Prof. Gema Sánchez Medero. Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. xxi. 239-267. Revista Cenipec. 31. 2012. Enero-Diciembre. ISSN: 0798-9202

Prof. Gema Sánchez Medero

Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. xxi

Recepción: 06/03/2011. **Aceptación:** 01/03/2012.

Prof. Gema Sánchez Medero
UNIVERSIDAD COMPLUTENSE DE MADRID
MADRID - ESPAÑA
gsmedero@cps.ucm.es

Resumen

La enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos está haciendo que éstas sean más vulnerables a los posibles ataques cibernéticos. Además, Internet es un medio de fácil acceso, donde cualquier persona, guardando su anonimato, puede proceder a realizar una acción difícil de asociar, virtualmente indetectable y difícil de contrabandear. Por tal motivo, en este artículo hemos analizado el uso que están haciendo de la red, los terroristas, los delincuentes y los servicios de seguridad de los Estados, y las medidas se están adoptando para evitar en la medida de lo posible estos ataques y actividades delictivas.

Palabras clave: internet, ciberataques, ciberseguridad, red, web.

Cyber-crime, cyber-terrorism and cyber-war: the new challenges of the twenty first century

Abstract

The Occidental Societies are becoming more vulnerable by the possible cybernetic attacks because of their large dependency on Computer and Electronics Systems. Moreover, Internet is an easily accessible, where any person, keeping your anonymity, you may proceed to perform a difficult act of linking virtually undetectable and difficult to smuggle. Therefore, in this article we discussed the use of the network are doing, terrorists, criminals and the security of states, and the measures being taken to avoid as far as possible these attacks and activities crime.

Keywords: internet, cyberattacks, cybersecurity, network, web.

Cyber-crime, cyber-terrorisme et cyber-guerre: les nouveaux défis du XXIe siècle

Résumé

L'énorme dépendance que les sociétés occidentales éprouvent vis-à-vis des systèmes informatiques et électroniques les rend en retour plus vulnérables à des possibles attaques cybernétiques et à la fraude à travers le net. De plus, internet offre des possibilités d'accès faciles et les moyens pour que quelconque réalise une action difficilement associable, relevant toute possibilité d'identification virtuelle et pouvant difficilement faire l'objet de contrebande. Par conséquent, nous avons analysé dans cet article, l'utilisation que font les délinquants, voire les terroristes. Parallèlement, nous analysons les mesures adoptées par les appareils de sécurité des États qui pour éviter tant que faire se peut ces attaques et ces activités délictuelles.

Mots clés: terrorisme, internet, cyber-attaques, net, web.

Cibercrime, ciberterrorismo e ciberguerra: Os novos desafios do século XXI

Resumo

A enorme dependência das sociedades ocidentais a sistemas informáticos e eletrônicos as tornam mais vulneráveis a possíveis ataques cibernéticos e a fraude na rede. Além disto, a Internet é um meio de fácil acesso, onde qualquer um, anonimamente, pode realizar uma ação difícil de associar, virtualmente indetectável e difícil de contrabandear. Por tal motivo, tem-se analisado neste artigo o uso que estão fazendo da rede, os terroristas, os delinqüentes e os serviços de segurança dos Estados, e as medidas que estão adotando para evitar na medida do possível estes ataques e atividades delitivas.

***Palavras chave*:** internet, ciberataques, cibersegurança, rede, web.

1.- Introducción

Las TIC (Tecnología de la Información y el Conocimiento) está generando una revolución sin precedentes, ya que el ciberespacio se está convirtiendo en un punto de encuentro para millones de personas, gracias a su flexibilidad en el uso y a la gran cantidad de información que se está poniendo a disposición de los cibernautas. Indudablemente, eso está contribuyendo a que la red esté alcanzando una enorme repercusión, hasta el punto que ya son muchos los que se atreven a afirmar que su aparición ha marcado un antes y un después en la era de la información y la comunicación. Es más, hoy en día todo parece estar interconectado, los sistemas de seguridad, defensa, comerciales, energéticos, sanitarios, comunicación, transporte, bancarios, alumbramiento, bibliotecarios, etc. De tal manera que nos encontramos ante un mundo hiperconectado, donde la red es un elemento crucial y vital para las sociedades más avanzadas, aunque en realidad es para todos aquellos que se hayan incorporado al tren de la era digital.

Pero no todo es positivo, dado que el ciberespacio también está favoreciendo la aparición de nuevos problemas y amenazas a las que se van a tener que hacer frente. Tal es así, que cada vez está siendo más frecuente que salgan a la luz noticias sobre algún hecho ilícito que se ha producido en Internet. El problema es que aún no se ha valorado el verdadero alcance del problema. Y todavía son muchos los que consideran que un ataque cibernético es algo relacionado con la ciencia ficción, o reservado a las películas de acción. Pero la realidad parece ser otra muy distinta, aunque hasta el momento no se ha producido ninguna acción que haya afectado gravemente a los sistemas o instituciones de algún país. Aunque no cabe duda que todos podemos ser víctimas en la medida en que realizamos algún tipo de actividad usual, como podría ser adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente, usamos teléfonos con tarjetas electrónicas, utilizamos Internet, etc, y lo que es más grave podemos no saberlo. Por eso, en este artículo hemos decidido analizar que actividades están llevando a cabo en el ciberespacio, delincuentes, terroristas y Estados, para así poder determinar si éstas supondrán un nuevo desafío para la sociedad, y en caso de que fuera así, que medidas se están tomando para intentar contrarrestar estos nuevos peligros.

2.- ¿Qué es el cibercrimen, el ciberterrorismo y la ciberguerra?

El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el *computer hacking*, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad, y el crimen organizado (Rodríguez Bernal, 2007: 9). Pero a diferencia de otros tipos de delitos, el cibercrimen se vale del ciberespacio para realizar sus actividades delictivas. En cambio, el ciberterrorismo va más allá de la ciberdelincuencia, por mucho que algunos consideren que ambos son una misma cosa. Indudablemente tienen cierta vinculación, porque en muchas ocasiones los ciberterroristas desempeñan actividades delictivas en la red, pero la causa que las motivan y los beneficios que esperan unos y otros son diferentes. El ciberterrorismo es la convergencia del ciberespacio y el terrorismo, es decir, "la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos-religiosos". Por tanto, viene a ser la evolución que resulta de cambiar las armas, las bombas y los misiles por una computadora para planificar y ejecutar unos ataques que produzcan los mayores daños posibles a la población civil. Esto implica una gran diferencia respecto al cibercrimen, el ciberterrorismo busca originar el mayor daño posible por razones político-religiosas mientras que las acciones del cibercrimen están dirigidas a conseguir un beneficio principalmente económico.

La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde "la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento", etc (Colle, 2000). No obstante, para los que consideran que la *cyberwar* y la *netwar* son una misma cosa, hay que puntualizar, la ciberguerra es la utilización

de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los propios (Sánchez, 2008: 15).

En todo caso, si tuviéramos que enumerar las características de una guerra cibernética éstas serían: complejidad, asimetría, objetivos limitados, corta duración, menos daños físicos para los soldados, mayor espacio de combate y menor densidad de tropas, transparencia, lucha intensa por la superioridad de la información, aumenta la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra convencional (Thomas, 2001). Pero tal vez, de todas ellas, la más importante sea la de asimetría, porque la guerra cibernética proporciona los instrumentos necesarios para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos, sólo siendo necesario un ordenador y unos avanzados conocimientos informáticos. Más, cuando los objetivos de este tipo de guerra son: 1) Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo; 2) Interrumpir o romper el flujo de la información; 3) Destruir físicamente la información del adversario; 4) Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información, 5) Impedir al adversario acceder y utilizar los sistemas y servicios críticos; 6) Engañar a los adversarios; 7) Lograr acceder a los sistemas del enemigo y robarles información; 8) Proteger sus sistemas y restaurar los sistemas atacados; 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.

Los guerreros del ciberespacio hoy son consultores e ingenieros equipados con arsenales informáticos ajenos a la imagen convencional de los armamentos, y los encargados de combatir a los "villanos" en el escenario bélico virtual llevarán micrófonos y audífonos, computadores portátiles, sensores, etc. Sus procedimientos se asemejan bastante al de los hackers, aunque sus fines, casi siempre, son completamente distintos[1]. Lo primero que hace cualquier hacker es visitar o buscar algunos de los sitios donde hay *scripts*[2] 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 éste sitio, ya que éste puede proporcionar las "entradas" que nos permitan romper su código. La información sobre las fallas del software inmediatamente pasan a ser de conocimiento público dentro de la comunidad hacker[3], evidentemente cuando se trata de cibersoldados la información obtenida no se publicita. Así, una vez que un hacker encuentra un agujero, penetrar el sistema es sólo una cuestión de persistencia, aunque la enorme mayoría de los intentos terminan en fracaso.

3.- El uso pasivo de internet, por parte de los grupos terroristas y los Estados

Todavía no se ha producido un ataque cibernético que haya causado grandes destrozos o pérdidas humanas, es decir, ninguno que nos pueda inducir a proclamar el inicio de una verdadera ciberguerra o un ataque ciberterrorista,

[1] La comunidad hacker se ha declarado más de una vez contraria a la ciberguerra, basándose en una declaración conjunta hecha por conocidos grupos norteamericanos y europeos, a finales de 1998, donde negaron querer convertirse en "facciones paramilitares" y aseguraron que no serán ellos los que ayuden a los EE.UU a justificar, con casos reales, los fondos asignados a la infoguerra.

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

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

ya que hasta el momento, sólo se ha encontrado rastros de visitas o intentos de acceso a infraestructuras estratégicas, 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). Pero eso es precisamente un problema, ya que aún no se ha valorado el verdadero alcance de esta cuestión. Así, todavía son muchos los que consideran que un ataque cibernético es algo relacionado con la ciencia ficción, o reservado a las películas de acción. Pero la realidad parece ser otra muy distinta, aunque hasta el momento, como hemos mencionado, no se ha producido ninguna acción que haya afectado gravemente a los sistemas o instituciones de algún país. No obstante, debemos tener en cuenta que todos podemos ser víctimas en la medida en que realizamos algún tipo de actividad usual, como podría ser adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente, usamos teléfonos con tarjetas electrónicas, utilizamos Internet, etc, y lo que es más grave podemos no saberlo.

Por todo ello, podemos decir que tanto unos como otros están haciendo, de momento, un uso pasivo de la red:

3.1.- El uso de la red de los grupos terroristas

Los grupos terroristas están utilizando, principalmente, la red para financiarse, reclutar nuevos miembros, adiestrar a los integrantes de las distintas células, comunicarse, coordinar y ejecutar acciones, encontrar información, adoctrinar ideológicamente, promocionar sus organizaciones y desarrollar una guerra psicológica contra el enemigo (Weimann, 2004a).

3.1.1.- Financiación

Los grupos terroristas están empleando la red, como otras organizaciones, para financiarse. En ella han encontrado un nuevo medio para recaudar fondos para la causa. Por tal motivo, los terroristas están utilizando sus páginas web para solicitar donaciones a sus simpatizantes. Por ejemplo, el sito 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; o los terroristas chechenios han divulgado por la red el número de cuentas bancarias en las que sus simpatizantes podían hacer sus aportaciones. 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.

3.1.2.- 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 equivocas, amenazar o divulgar las imágenes de sus atentados. 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 las sociedades occidentales, pero además han cuestionado la legitimidad y los efectos de la "Operación Libertad Iraquí" (Merlos, 2006). De esta manera, los grupos están consiguiendo trasmitir una imagen interna de vigor, fortaleza y pujanza, y sus mensajes están alcanzando un impacto global (Merlos, 2006). Todo para intentar minar la moral de los EE.UU y sus aliados, y fomentar la percepción de vulnerabilidad de esas sociedades (Merlos, 2006). 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 (2003) denomina "*frustración delegada*", es decir, la rebelión ante la injusticia que sufren otras personas, pero también para levantar la moral de los combatientes.

3.1.3. 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" (Weimann, 2004b). En segundo lugar, porque los grupos terroristas cuentan con páginas web 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. Aunque es cierto que en la inmensa mayoría de los casos la captación se produce a través de lazos de amistad y de trato personal (Sageman, 2004), aunque Internet, como reconocen los propios círculos yihadistas, también está facilitando esta labor.

3.1.4.- Interconexión y 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[4], la encriptación[5] y los semáforos rojos[6]. Pero también cuelgan 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 manipulan páginas electrónicas de

[4] Permite el ocultamiento de mensajes u objetos, dentro de otros, llamados "portadores", de modo que no se perciba su existencia.

[5] Codifica o cifra una información de manera que sea ininteligible para cualquier intruso, aunque sepa de su existencia.

[6] 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.

empresas privadas u organismos internacionales para crear en ellas ficheros adjuntos con propaganda; u ocultan datos o imágenes en website de contenido pornográfico. Aunque entre todos los métodos que emplean el más creativo es el de 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 *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.

3.1.5.- Coordinación y ejecución de acciones

Pero los terroristas no sólo 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 o cualquier otra acción que repercuta de manera diferente a 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. 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.

3.1.6.- Fuente 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 ella libre 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.

3.1.7.- 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 Internet, las esperanzas de conseguir publicidad para sus causas y acciones dependían de lograr la atención de los medios de comunicación. 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, además de poder manipular su propia imagen y la de sus enemigos (Weimann, 2004a). De esta manera, la propaganda de los grupos catalogados como "terroristas" se ha hecho común en Internet. 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, y hasta del Ku Klux Klan, etc. Pero además de las páginas oficiales, los grupos terroristas, están utilizando los foros para hacer públicos sus puntos de vista, y así poder interactuar con otros consumidores de este tipo de sitios web. En estos foros suelen registrarse destacados miembros de las organizaciones terroristas, que con objeto de evitar los inconvenientes asociados a la "inestabilidad" de sus web oficiales, utilizan estas plataformas para colgar nuevos comunicados y enlaces hacia nuevos materiales (Torres, 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 también pueden estar controlados por sus administradores para evitar el envío de mensajes que contradigan el ideario yihadista.

3.2.- El uso de la red de los Estados

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, 2009). Más aún si tenemos en consideración que las amenazas pueden proceder de cualquier lugar o persona, siendo relativamente baratas, difíciles de contrabandear, complicadas

de asociar, etc. Ya no se trata de *hackers* que de forma deportiva tratan de descubrir los fallos en los sistemas de seguridad, o de *crackers* que con una mentalidad nihilista parecen disfrutar de la destrucción, sino de acciones dirigidas a paralizar las capacidades militares o los servicios públicos de un gobierno enemigo (Sánchez, 2009). Por eso, ya son muchos los Estados, sobre todo los más desarrollados, los que han puesto en marcha programas para encontrar, y si es necesario atacar, los puntos débiles de los sistemas informáticos de sus adversarios, al mismo tiempo que 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.

3.2.1.- Oficinas gubernamentales

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

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

3.2.2.- Sistemas de control

Existen diferentes sistemas de control, y tal vez lo más conocidos sean: Echelon, Enfopol, Carnivore y Dark Web. El primero, el "Echelon" o la "Gran Oreja", es un sistema automatizado de intercepción global de trasmisiones operado por los servicios de inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Su objetivo inicial era controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados durante la Guerra Fría. Aunque en la actualidad se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar tramas terroristas y planes de narcotráfico, inteligencia política y diplomática. Su funcionamiento básico consiste en situar innumerables estaciones de intercepción electrónica en satélites y en otros puntos para capturar las comunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Después cada estación selecciona, mediante la aplicación de unas palabras claves, toda aquella información que guarda relación con el fin que persigue el Sistema Echelon. Además, cada uno de los cinco países que componen el sistema facilitan a los demás "diccionarios de palabras claves" para que los incorporen como "filtros automáticos" a los aparatos de intercepción de las comunicaciones. Lógicamente estas "palabras claves" y "diccionarios" varían con el tiempo y de acuerdo con los intereses particulares de los países integrantes del sistema.

La idea de este proyecto es detectar determinadas palabras consideradas "peligrosas" para la seguridad nacional de 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. 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. Pero pese a todo, el sistema está atravesando serios problemas por el exceso de información. Hasta tal punto, que todo indica que en la actualidad, relativamente pocos son los mensajes y las llamadas telefónicas que se trascriben y registran. La mayoría son eliminados después de ser leídos por el sistema (Pachón, 2004).

En todo caso si hoy conocemos lo que es el sistema Echelon ha sido gracias al espionaje industrial. Los intereses económicos de los países implicados y de las multinacionales han sido la causa que ha llevado a este sistema al debate público (Rodríguez, 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, 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, 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, 2008).

El segundo, el "Enfopol"[7] es consecuencia directa del deseo de los gobiernos europeos de no quedarse atrás en esta carrera de escuchas cibernéticas. Por esta razón, pusieron a funcionar su propio plan de interceptación de telecomunicaciones en Europa, Estados Unidos, Australia y otros países. Así, Enfopol intenta imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tenga acceso total a las comunicaciones de sus clientes, así como a la información sobre los números marcados y los números desde los que se llama. En el caso de Internet, "los proveedores deben facilitar <<una puerta de atrás>> para que puedan penetrar a sus anchas por los sistemas privados. Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas). Todo sin que sea necesaria una orden judicial" (Añover, 2001). Pero todavía es más exigente para la criptografía. Se pide que sólo se permitan este tipo de servicios siempre que estén regulados desde un "tercero de confianza", que deberán entregar automáticamente cuando le sea solicitado: la identificación completa del usuario de una clave, los servicios que usa y los parámetros técnicos del método usado para implementar el servicio criptográfico.

El "Carnivore"[8] es la tercera generación de los sistemas de espionaje de redes del FBI[9]. Un sistema que ha sido diseñado por la Oficina Federal de Investigaciones (FBI) para capturar aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la agencia. Se especula incluso que sea capaz de espiar el disco duro del usuario que se considere sospechoso y, todo ello, sin dejar rastro de su actividad. Para ello, se coloca un chip en los equipos de los proveedores de servicios de Internet para controlar todas las comunicaciones electrónicas que tienen

[7] El programa fue acordado, el 17 de enero de 1995, mediante un "procedimiento escrito" consistente en notas de télex entre los ministros comunitarios de la Unión Europea. No hubo debate público sobre el mismo, ni siquiera se realizaron consultas a los 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, justo un año después de que la Revista Telepolis destapara el asunto.

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

[9] 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.

lugar a través de ellos, así cuando encuentra una palabra clave, eso sí con el visto bueno de la corte, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hacen a sitios de la red y las sesiones de chat en las que participa. Esto junto con el control de las direcciones de IP y de los teléfonos de conexión, permite la detección de lo que consideran "movimientos sospechosos" en la red (Busón, 2009). No obstante, ésta aplicación forma parte de un programa más complejo y amplio de vigilancia, llamado Cyber Knight (Caballero cibernético), el cuál 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.

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

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

3.3.3.- Ejércitos de cibersoldados

Sin lugar a dudas, se debe estar desarrollando sofisticadas herramientas informáticas capaces de desmantelar las defensas enemigas, de sembrar el caos en las comunicaciones o de falsificar los datos sobre las posiciones de las tropas (Sánchez, 2009). Por este motivo, un gran número de Estados están creando ejércitos de cibersoldados que puedan hacer frente a esta nueva amenaza y lanzar la suya propia. En EE.UU ha reunido un grupo de hackers de elite que se estaría 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, y que tiene la responsabilidad total de defender la red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información y dañar las comunicaciones rivales hasta inutilizarlas. Un comando que tiene como contraparte en el Grupo Especial de Tareas para la Libertad de la Internet Global (Global Internet Freedom Task Force, GIFTF, por sus siglas en inglés), una organización multiagencias[10] subordinada al Departamento de Estado. En Alemania, la Unidad Estratégica de Reconocimiento del Ejército Alemán se ha desplegado para coordinar un equipo de soldados que estén involucrados en el ensayo de nuevos métodos de infiltración, manipulación y explotación –e incluso la destrucción- de las redes informáticas. Por ello, este equipo está aprendiendo a instalar software maliciosos en ordenadores sin el conocimiento de los usuarios, robar contraseñas y datos confidenciales, etc. En España, el Ejército de Ciberdefensa (ECD09) de las Fuerzas Armadas Españolas está compuesto por militares especialistas en telecomunicaciones e informática, que han hecho cursos avanzados, militares y civiles, en seguridad de las 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.

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

[10] Participan agencias del gobierno, universidades e investigadores privados que “se mantienen operativos las 24 horas del día”.

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 que se especializan en la guerra informática. También está contratando a graduados en informática para desarrollar sus capacidades en la guerra información y, así, crear un ejército de hackers civiles. Todo, tal vez porque los chinos se han dando cuenta que, de momento, no pueden ganar a 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).

4.- La presencia de los delincuentes y criminales en la red

El cibercrimen se está valiendo de la red, por ejemplo, para obtener dinero de forma fraudulenta, bloquear páginas web con fines políticos, propagar malware, etc,

4.1.- Obtener dinero de forma fraudulenta

Tal vez el más corriente de los fraudes a través de la red sea el *mail spoofing* y la *web spoofing*. El primero es un procedimiento mediante el cual se pretende suplantar el correo electrónico de un usuario o crear correos electrónicos supuestamente verídicos a partir de un dominio para poder enviar mensajes como si formasen parte de esa identidad. Por ejemplo, cada vez es más frecuente encontrar en nuestros correos mensajes de una entidad bancaria como el BBVA (Banco Bilbao Vizcaya Argentaria) o la CAM (Caja de Ahorros para el Mediterráneo) que dispone de una dirección correo electrónica que solemos identificar con nombre@bbva.es o nombre@cam.org. En estos mensajes los presuntos clientes suelen recibir la siguiente información: "Este mensaje fue enviado automáticamente por nuestro servidor para verificar su dirección de correo electrónico. A fin de validar su dirección de correo electrónico, por favor haga clic en el enlace de abajo". De esta manera, obtienen la dirección de su correo electrónico y sus datos, pero también es común que el *mail spoofing* se emplee como una estratagema de ingeniería social para solicitar el número de las tarjetas de crédito a determinados usuarios confiados que piensan que la procedencia del mensaje se deriva supuestamente de la propia empresa de la que son clientes. El segundo consiste en una técnica de

engaño mediante el cual se hace creer al internauta que la página que está visitando es la auténtica cuando en realidad se trata de una réplica exacta de la misma pero que se encuentra controlada y monitorizada por un ciberdelincuente que pretende extraerle información y dinero, dependiendo, si se limita a seguir, vigilar, leer y grabar todas las actividades que realice el usuario, o bien, si se dedica a manipular algunos de los datos o, simplemente, le sustrae dinero o utiliza estos datos para efectuar compras en su nombre.

Otro de fenómeno relacionado con este aspecto sería los ciberocupas, que son aquellos individuos o empresas que registran para si dominios asociados a marcas, empresas o instituciones con la intención de obtener un beneficio revendiéndolo a su propietario legítimo. Otra cuestión son las llamadas telefónicas, un fraude que se realiza entre el módem del ordenador y el proveedor de Internet. Este proceso se realiza habitualmente mediante un nodo local de modo que la tarifa telefónica a pagar le corresponde a una llamada local, de ahí, que el fraude consista en desviar inadvertidamente la llamada del nodo local a otros prefijos de tipo comercial muchos más caros. Otro tema es el cibersexo, uno de los negocios más rentables de la red, ya que la libertad de acceso y el supuesto anonimato contribuye a este hecho. El sexo en Internet no está penalizado, siempre y cuando cumpla con todos los requisitos legales. El problema es que éste se convierte en ilegal cuando hacemos referencia a la pornografía infantil, o la venta de sexo sin consentimiento a través de Internet, o cuando se engaña a los clientes haciéndoles creer que el acceso a los contenidos de sus páginas es gratuito, cuando son tarifados por una línea de alto coste.

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

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

4.2.- Bloquear páginas web

Consiste en adentrarse en las web de instituciones, organizaciones, empresas o gobiernos para paralizarlas durante un determinado tiempo con el fin de generar caos, confusión e incertidumbre. Tal vez, el más conocido haya sido el protagonizado por Estonia el 27 de abril de 2007, cuando las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reformas quedaron 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 los estonios acusarán al gobierno ruso de estar detrás de estos ataques, aunque el Kremlin siempre negó su implicación en el asunto. Pero también los que se produjeron durante el conflicto bélico entre Rusia y Georgia. Los mismos tuvieron como consecuencia que distintas páginas web gubernamentales se viesen comprometidas, con continuos ataques de denegación de servicio distribuidos contra otras páginas del gobierno, teniendo como resultado la migración de ciertos sitios a servicios de posting de Estados Unidos, incluso un grupo de ciberactivistas proruso proporcionó ayuda en su página oficial para potenciar a los usuarios de Internet con herramientas para realizar ataques distribuidos de denegación de servicio,

proporcionar una lista de páginas georgianas vulnerables a inyección SQL y publicar una lista de direcciones de correos de políticos georgianos para ataques dirigidos y spam[11].

4.3.- Propagar malware

La cantidad de malware y la evolución de sus técnicas de infección y propagación se han incrementado de manera considerable a través de los últimos años. No obviemos, que cuando hablamos de malware podemos hacer referencia a un virus, un caballo de Troya, una puerta trasera (*backdoor*), un programa espía (*spyware*), o un gusano. Además, a causa de un malware puede derivarse otros ataques como puede ser: DDoS (Distributed Denial of Services), distribución de correo spam, propagación de virus y gusanos hacia otras redes, sitios *phishing*, expansión de *botnets* (redes de equipos comprometidos), fraudes de banca electrónica, *pharming* y *driving*, entre otros muchos otros (Fuentes, 2008: 4).

5.- ¿Cómo se están preparando todos estos actores para desempeñar sus acciones en el ciberespacio?

No nos cabe ninguna duda que todos estos actores se están preparando para incrementar su presencia en la red, dada cuenta que es un medio que les proporciona unas ventajas superiores a los tradicionales. Tal es el caso, que los Estados y los grupos terroristas se están preparando concienzudamente para la ciberguerra. Pero no son los únicos que están volcando en la red, cada vez son más los delincuentes que se están familiarizando con este nuevo tipo de técnica y están trasladando sus actividades al ciberespacio. Los Estados están creando una serie de sistemas de control de comunicación que les está proporcionando una valiosísima información, pero ahí no queda la cosa, sino que también están dotando de unidades especiales de soldados que no sólo tienen como misión garantizar la seguridad de sus estados sino que además tienen encomendada la labor de entrar en los servidores de los posibles enemigos para robar, o manipular,

[11] Informe Cibercrimen de 2008. En: http://www.s21sec.com/descargas/S21sec-ecrime-Informe-Cibercrimen-2008.pdf

o dañar, o destruir la información. Pero también habría que mencionar que tanto los Estados, los grupos terroristas y los ciberdelincuentes están acudiendo a los antiguos países de ideología comunista o a países como Pakistán o India para contratar a expertos informáticos que se dejan seducir por aquellos que puedan pagar sus servicios a un buen precio, sin importarles los fines a los que están dirigidas sus acciones. Al mismo tiempo que están intentando que sus miembros se vayan adaptando y acostumbrando a utilizar las herramientas del mundo digital, ya que sus organizaciones y actividades se están trasladando en buena medida a la red. Por no hacer mención a que todos ellos se han dotado de un equipo de personas que se dedican únicamente a pensar y hallar la forma de seguir perpetuando y de realizar nuevos ataques, más novedosos y más difíciles de contrarrestar.

6.- Conclusiones

Internet se ha convertido en el espacio ideal para la ciberdelincuencia y el ciberterrorismo, ya que les ofrece fácil acceso, poco o ningún control gubernamental, anonimato, rápido flujo de información, altísimo impacto, escaso riesgo, barato y indetectable. Además, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarias de seguridad de los Estados es imposible garantizar la seguridad plena de los sistemas informáticos. La única solución realmente efectiva y eficaz es apagar Internet o suprimirlo, pero esta alternativa no es, lógicamente, razonable en mundo como el actual, pese a las excepciones particulares como son las de los Emiratos Árabes, Corea del Norte o China. Aunque también existe otra posibilidad, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten, y esperar a ver cual es el resultado final. Las otras soluciones aquí planteadas como han sido los sistemas de control de comunicación, la creación de agencias y de cibersoldados, de momento, no están resultando ser totalmente efectivas. Es cierto, que están contribuyendo a detectar a ciberdelincuentes y ciberterroristas, pero todavía no son capaces de controlar ni impedir su actividad en la red.

En todo caso, como hemos dejado patente, la ciberdelincuencia, el ciberterrorismo y los Estados se están volcando en la red para desempeñar y desarrollar sus actividades, pero eso sí, con fines y objetivos distintos. Los

ciberdelincuentes emplean Internet para defraudar, dañar y bloquear con el fin de conseguir un beneficio económico o alcanzar sus intereses; los grupos terroristas están trasladando sus organizaciones difusas al ciberespacio como una forma de diluirse en un lugar que parece difícil de contrarrestar, y de ahí, que estén utilizando la red para financiarse, reclutar, entrenarse, comunicarse, coordinarse, adoctrinarse, publicitarse, etc, para continuar manteniendo sus organizaciones y alcanzar sus objetivos; y los Estados han transformado el ciberespacio en nuevo campo de batalla que le proporciona más ventajas que el tradicional, ya que si por algo se caracteriza la guerra cibernética es por su asimetría, corta duración, reacción rápida, económica, pero sobre todo, por ocasionar menos daños físicos para los soldados, un mayor espacio de combate, una lucha intensa por la superioridad de la información, un aumento de la integración y un ataque que puede ser lanzado desde cualquier lugar y casi indetectable (Thomas, 2001). En definitiva, no necesita, como en otras formas de enfrentamiento, tener sofisticado armamento y un gran ejército o estar próximos al "blanco" a batir, sólo basta con tener un ordenador y conocimientos informáticos. Además puede originarse desde cualquier parte del mundo, e incluso, simultáneamente, de lugares distantes unos de otros, sin tener que correr grandes riegos. Por si fuera poco, la continua proliferación de nuevas herramientas informáticas, así como su libre acceso y diseminación, hace más difícil la identificación del presunto atacante y más fácil mantener el anonimato, y por ende, sus efectos pueden ser igual de devastadores que la guerra convencional. De manera, que se ha ampliado enormemente el abanico de actores que pueden intervenir y originar un conflicto.

No obstante, de momento tanto Estados como grupos terroristas están haciendo un uso pasivo de la red como hemos podido comprobar. Aunque eso sí, no podemos afirmar lo mismo de los ciberdelincuentes. Aunque en todo caso, creemos que tarde o temprano unos y otros harán un uso más activo del ciberespacio para perpetuar y realizar sus acciones. Pero no somos los únicos que pensamos en tal hecho, en el informe anual que realiza la empresa de seguridad McAfee se llegó a sostener que vamos camino de una "guerra fría cibernética". De ahí, que se pueda llegar a decir que la ciberguerra, la ciberdelincuencia y el ciberterrorismo sean unas de las mayores amenazas a las que tendremos que hacer frente en el siglo XXI.

REFERENCIAS BIBLIOGRÁFICAS

Adams, J. (1999). *La próxima guerra mundial. Los ordenadores son las armas y el frente está en todas las partes*. Buenos Aires: Granika.

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

Barca, H. (2000). *Ciberguerra. Batallas sin sangre*. Ciberpaís, 4.

Brookes, P. (2007). *Contrarrestando el arte de la guerra informática*. *Grupo de Estudios Estratégicos*, nº 2011, octubre. En: http://www.gees.org/articulo/4637/

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

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

Carrillo, P. (2006). *Terrorismo y Ciberespacio*. En http://www.assessorit.com/articulos/pcarrillo-paper.pdf.

Cohen, F. (2002). *Terrorism and cyberspace*. Network Security, 5.

Colle, R. (2000). *Internet: un cuerpo enfermo y un campo de batalla*. Revista Latina de Comunicación Social, 30, junio. En: http://www.ull.es/publicaciones/latina/aa2000qjn/91colle.htm

Dacha, C. (2004). *Historia de nunca acabar*. Revista Latinoamericana de Comunicación Chasqui, marzo, 85, 66-71.

Fuentes, L. (2008). *Malware, una amenaza de Internet*. Revista Digital Universitario, 9 (4), 1-9.

Gutiérrez, M. (2005). *Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)*. Redur, 3, 69-92.

Jordán/Torres, R. (2007). *Internet y actividades terroristas: el caso del 11-M*. El profesional de la información, marzo-abril, 16 (2), 123-130.

Josrojabar, F. (2003). *Los nuevos mártires de Alá*. Madrid: Ediciones MR.

Larkin, E. (2005). *Cibercrimen (I): Delincuentes profesionales online*. PCWorld, 224, 26-30.

Merlos, A. (2006). *Internet como instrumento para la yihad*. Araucaria, diciembre, 8, 80-99.

_____ (2008). *La evolución estructural de Al Qaeda: ventajas operativas y desafíos para el contraterrorismo*. Madrid: Tesis Doctoral de la Universidad Complutense.

Orta, R. (2005). *Ciberterrorismo*. Revista de Derecho Informático, mayo, 082.

Pachón, G. (2004). *La red Echelon: Privacidad, Libertad y Criptografía*. Virtualidad Real. Programa de Doctorado en SIC. Universitat Oberta de Catalunya. En: http://www.virtualidadreal.com/Red%20Echelon.pdf

Puime, J. (2009). *El ciberespionaje y la ciberseguridad*. En: CESEDEN, *La violencia del Siglo XXI. Nuevas dimensiones de la guerra*. Monografías del CESEDEN, octubre, 112, 42/70.

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

Rogríguez, A. (2007). *Los cibercrímenes en el espacio de libertad, seguridad y justicia*. Revista de Derecho Informático, febrero, 103, 1-42.

Ruiloba, J. (2006). *La actuación policial frente a los déficits de seguridad de Internet*. Revista de Internet, Derecho y Política, 2, 52-62.

Sageman, M. (2004). *Understanding terror networks*. Philadelphia: University of Pennsylvania Press.

Sánchez, G. (2008). *Ciberterrorismo: La guerra del siglo XXI*. El Viejo Topo, marzo, 242, 15/24.

_____ (2009). *21st Century to two new challenges: Cyberwar and Cyberterrorism*. Nómadas. Mediterranean Perspectives, marzo, 1, 665-681.

_____ (2009). *Ciberguerra y Ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica*. En: Amérigo Cuervo-Argango, F. y De Peñaranda Algar, J. (Comp.) *Dos décadas de Posguerra Fría. Actas de I Jornadas de Estudios de Seguridad*. (215-241) Madrid: Instituto Universitario General Gutiérrez Mellado-UNED, pp. 215/241.

Thomas, T. (2001). *Las estrategias electrónicas de China*. Military Review, julio-agosto, 72-79.

Toffler, A. (1995). *Onward Cyber-Soldiers*. Time Magazine, agosto, 146.

Torres, M. (2007). *La dimensión propagandística del terrorismo yihadista global*. Granada: Tesis Doctoral de la Universidad de Granada.

Waston, S. (2007). *Científicos usamericanos quieren desembarazarse de la red de Internet*. Rebelión. En: http://www.rebelion.org/noticia.php?id=49932.

Weimann, G. (2004a). *How modern terrorism uses the internet. United States*. En: http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=1259&paper=1542

_____ (2004b). *United Status Institute of Peace, How modern terrorism uses the Internet*. En: http://www.usip.org/pubs/specialreports/sr116.html.

_____ (2006). *Terror on the Internet. The new arena, the new challenges*. Washington: United States Institute of Peace Press.

Zubir, M. (2006). *Maritime deputes and cyber warfare. Issues and options for Malaysia*. En: http://www.mima.gov.my/mima/htmls/papers/pdf/mokhzani/mokhzani%20%20maritime%20dispute%20and%20cyber%20warfare%20-20issues%20and%20options%20for%20malaysia%201.pdf.