idea de que es imposible "la victoria sobre el Islam" (Torres Soriano 2009a, 234). Por ello, suelen negar los reverses sufridos, como una estrategia de mantener su imagen de invulnerabilidad. Por eso, es frecuente que nieguen abiertamente la muerte o detención de algunos de sus miembros, o incluso dejen de hacer referencia a ellos, como si nunca hubieran existido. Al mismo tiempo que se dedican a ensalzar y magnificar sus victorias, como una forma no sólo de minar la moral del enemigo sino también de la de incrementar la de sus seguidores (Sánchez, 2010a).

b. Deslegitimar a los gobernantes y las motivaciones que llevaron a emprender acciones contra ellos. De ahí, que su acción propagandística vaya dirigida a denunciar los que ellos consideran los verdaderos motivos que han llevado a estos gobernantes a iniciar todo tipo de acciones para acabar con ellos. Con ello, no sólo intenta desprestigiar a la clase política de estos países sino romper su unidad y fomentar la división. Por ejemplo, en un video difundido el 5 de mayo de 2007, Ayman Al Zawahiri hablaba con un entrevistador anónimo sobre la composición racial de las tropas norteamericanas. En la misma, vino a decir que estaba dolido cuando veía a un negro americano luchando contra los musulmanes bajo la bandera americana, y de esta manera se preguntaba porque luchaban contra ellos cuando el régimen racista americano les perseguía a los dos (Sánchez, 2010a).

c. Transferir la culpabilidad. Así, la acción comunicativa está condicionada por la búsqueda de un efecto psicológico denominado

"transferencia de culpabilidad" (Tugwell, 1985), que se produce cuando la víctima de un atentado o la sociedad trasladan su responsabilidad de ese crimen hacia un actor diferente al que llevó a cabo dicha acción violenta. Así, ocurrió, por ejemplo, en el asesinato de Kenneth Bigley cuando sus familiares no dudaron en pedir al Primer Ministro, Tony Blair, que cediese ante la demanda de sus captores, o cuando su hermano tras conocerse la noticia de su asesinato declaraba: "Por favor, parad la guerra y evitad que se pierdan otras vidas. Esto es ilegal. Hay que pararlo. Blair tiene las manos manchadas de sangre" (Torres Soriano 2009a, 243) (Sánchez, 2010a).

d. Generar un clima de alerta permanente que provoque una psicosis generalizada. Por ello, inundan la red de videos particularmente espectaculares o crueles, o de mensajes amenazantes o sobre posibles atentados, para obtener una repercusión mediática que no haga otra cosa que incrementar la sensación de vulnerabilidad de los países occidentales (Sánchez, 2010a).

e. Radicalizar a sus seguidores y reclutar nuevos simpatizantes. Para ello, se han dedicado a difundir, burlando los controles de los Estados, todo tipo de materiales sobre los ataques y atrocidades que están padeciendo los musulmanes, por ejemplo, en Irak o Palestina (Sánchez, 2010a).

La importancia de Internet es indudable. Téngase en cuenta, que muchos individuos utilizan la red para informarse sobre el Islam, en todas las variantes e interpretaciones, así como un lugar para encontrar *online* a otros individuos que se encuentran en la misma situación (Caño Paños, 2008: 81). Es evidente que aquel sujeto inmerso en la búsqueda de "respuestas" a las cuestiones vitales que se plantea, se ve invariablemente expuesto a una plétora de interpretaciones del Islam de carácter extremista a las que puede tener acceso a través de Internet (Caño Paños, 2008: 81). Así, la red está haciendo posible que muchos sujetos que residen en occidente se estén adscribiendo a la causa islamista. Esto explica que la mayoría de los "nuevos" terroristas adscritos al islamismo radical son sujetos que, bien nacieron en Occidente (Mohammed

Sidique Khan), bien se trasladaron siendo niños (Jamal Zougam), bien acudieron a universidades occidentales con la intención de recibir una mejor formación académica (Mohammed Atta), o bien se convirtieron al Islam tras desarrollar un modo de vida plenamente occidentalizado (Jermaine Lindsay) (Caño Paños, 2008, p. 69).

Así este tipo de información se puede encontrar a través distintos métodos. Por ejemplo, a través de los blogs yihadistas. En Francia uno de los foros islamistas más activos es Ansar Al-Haqq. En él se puede encontrar noticias del frente afgano, vídeos de la compañía mediática de Al-Qaeda Al-Sahaba y del FIMG, etc. Otro foro es Nida Al-Tawhid, en este se aclara que se reconoce las leyes de la Sharia islámico, en lugar del Estado francés. Además, en el mismo se destaca enlaces a documentos de jeques contemporáneos tales como Abu Muhammad Al-Maqdisi y Abu Qatada Al Filastini, y a textos de Ibn Taymiyya. Pero también a través de las revistas *online*. Por ejemplo, en la red se puede encontrar revistas electrónicas yihadistas en inglés, como Inspire e InFight, o en árabe, inglés y francés como Dabiq. Este simple detalle indica que estas revistas no están dirigidas a un público islámico que usaría mayoritariamente el árabe si no a un público occidental. Sus artículos se ilustran principalmente con material de agencias de prensa y suelen seleccionarse por su impacto psicológico, imágenes de blindados destruidos por artefactos explosivos o entierros de soldados de la OTAN son recurrentes en sus páginas.

Pero en la relación de los grupos terroristas con el ciberespacio no es tan idílica como parece. La red está llena de presuntas vulnerabilidades para la difusión del mensaje terrorista e yihadistas. Por ejemplo, es cierto, que Internet brinda un canal perfecto de comunicación para los terroristas, pero no siempre es así, por ejemplo, en los regímenes dictatoriales o aquellos en los que el Estado ejerce un excesivo control sobre su población, se combina el escaso respeto por el secreto de las comunicaciones, con el más hiriente subdesarrollo material. Lo que indudablemente induce a que una buena parte de esa población que *a priori* podría consumir este tipo de información se retraiga de hacerlo, ante el control de los canales de comunicación, y por tanto, de su pérdida de anonimato. Además, hay que tener en cuenta otro hecho, cada vez más se están desarrollando programas que pueden ser introducidos en un ordenador

sin ser detectados, permitiendo al controlador monitorizar todo su tráfico de datos. Por no hablar de los constantes ataques cibernéticos que sufren las webs de este tipo de grupos para conseguir inutilizarlas, por lo menos, hasta que es reubicada en otro espacio, o la cantidad de páginas que están surgiendo "presuntamente" en defensa de este tipo de causas, pero realmente se tratan de web tapaderas de los servicios de inteligencia, o el incremento de medidas que caminan hacia una mayor capacidad de control del ciberespacio por parte de los servicios de inteligencia, o la creación, de multitud, de unidades especializadas en la lucha en el ciberespacio, o el establecimiento de mecanismos de colaboración entre los Estados y su infraestructuras críticas, o la adaptación de las regulaciones y las legislaciones a los nuevos problemas del ciberespacio, etc.

3.7 Ataques cibernéticos que no ciberguerra

Hoy en día todavía no ha habido ningún ataque que nos permita hablar de ciberguerra propiamente dicha, 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 o cibersoldados, 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, 2008a: 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 se presenta sobre algunos de los miles de ataques cibernéticos que se han producido en los últimos años (Sánchez, 2010c).

Tabla 1. *Ejemplos de conflictos cibernéticos*

Década de 1980
• La National Security Agency (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 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 a la 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 6 millones de dólares.
Década de 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 informáticos de la policía secreta iraquí. Además, según el Pentágono, un grupo de hackers holandeses se ofreció a Saddam 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 lanzando un "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 los 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 GPS y redes informáticas del Pentágono. El presunto terrorista Khalid Ibrahim, del grupo separatista indio Harkat-ul-Ansar, intentó contactar con uno de ellos por IRC 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 croata fue 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 2000

- La ciudad de New 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 por ciento 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 Hamas 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 (DDoS). Hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallin de un monumento de la época soviética. 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 los 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 ataque del gusano "Nimda" en septiembre de 2001, se propagó en una hora por EE.UU, probando diversas formas de infectar los sistemas que invadía hasta lograr el acceso o la destrucción de archivos.

- Tras el hackeo de Ashley Madison más de 37 millones de clientes, casados y adúlteros, al descubierto y sus datos personales y financieros fueron expuestos.

- 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 India, el Centro Nacional de Informática (NIC) 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 "hackeo" 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.

- El ataque a Irán a los sistemas industriales. Stuxnet es un programa de software dañino del tipo troyano muy avanzado, que aprovecha la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC, empleados en los sistemas SCADA (*Supervisory Control and Data Acquisition*) fabricados por Siemens y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Se piensa que una vez dentro de una planta podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara. El troyano queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo. Este tipo de troyanos no van destinados a la infección masiva de ordenadores domésticos sino que está pensado para atacar a infraestructuras críticas o incluso sabotajes industriales, donde puede aumentar o disminuir el caudal de un oleoducto o dañar a una central nuclear.

- Los ataques que están protagonizando el grupo Lulzsec y Anonymous, contra la página de la CIA, Sony, PayPal, Bankia, ENEL, y de los gobiernos de Argelia, Libia, Irán, Chile, Colombia, Nueva Zelanda, etc.

- La creación del virus Flame, un virus diseñado para recopilar información sensible y presente en ordenadores de Irán, Oriente Próximo, e incluso EE.UU.

- El ciberataque yihadista que sufrió la segunda cadena de televisión del mundo en difusión, TV5Monde.

- El robo de 5 millones de dólares en bitcoins que sufrió Bitstamp, el tercer intercambiador de la divisa virtual a nivel mundial. La brecha de seguridad de su sistema produjo la sustracción de 19.000 bitcoins y obligo la suspensión del servicio durante 24 horas.

- Los ataques de ransomware secuestraron información de compañías y exigían dinero para liberar la información. Este ataque cibernético afecto a miles de ordenadores de las principales compañías y hospitales en países como Reino Unido, Estados Unidos, Rusia, Italia, Vietnam, China, España, Colombia y Taiwán. Los ataques de ransomware nombrados WanaCryptor 2.0, WannaCry, WCry o WCrypt secuestraron los datos de las empresas para pedir lo equivalente a 300 dólares en bitcoins para liberar la información.

Fuente: Sánchez, 2010c.

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 se comparan con las que podría generar una verdadera guerra cibernética. Incluso el 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. Pero tampoco se puede considerar ciberguerra el ataque que han experimentado

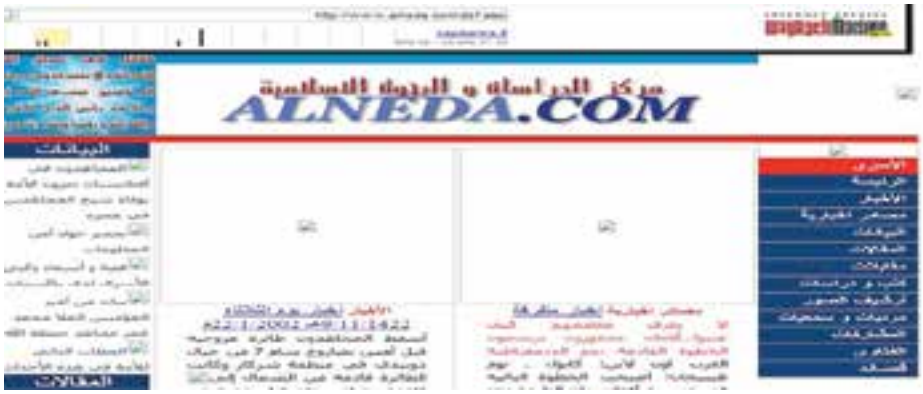
un buen número de países en el 2017, que implicaba el robo y bloque de información hasta que no se pagara 300 bitcoins para liberarlo.

3.8 El ciberterrorismo en el internet profundo

Hay una parte de internet que no es accesible a los motores de búsqueda tradicionales, es normalmente los que se denomina "internet profundo o invisible". Se trata, pues, de todo el contenido inaccesible desde los buscadores tradicionales por diferentes motivos, como tratarse de páginas y sitios web protegidos con contraseña, documentos en formatos no reconocibles o contenidos que requieren interrogar a su base de datos para poder acceder a la información. Los motivos por los que no toda la información está disponible en los buscadores ordinarios son: 1) hay sitios web que no permiten que los robots de los buscadores accedan a sus páginas o para acceder a ellas se necesita algún tipo de credencial, 2) hay información almacenada y accesible, pero está cifrada solo para que ciertos usuarios puedan interpretarla, con lo cual su información no puede ser catalogado, 3) las redes de intercambio P2P no permiten hacer un catálogo centralizado y único de información, 4) para garantizar el anonimato de la interconexión de las redes se hizo necesario que las comunicaciones no fueran accesibles para que cualquiera pudiera interceptarlas en tránsito, esto obligo a que existiera un servicio de consulta de documentos privados.

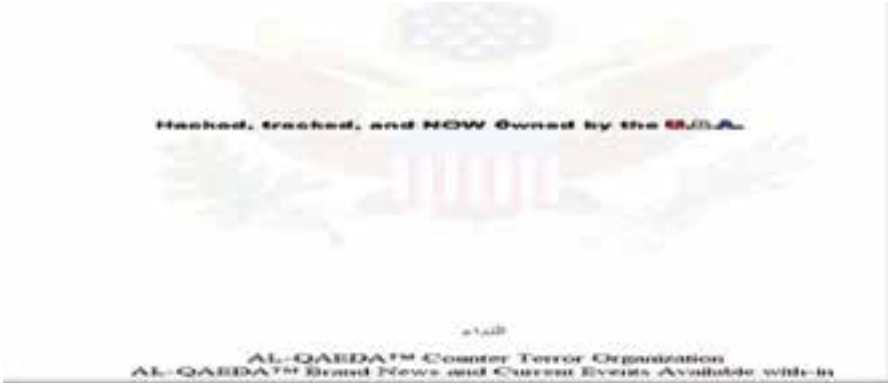
Se estima que el tamaño del internet profunda es de 500 veces más a la web superficial, esto significa que los buscadores tradicionales no rastrean el 99% del contenido de internet. En el Internet profundo puede encontrarse información que es válida para sistematizar en una base de datos (p. ej. directorios telefónicos, archivos gráficos, multimedia, etc), información que es nueva y cambia constantemente, sitios de compañías e instituciones, páginas internas de sitios muy grandes que son creadas dinámicamente, además de todo un mundo de actividades que ilícitas que buscan el anonimato. De ahí que se haya convertido en lugar ideal para realizar todo tipo de actividades criminales. Tal es así, que según el informe de Trend Micro llamado "Below the Surface: Exploring the Deep Web", más del 25% de vínculos entre la Internet oculta y visible tienen fines de explotación infantil, o por ejemplo, las ofertas de 180.000

dólares que se pueden encontrar por asesinar a una personalidad o político. Por tal motivo, los ciberterroristas también han encontrado en este internet profundo un lugar para seguir realizando sus actividades en la red. Así, por ejemplo, en las bibliotecas, que son aquellas webs que se dedican a archivar páginas antiguas y que dejan de estar por tanto en circulación, se puede hallar la que fue la web oficial de Al Qaeda (www.alnelda.com):



Fuente: http://web.archive.org/web/20020129223155/http://alneda.com/. Consultada el 22 de agosto de 2015.

En wcambio, si se consulta el internet superficial la web que aparece ahora:



Fuente: www.alnelda.com, consultada el 22 de agosto de 2015.

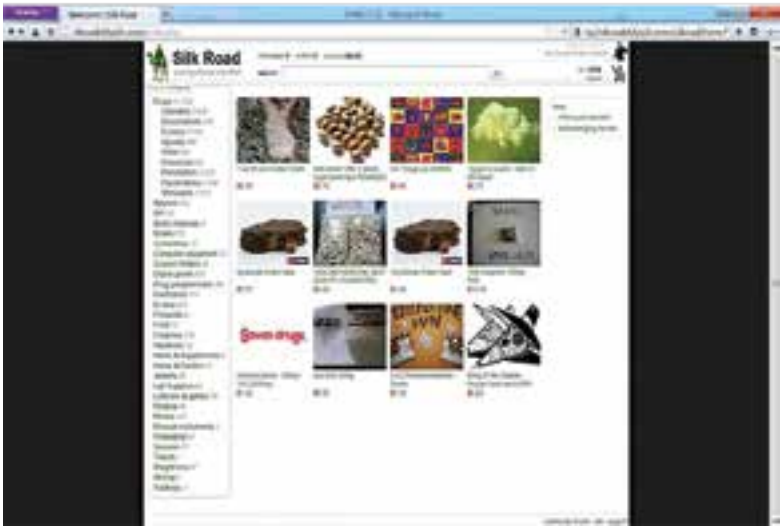
Por lo tanto, el éxito de cerrar webs de grupos terroristas es relativo, ya que siendo un usuario medianamente avanzando en internet no sólo se pueda consultar información nueva sino que se puede examinar el contenido antiguo.

Son varias las redes ocultas implementadas. Por ejemplo, en el año 2000 surgió Freenet, con el objetivo de vencer la censura y proporcionar el anonimato en las comunicaciones. Esta red se basa en la tecnología P2P, y se dedica a almacenar trozos de información en los equipos de los usuarios que participan en la red. Cuando se necesita recuperar algún documento, se debe encontrar los trozos sueltos guardados en los diversos equipos. Esta transferencia se realiza de manera cifrada, y se efectúa de dos maneras: se puede intercambiar información con cualquier otro nodo conectado a Freenet, o bien se puede trabajar en modo de alta seguridad solo con aquellos que se hayan añadido anteriormente como nodos de confianza.

Además, el internet profundo también permite navegar de forma anónima en las llamadas redes privadas virtuales (VPN). Las más populares son TOR y I2P. La primera se desarrolló con el fin de proteger las comunicaciones gubernamentales, y para ello, se ocultaba la verdadera IP del ordenador, impidiendo que la ubicación del usuario sea localizada. Además, con este servidor se puede eludir la censura, ya que tiene una opción para ayudar a los usuarios ubicados en países que tienen un acceso restringido a internet que se liberen de su vigilancia en la red. Dado que cuando se quiere realizar algún tráfico de manera anónima, la persona debe elegir 3 nodos de la red para que se establezca un circuito o túnel virtual, y a partir de entonces toda la información se cifra 3 veces consecutivamente, uno para cada nodo. Cuando llega la información al primer nodo, éste descifra lo recibido (que se cifró con la clave pública de este primer nodo), comprueba cuál es el siguiente nodo del túnel y le envía la información. El segundo nodo la recibe, realiza la misma operación de descifrado con su clave privada, y retransmite lo que corresponde al tercer y último nodo; éste vuelve a descifrar con su clave privada y envía ya la información a Internet. Para el usuario todas estas operaciones están ocultas, y no es necesario ni siquiera saber que se realizan, pues basta con instalar un software de manejo bastante sencillo.

La segunda surge como alternativa a la red TOR y está pensada para proteger la comunicación de seguimiento de las redes de vigilancia y la monotorización por terceras partes como los ISPs (proveedores de internet). En concreto, surge en 2002 y se basa en comunicaciones cifradas y distribución P2P de información. En su funcionamiento habitual se establecen túneles entrantes y salientes por los que circula la información sometida a cuatro capas de cifrado, y los extremos de las comunicaciones se identifican mediante sus claves públicas, de tal manera que ningún nodo puede conocer el remitente o el destinatario reales de las comunicaciones (Sánchez, 2015).

El anonimato ofrece una protección extra para todo tipo de actividades delictivas, por eso plataformas ilegales como "Silk Road Reloaded", conocido como mercado negro, se están valiendo de estos métodos para desarrollar su actividad comercial legal e ilegal (Sánchez, 2015).



Fuente: http://silkroadvb5piz3r.onion/silkroad/home

De esta manera, el anonimato supone una ventaja para la realización de actividades delictivas (violación de la propiedad intelectual, spam, ciberacoso, estaba, robo de identidad, etc), sino también para el

encubrimiento de actividades terroristas como filtrados de información, actividades de inteligencia en fuentes abiertas, acciones de propaganda, comprar de material, ciberguerra, etc (De Salvador Carrasco, 2012: 2) (Sánchez, 2015).

3.9 Medidas de contención de los ciberataques

Antes de nada hay que advertir que no existe ninguna tecnología capaz de hacer una red completamente segura. Una forma de reducir la exposición de pérdidas, robos, colapso, rupturas, de los ciberataques es apagar el ordenador. Pero como eso parece más que improbable, o mejor dicho imposible. De ahí, que lo primero que deberían hacer los países es incrementar la concienciación sobre el entendimiento y naturaleza de las infraestructuras de información crítica. En este sentido, los Estados deberán analizar sus infraestructuras y las dependencias entre las mismas para mejorar sus estrategias de coordinación y protección; crear organismos y sistemas de seguridad nacionales; promover alianzas entre el gobierno, el sector privado y público para analizar las infraestructuras críticas, con el objetivo de prevenir, investigar y responder a los daños o ataques en la misma; analizar la vulnerabilidades de las infraestructuras, y averiguar qué tipos de amenazas o incidentes pueden producirse en las mismas; crear y mantener redes de notificación y comunicación ante la crisis y probarlas con frecuencia para intentar generar una cultura de prevención y acción segura y estable en este tipo de situaciones; desarrollar ejercicios y entrenamientos para mejorar su capacidad de respuesta, y así probar los plantes de continuidad y contingencia, etc. Pero al mismo tiempo es necesario impulsar una cultural de sensibilización de ciberseguridad en la población. Más cuando según datos de la ONU sólo el 1% de los delitos cibernéticos son denunciados a la policía.

Los países deben también promover la cooperación internacional, cuando sea aprobado, ya que unos pueden aprender de otros en función de sus respectivas experiencias. En este mismo sentido, los países deben impulsar el desarrollo y la coordinación de sistemas de emergencias, compartir y analizar información relacionada con vulnerabilidades, amenazas e incidentes y coordinación de investigaciones de ataques sobre las infraestructuras de acuerdo con las regulaciones y leyes

vigentes, o facilitar el seguimiento de los ataques a las infraestructuras críticas, considerando la revelación de la información requerida a otras naciones, etc. Ya que el intercambio de información sobre incidentes es fundamental. El problema es que existen grandes dificultades para conseguirlo, dado el miedo que existe a la hora de intercambiar datos confidenciales, privados o potencialmente comprometedores (Maroto, 2009: 57). De ahí, que sea necesario crear organismos de ámbito internacional de vigilancia y alarma, en la que participen el mayor número de Estados para facilitar la cooperación y el intercambio de información, y promover una "cultura de seguridad global".

Los países deben promover la investigación y desarrollo a nivel nacional e internacional, así como impulsar la aplicación de tecnologías de seguridad que se encuentren alineadas con las mejores prácticas y estándares internacionales. Además, es necesario intentar acabar con los sitios web y foros relacionados con los grupos insurgentes y terroristas, la supresión de sus cuentas de correo electrónico, la eliminación de todo el contenido insurgente que exista en otros sitios web, etc. Asimismo, los Estados tendrán que infiltrarse en sus foros y en su organización, para averiguar sus intenciones y generar confusión en las mismas para erosionar la confianza en un grupo o líder, que disuada a los posibles nuevos reclutas. Por otra parte, como la mayoría de las vulnerabilidades de seguridad se pueden mitigar a través de buenas prácticas de seguridad, y éstas no sólo consisten en hacer referencia a 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. Y esto requiere no sólo invertir en programas y software, sino también en formación para el personal, es necesario contar con un equipo de personas expertas en este tipo de cuestiones, para que no se cometa un fallo en los sistemas de seguridad.

Los países deben favorecer la tipificación de gran cantidad y variedad de delitos informáticos. En España, por ejemplo, está tipificado como delitos, el ataque a datos y a redes, así como la intercepción de datos. Además son castigados penalmente: la modificación, el borrado, la destrucción o la alteración y el acceso no autorizado a bases de datos, textos o programas mediante el *cracking* y la diseminación de virus. En México,

las leyes federales prevén varios tipos, de los cuales pueden relacionarse con el ciberterrorismo: la modificación, el conocimiento de información, la eliminación, destrucción, borrado o inutilización de datos o la provocación de pérdida de los mismos. En Venezuela, la Ley Especial contra los Delitos Informáticos (2001) establece que dependiendo de su origen, motivación y fin pueden clasificarse como ciberterrorismo: la inutilización de sistemas, la creación, la introducción o la transmisión, por cualquier medio, virus o programas análogos; y el acceso indebido o el sabotaje a sistemas protegidos por medidas de seguridad o destinados a funciones públicas o que contengan información personal o patrimonial de personas naturales o jurídicas. En EE.UU. la legislación federal, de fecha 15 de abril de 2002, establece penas para: el acceso no autorizado de sistemas informáticos, previendo específicamente el acceso a sistemas del gobierno relacionados con la seguridad de Estado, por lo que se encuentra castigada la comunicación, la entrega, la transmisión e incluso el sólo intento de realizar los actos antes mencionados; el uso de cualquier computador de uso oficial o que se esté utilizando en algún momento como oficial que afecten al gobierno; y el acceso de computadoras sin la autorización, o quien tenga acceso a la misma se exceda del permiso que obtuvo (Orta Martínez, 2005). En Sudáfrica existe, desde finales del 2007, una ley destinada a proteger al país contra el ciberterrorismo. Pero la tónica habitual, como estamos viendo, no es así (Sánchez, 2009d).

La mayoría de las legislaciones de los diferentes países están dirigidas a proteger básicamente la utilización indebida de la red, incluso algunas de ellas prevén la creación de órganos especializados que protejan los derechos de los ciudadanos, pero poco más. No obstante, los ministros de Justicia e Interior de los 27 países de la Unión Europea expresaron, el 7 de diciembre de 2007, su amplio apoyo al proyecto de penalizar el uso de Internet con fines terroristas. La propuesta, elaborada por la Comisión Europea, obligará a cada Estado a fijar sanciones penales por la distribución en Internet de propaganda terrorista, el reclutamiento de actividades y la difusión de información sobre cómo utilizar explosivos, bombas, armas y sustancias tóxicas para la realización de atentados terroristas (Sánchez, 2009d).