CIBERESPACIO Y EL CRIMEN ORGANIZADO. LOS NUEVOS DESAFÍOS DEL SIGLO XXI

Cyberspace and Organized Crime. The new challenges in XXI century

Gema SÁNCHEZ MEDERO[1]
Facultad de Ciencias Políticas y Sociología
Universidad Complutense de Madrid
Madrid, España
✉*gsmedero@cps.ucm.es*

Vol. X, N° 16, 2012, 71-87
Fecha de recepción: 10 de octubre de 2010
Fecha de aceptación: 29 de marzo de 2011
Versión final: 22 de junio de 2012

RESUMEN. La enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos está haciendo que estas sean más vulnerables a los posibles ataques cibernéticos y al fraude en la red. Ade-

[1] Profesora titular interina de Ciencia Política y de la Administración de la Facultad de Ciencias Políticas y Sociología en la Universidad Complutense de Madrid. Es Doctora en Ciencias Políticas por la Universidad Complutense de Madrid. Ha sido profesora de Ciencia Política en la Universidad Carlos III, y en la Universidad de Costa Rica, consultora de la Universidad Oberta de Catalunya y profesora de numerosos cursos de posgrados. Ha publicado distintos artículos: "Guerra Asimétrica: La guerra del siglo XXI", "Internet: Una herramienta para la guerra del siglo XXI", "Internet: Una nueva estrategia comunicativa para los grupos armados", "PP & CDS. Pactos y Alternativas de Gobierno de Centro-Derecha en 1989","Los partidos políticos españoles", "¿Qué sucedió el 2 de diciembre de 2007 en Venezuela?", "¿Quién ganó las elecciones autonómicas y municipales celebradas el 27 de mayo de 2007 en España?", "El centro mató a la izquierda", "Una respuesta serena a los detractores del Informe sobre Inmigración en España", "*21st Century to two new challeges: Cyberwar and Cyberterrorism*", "El PP ante su XVI Congreso Nacional: Se rompe la tónica imperante", "Una nueva estrategia comunicativa de los grupos terroristas", etc.

más, 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 no hablar del alto impacto que puede alcanzar, al golpear directamente y por sorpresa al adversario. Con esto, la red se está convirtiendo en ese lugar ideal para que los delincuentes y los terroristas lleven a acabo sus acciones y actividades. Aunque no solo ellos han trasladado su campo de batalla al ciberespacio sino que también lo han hecho los Estados, que están empezando a emplear este medio para atacar a sus enemigos. De ahí que el cibercrimen, el ciberterrorismo y la ciberguerra hayan pasado a ser tres de las más importantes amenazas que parecen acechar a las sociedades occidentales. 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 que se están adoptando para evitar en la medida de lo posible estos ataques y actividades delictivas.

Palabras clave: cibercrimen, ciberterrorismo, ciberguerra, Internet, ciberataques, red y web

ABSTRACT. The Occidental Societies are becoming more vulnerable by the possible cybernetic attacks because of their large dependency on Computer and Electronics Systems and fraud in the network. 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, let alone can achieve high-impact, striking directly and surprise the enemy. Therefore, the network is becoming "that ideal place" for delinquents and terrorists from carrying out their official actions and activities. Although they have not only taken their battle to cyberspace, but so have states that are beginning to employ this means to attack their enemies. Hence, cybercrime, cyberterrorism and cyberwarfare have become three of the major threats that seem to haunt Western societies. 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: cybercrime, cyberterrorism, cyberwar, Internet, cyberattacks, network and web

Introducción

Las Tecnología de la Información y la Comunicación (TIC) 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. En cualquier caso, en la red estamos proyectando nuestro trabajo; es nuestro escenario de ocio, de comunicación, buscamos información y depositamos nuestra intimidad y privacidad, nuestra vida laboral y económica, etc.

Pero no todo es positivo, dado que el ciberespacio también está favoreciendo la aparición de nuevos problemas y amenazas a las que habrá 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 asunto es que aún no se ha valorado el verdadero alcance del problema. Todavía son muchos los que consideran que un ataque cibernético es algo relacionado con la ciencia ficción, o reservado a las películas de acción. 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, 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 qué actividades están llevando a cabo en el ciberespacio delincuentes y terroristas, para así poder determinar si estas supondrán un nuevo desafío para la sociedad, y en caso de que fuera así, qué medidas se están tomando para intentar contrarrestar estos nuevos peligros.

¿Qué es el cibercrimen y el ciberterrorismo?

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 otras actitudes que atenten contra la moralidad, y el crimen organizado (Rodríguez Bernal, 2007: 9). A diferencia de otros tipos de delitos, el cibercrimen se vale del ciberespacio para realizar sus actividades delictivas. Así, se puede entender la ciberdelincuencia como aquellas actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas.

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.

El uso pasivo de Internet, por parte de los grupos terroristas

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 un ataque ciberterrorista, ya que hasta el momento, solo se han 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). Por eso, podemos decir que unos y otros están haciendo, hasta ahora, un uso pasivo de la red.

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).

a) 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 sitio web del Ejército Republicano Irlandés (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. 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.

b) Guerra psicológica

Se está 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. 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 II, 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, y han cuestionado la legitimidad y los efectos de la "Operación Libertad Iraquí" (Merlos García, 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 García, 2006). Todo para intentar minar la moral de los EE.UU. y sus aliados, y fomentar la percepción de vulnerabilidad de esas sociedades (Merlos García, 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.

c) Reclutamiento

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), Internet, como reconocen los propios círculos yihadistas, también está facilitando está labor.

d) 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[2], la encriptación[3] y los semáforos rojos[4]. 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 empresas privadas u organismos internacionales para crear en ellas ficheros adjuntos con propaganda; u ocultan datos o imágenes en websites 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.

e) 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 me-

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

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

[4] 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.

diante 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.

f) 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 estos 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.

g) 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 este modo, 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, Euskadita Askatasuna (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 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 también pueden estar controlados por sus administradores para evitar el envío de mensajes que contradigan el ideario yihadista.

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.

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 entidades bancarias como el Banco Bilbao Vizcaya Argentaria (Bbva) o la Caja de Ahorros para el Mediterráneo (CAM), que disponen de una dirección electrónica de correo 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 la 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 sí 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 este 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. En otras ocasiones, la compra de productos se realizan con tarjetas falsas, y después los productos se venden a precios muy bajos, con lo cual los beneficios son muy altos. Esta dinámica de fraude exige una estructura capaz de obtener tarjetas para las compras, infraestructura para la recepción de los productos y canales de venta posteriores de objetos procedentes del fraude, es decir, una mínima estructura organizativa. 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 de una serie de productos que en nuestro país solo 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.

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). Un hecho semejante 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[5].

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: Distribuidos de Denegación de Servicio (DDoS), 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). La solución ha sido los antivirus, pero frente a ellos, los hackers desarrollan cada vez más virus y más complejos, algunos prácticamente indetectables, como los rootkits. Con esto se ha entrado una espiral sin fin de acción-reacción entre los hackers y las empresas de software.

Blanquear dinero

La tipología de las mulas es muy diversa y ha sufrido una evolución significativa. En los inicios, las bandas organizadas enviaban a los distintos países donde operaban, personal de la banda con varias identidades falsas y con cada una de ellas y en distintas entidades y sucursales abrían cuentas bancarias para recibir el dinero de sus víctimas. Posteriormente, trasladaron a miembros de la banda a captadores de mulas, entre colectivos de inmigrantes naturales de los países donde se ubicaba la cabeza de la banda organizada. Los captadores se dedicaban a ofrecer ciertas ganancias a quienes estaban dispuestos a colaborar. Además, les daban las instrucciones necesarias, incluso para hacer frente a la acción policial, con coartadas creíbles, como la recepción de ingresos procedentes de herencias de amigos de su país, remitidas para evitar la acción fiscal de su gobierno, o ingresos procedentes de separaciones matrimoniales de amigos para evitar el control del cónyuge. También se captaban *mulas* vinculadas al mundo de la droga que estaban

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

dispuestas a ofrecer sus cuentas por las escasas ganancias que les permitirían adquirir nuevas dosis de droga.

Hoy en día, sin dejar de lado estos procedimientos, se ha optado por el engaño. Este consiste en remitir mensajes de correo electrónico a multitud de usuarios proponiéndoles una colaboración financiera para una empresa que va empezar a operar en el país. Las ganancias serán porcentuales en función de lo que recibe en su cuenta, y aseguran que se puede llegar a ganar cantidades hasta 3.000 € con dedicación exclusiva. La cobertura de las empresas es muy diversa y muchas de ellas creíbles, como el caso de la agencia matrimonial de mujeres de países del este, que se desplazan al país de la «*mula*», y cuando contraen matrimonio, el supuesto cónyuge abona los servicios a través de ingresos al colaborador financiero o *mula*. Tal es la actividad de captación de *mulas* mediante las técnicas de engaño, que se ha creado en torno a él redes de delincuentes especializados en el tema, capaces de diseñar engaños, acompañados de la infraestructura tecnológica necesaria, como son páginas web simulando empresas o negocios legales, capaces de obtener listados de usuarios que concurren, aportando sus currículos, a portales de trabajo, y capaces de lanzar campañas dirigidas a estos usuarios seleccionados para el engaño, que la función de captación de *mulas*, también se empieza a ofrecer como servicio para el mundo del crimen organizado. En todo caso, la función de la mula no es otra que recibir el dinero procedente del fraude, en su cuenta corriente y remitirlo, previa comunicación, vía empresa de transferencia de dinero, a un tercer destinatario.

¿Cómo intentar reducir los peligros de la red?

Realmente está resultando sumamente difícil encontrar soluciones que resulten efectivas para intentar poner freno a todas aquellas actividades relacionadas con el ciberterrorismo y el cibercrimen. La primera solución sería desconectar al ordenador de la red, aunque está parece totalmente imposible ante unas sociedades que cada vez se hayan más hiperconectadas. La segunda es identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto solo se puede conseguir con la ciberinteligencia[6]. El problema que se plantea es que Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos; además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde, de forma anónima, las personas pueden conectarse y realizar actividades ilícitas. Lo mismo ocurre con las redes inalámbricas libres al alcance de equipos con conexiones capaces de conectarse a esas redes con el anonimato de la no

[6] El fin prioritario de la ciberinteligencia es el cúmulo de la información necesaria para entender el funcionamiento actual y futuro de la red, lo que lleva a que la inteligencia debe crecer continuamente con la misma velocidad que el desarrollo de las nuevas tecnologías, debe transformarse con ella para mantener la capacidad de identificar las amenazas y las contraamenazas, vulnerabilidades y respuestas frente a estas, así como los factores desencadenantes de las distintas actuaciones maliciosas.

pertenencia al grupo autorizado (Ruiloba, 2006:53). Pero estas no son las únicas dificultades a las que deben hacer frente los policías cuando realizan investigaciones en la red. Por ejemplo, cuando los posibles delincuentes saben que una máquina está comprometida por ser accesible a través de una conexión, pueden convertirla en una *virtual work station* para navegar a través de su dirección sin ser detectados; o cuando utilizan las máquinas cachés de algunos proveedores de comunicaciones para optimizar su rendimiento, ya que garantizan el anonimato de los usuarios para delinquir (Ruiloba, 2006:53).

No obstante, para intentar evitar estas posibles deficiencias jurídicas están tipificando gran cantidad y variedad de delitos informáticos. El problema es que la mayoría de las legislaciones 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. Ahora el Convenio sobre Cibercrimen (Ruiloba, 2006:53) posee contenidos de diverso carácter como, por ejemplo, delitos de intrusión en el que se integran infracciones penales contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, delitos patrimoniales (falsificaciones y fraudes a través de Internet como *phishing* y *pharming*), delitos de contenidos en los que exclusivamente se incluyen delitos de corrupción de menores en su modalidad de pornografía infantil, y delitos de infracción de la propiedad intelectual y derechos conexos, que comprenden todos aquellos dirigidos contra la propiedad intelectual y de los derechos afines, según la legislación de cada parte, entre otros.

La *tercera solución* posible, es dotarse de medios de seguridad, aunque siempre considerando que existe la posibilidad de que sean vulnerados. La *cuarta solución* es intentar adelantarse a cualquier acto delictivo mediante el control de sistemas de información como Echelon, Enfopol, Carnivore y Dark Web. El primero, fue creado en la década de los años 70 por EE.UU., pero más tarde se le unieron Gran Bretaña, Canadá, Australia y Nueva Zelandia. Su objetivo inicial era controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados. Pero en la actualidad está siendo utilizado para localizar tramas terroristas y planes de narcotráfico, inteligencia política y diplomática. Su funcionamiento consiste básicamente 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 estas señales recepcionadas son procesadas por una serie de supercomputadoras que reciben el nombre de "Diccionarios" y que han sido programadas para que busquen patrones específicos en cada comunicación, ya sean direcciones, palabras o, incluso, verificaciones. La idea de este proyecto es detectar determinadas palabras consideradas "peligrosas" para la seguridad nacional de los Estados Unidos o para los países participantes en el proyecto. 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[7].

[7] A Canadá le corresponde el control del área meridional de la antigua Unión Soviética; a EE.UU. gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China; a Gran Bretaña,

Por su parte "Enfopol es la versión europea de un sistema de control de comunicaciones. Lo que intenta es 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, todo sin que sea necesaria una orden judicial" (Añover, 2001). En el caso de Internet, "los proveedores deben facilitar «una puerta de atrás» para que puedan penetrar a sus anchas por los sistemas privados". Pero todavía es más exigente para la criptografía. Se pide que solo se permita este tipo de servicios siempre que esté regulado desde un "tercero de confianza", que deberá 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 tercero es 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 esto 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 sospechosa, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hace 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, 1998).

El cuarto, es un proyecto desarrollado por el Laboratorio de Inteligencia Artificial de la Universidad de Arizona, que utiliza 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 las herramientas desarrolladas en este proyecto, el *Writeprint*, extrae automáticamente miles de características multilingües, estructurales y semánticas para determinar quién está creando contenidos "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 copiados, enlazados o discutidos[8]. Pero el *Dark Web* también utiliza un complejo software de seguimiento de páginas, para lo que emplea los *spiders* de los hilos de

Europa, Rusia y África; a Australia, Indochina, Indonesia, y el sur de China; y a Nueva Zelandia, la zona del Pacífico Occidental.

8 Ver el siguiente artículo: http://www.laflecha.net/canales/blackhats/el-proyecto-dark-web-rastreara-la-actividad-online-de-terroristas/

discusión de búsqueda y otros contenidos, con el objetivo de encontrar las esquinas de Internet en donde las actividades terroristas se están llevando a cabo.

La *quinta solución* posible es el establecimiento de organismos gubernamentales destinados a luchar contra los posibles ataques cibernéticos. En este sentido, habría que mencionar que un gran número de gobiernos están creando Oficinas de Seguridad Informática para, desde la legalidad, combatir el cibercrimen, el ciberterrorismo y la ciberguerra. Por ejemplo, Alemania acaba de crear la Oficina Federal para la Seguridad de las Tecnologías de Información (BSI), que vendrá a ser una especie de centro de vigilancia de datos para las agencias gubernamentales; Japón ha conformado un equipo antiterrorista compuesto por unos 30 especialistas informáticos y un responsable de la Oficina de Seguridad del Gobierno; China y su Ejército de Liberación Popular ha constituido el Centro de Guerra de la Información para que dirija las acciones en relación a la ciberguerra, etc.

La *sexta solución* es la propuesta realizada por algunos investigadores estadounidenses de crear Internet 2. Una red separada de la Internet comercial, que une laboratorios y universidades de todo el mundo y que trabaja en el desarrollo de los sistemas de transmisión de información a grandes velocidades y a través de la fibra óptica (Sánchez Medero, 2009)[9]. Pero a diferencia del Internet comercial, Internet 2 estará extraordinariamente regulado y una Comisión Federal de Comunicaciones o el propio gobierno aceptará solamente «contenidos apropiados». Además, las directrices y las propuestas que están realizando, tanto la UE como EE.UU., para la retención de datos permitirán la regulación absoluta de la red (Waston, 2007). De esta manera, Internet 2 no escapará al control gubernamental y, por tanto, será menos permisible a las acciones delictivas.

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

No cabe duda que todos estos actores se están preparando para incrementar su presencia en la red, dado que es un medio que les proporciona unas ventajas superiores a los tradicionales. Así, cada vez son más los delincuentes que se están familiarizando con este nuevo tipo de técnica y están trasladando sus actividades al ciberespacio. 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, están intentando que sus miembros se vayan adaptando a utilizar las herramientas del mundo digital, ya que sus organizaciones y actividades se están trasladando en buena medida a la red. Todos ellos se han

9 Algunas de las aplicaciones en desarrollo dentro del proyecto de Internet 2 a nivel internacional son: telemedicina, bibliotecas digitales, laboratorios virtuales, manipulación a distancia y visualización de modelos 3D, aplicaciones todas ellas que no serían posibles de desarrollar con la tecnología de Internet de hoy (Sánchez Medero, 2009).

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.

Conclusiones

Internet se ha convertido en el espacio ideal para la ciberdelincuencia y el ciberterrorismo, ya que ofrece fácil acceso, poco o ningún control gubernamental, anonimato, rápido flujo de información, altísimo impacto, escaso riesgo, barato e indetectable. Además, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarías 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 un 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 cuál es el resultado final. Las otras soluciones aquí planteadas, como los sistemas de control de comunicación, la creación de agencias y de cibersoldados, de momento no están resultando 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 se ha hecho patente, los ciberdelincuentes y los ciberterroristas se están volcando en la red para desarrollar sus actividades, con objetivos distintos. Los ciberdelincuentes emplean Internet para defraudar, dañar y bloquear, con el fin de conseguir un beneficio económico o alcanzar sus intereses; y los grupos terroristas están trasladando sus organizaciones difusas al ciberespacio como una forma de diluirse en un lugar que parece difícil de contrarrestar, de ahí que estén utilizando la red para financiarse, reclutar, entrenarse, comunicarse, coordinarse, adoctrinarse, publicitarse, es decir, para continuar manteniendo sus organizaciones y alcanzar sus objetivos.

No obstante, de momento los grupos terroristas están haciendo un uso pasivo de la red como hemos podido comprobar. No obstante no podemos afirmar lo mismo de los ciberdelincuentes. En todo caso creemos que tarde o temprano unos y otros harán un uso más activo del ciberespacio para perpetuar y realizar sus acciones. En el informe anual que realiza la empresa de seguridad McAfee, se llegó a sostener que vamos camino a una "guerra fría cibernética". De ahí que pueda afirmarse que la ciberdelincuencia y el ciberterrorismo son unas de las mayores amenazas a las que tendremos que hacer frente en el siglo XXI. Todos y cada uno de nosotros podemos ser afectados por esta nueva amenaza, desde el mismo momento que realizamos todo tipo de actividades usuales como adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente. Por ejemplo, podemos ser víctimas de fraudes informáticos, de mani-

pulaciones para que se nos cargue mayor costo de la llamada, etc. Y lo que es más grave, podemos estar siendo víctimas en este instante de un hecho ilícito mediante el uso de las tecnologías e ignorarlo absolutamente. Así que la víctimas no solo son las grandes empresas multinacionales, bancos o administraciones públicas, sino cualquier ciudadano, consumidor y usuario habitual de la sociedad actual.

Bibliografía

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

Añover, Julián (2001). *Echelon y Enfopol nos espían*. En http://www.nodo50.org/altavoz/echelon.htm, recuperado el 27 de octubre de 2010.

Barca, Héctor (2000). "Ciberguerra. Batallas sin sangre". *Ciberpaís*, Nº 4.

Busón Buesa, Carlos (1998). *Control en el Ciberespacio*. En http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm, recuperado el 22 de octubre de 2010.

Carrillo Payá, Pedro (2006). *Terrorismo y Ciberespacio*. En http://www.assessorit.com/articulos/pcarrillo-paper.pdf, recuperado el 22 de octubre de 2010.

Cohen, Fred (2002). "Terrorism and cyberspace". *Network Security,* Nº 5.

Colle, Raymond (2000). "Internet: un cuerpo enfermo y un campo de batalla", en *Revista Latina de Comunicación Social*, Nº 30, junio. En: http://www.ull.es/publicaciones/latina/aa2000qjn/91colle.htm, recuperado el 17 de octubre de 2010.

Dacha, Camilo José (2004). "Historia de nunca acabar". *Revista Latinoamericana de Comunicación Chasqui*, marzo, Nº 85, pp. 66-71.

Fuentes, Luís Fernando (2008). "*Malware*, una amenaza de Internet". *Revista Digital Universitario*, Vol. 9, Nº 4, pp. 1-9.

Gutiérrez Francés, María Luz (2005). "Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)". *Redur*, Nº 3, pp. 69-92.

Jordán, Javier y Torres, Ricardo Manuel (2007). "Internet y actividades terroristas: el caso del 11-M". *El profesional de la información*, marzo-abril, Vol. 16, Nº 2, pp. 123-130.

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

Larkin, Eric (2005). "Cibercrimen (I): Delincuentes profesionales online". *PCWorld*, Nº 224, pp. 26-30.

Merlos García, Alfonso (2006). "Internet como instrumento para la yihad". *Araucaria*, diciembre, Nº 8, pp. 80-99.

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

Orta Martínez, Raymond (2005). "Ciberterrorismo". *Revista de Derecho Informático*, mayo, Nº 082.

Rodríguez Bernal, Antonio (2007). "Los cibercrímenes en el espacio de libertad, seguridad y justicia". *Revista de Derecho Informático*, febrero, Nº 103, pp. 1-42.

Ruiloba Castilla, Juan Carlos (2006). "La actuación policial frente a los déficits de seguridad de Internet". *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, Nº 2.

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

Sánchez Medero, Gema (2008). "Ciberterrorismo. La guerra del Siglo XXI". *El Viejo Topo*, marzo, Nº 242, pp. 15-23.

_____(2009). "21st Century to two new challenges: Cyberwar and Cyberterrorism". *Nómadas. Mediterranean Perspectives*, marzo, Nº 1, pp. 665-681.

Thomas, Timothy L. (2001). "Las estrategias electrónicas de China". *Military Review*, julio-agosto, pp. 72-79.

Toffler, Alvin (1995). "Onward Cyber-Soldiers", en *Time Magazine*, agosto, Nº 146

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

Waston, Steve (2007). "Científicos usamericanos quieren desembarazarse de la red de Internet". *Rebelión*. En http://www.rebelion.org/noticia.php?id=49932, recuperado el 17 de octubre de 2010.

Weimann, Gabriel (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, recuperado el 2 de octubre de 2010.

_____(2004b). *United Status Institute of Peace, How modern terrorism uses the Internet*. En: http://www.usip.org/pubs/specialreports/sr116.html, recuperado el 17 de octubre de 2010.

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

Zubir, Mokhzani (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, recuperado el 2 de octubre de 2010.