Internet: Una herramienta para las guerras en el siglo XXI

Dra. Gema Sánchez Medero

Publicada en la Revista Política y Estrategia N° 114 - 2009.

EN UN MUNDO tan hiperconectado algunos han empezado a preguntarse qué sucedería si el centro de control de Metro sufriera un ataque, si los periódicos online, cadenas de TV y radio, así como las agencias de noticias, se hicieran eco de una noticia falsa; si se accedieran ilegalmente al tablero de control de una presa hidroeléctrica y se realizara una apertura descontrolada de sus compuertas; si se hiciera un *blinds* de radar, generando un bloqueo de tráfico aéreo por 12 horas, etc. Más aún cuando resulta imposible garantizar la seguridad total de los sistemas informáticos y cuando solo es necesario disponer de un ordenador y de ciertos conocimientos informáticos para llevar a cabo este tipo de acciones. Con lo cual, son cada vez más los que sostienen que el siglo XXI será el de la ciberguerra y el ciberterrorismo, incluso, la empresa de seguridad informática McAfee, ha llegado a afirmar en su informe anual "Virtual Criminology"[1] que en las próximas décadas es posible que atravesemos por una "guerra fría cibernética", dominada por "ciberespías" y por "cibersoldados".

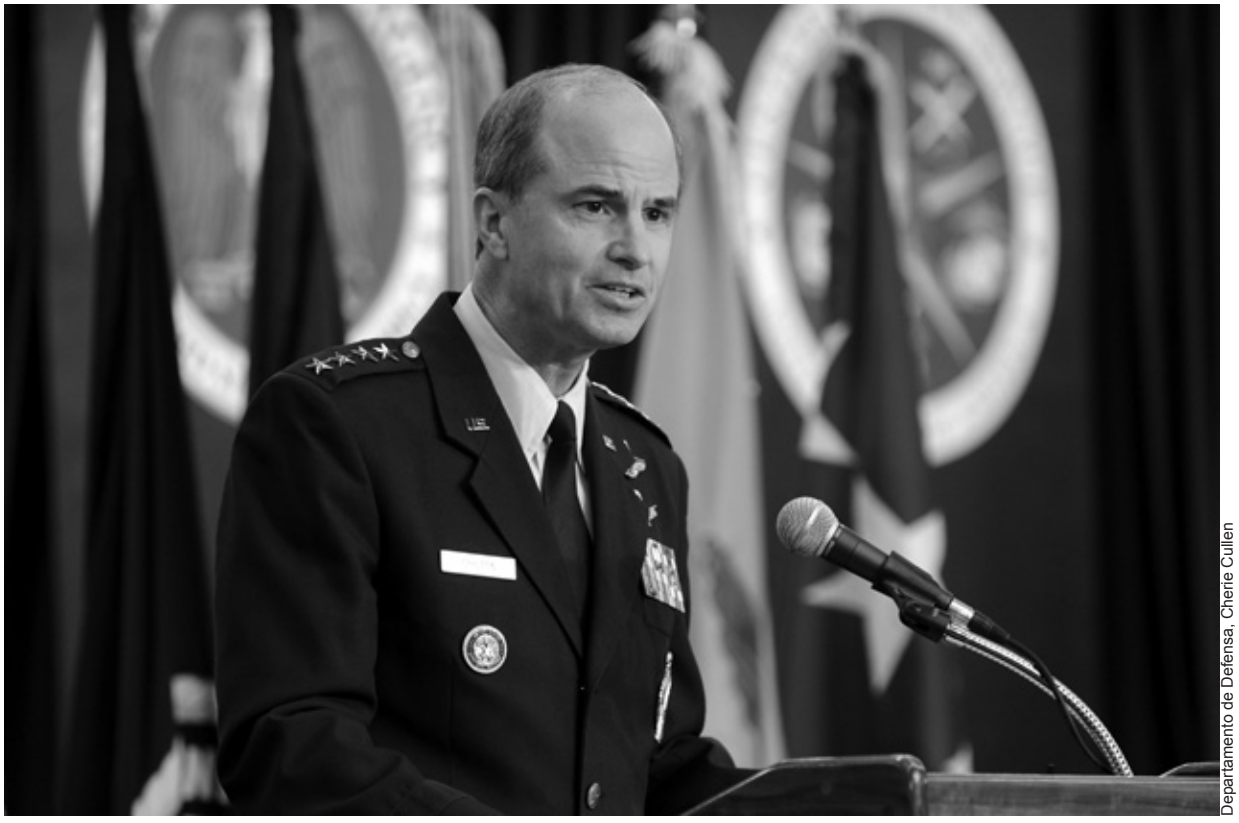
Departamento de Defensa, Cherie Cullen

Se expone el nuevo logotipo de Comando Cibernético de EUA en la ceremonia de activación del Comando en el Fuerte Meade, Maryland, 21 de mayo de 2010.

¿Qué es la ciberguerra y el ciberterrorismo?

La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle 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 le permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso para derrocarle. De ahí, que los objetivos de los ataques cibernéticos, pese a que puedan variar de uno a otro sean: 1) la explotación: cuando un atacante tiene como principal fin obtener información de los destinatarios o de los recursos de las metas; 2) el engaño: cuando un atacante permite a la meta seguir funcionando, pero manipula

Doctora en Ciencias Políticas por la Universidad Complutense de Madrid. Profesora Titular Interina del Departamento de Ciencia Política y de la Administración II. Facultad de Ciencias Políticas y Sociología. Universidad Complutense de Madrid, España. gsmedero@cps.ucm.es



Departamento de Defensa, Cherie Cullen

El general Kevin P. Chilton, Fuerza Aérea de EUA, Comandante del Comando Estratégico de EUA, se dirige al público en la ceremonia de activación del Comando Cibernético de EUA en el Fuerte Meade, Maryland, 21 de mayo de 2010.

la información que recopila la meta; 3) la destrucción: el atacante hace inoperable la meta, la destruye, ya sea la propia o la de los sistemas necesarios para que funcionen; ó 4) la interrupción o la denegación del servicio: cuando un atacante no destruye la meta, pero la pone fuera de servicio durante un período.[2]

Mientras que el ciberterrorismo, tal como lo concebimos hoy, es otra cosa. 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.

En todo caso, en uno y otro evento, una guerra cibernética se caracterizaría por ser compleja, asimetría, corta en el tiempo, más espaciada en el combate y con menos densidad de tropas, transparente, con objetivos concretos, mayor integración, e igual de devastadora que una guerra convencional.[3] Pero lo más importante es que la guerra cibernética proporciona a los más pequeños las herramientas necesarias para que puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con mínimos riesgos para ellos. Y es que la ciberguerra no solo cumple con todos los parámetros de la guerra asimétrica, sino que los potencia y los promueve; hasta el punto que se podría decir, que se ha convertido en uno de los prototipos de los conflictos asimétricos. No obviemos, que este tipo de amenazas pueden proceder de cualquier persona y lugar, son económicas, difíciles de contrabandear, complicadas de asociar, virtualmente indetectables, con un altísimo impacto, golpean directamente contra el adversario y siempre suponen una sorpresa para el enemigo, es decir, en ella se plasma toda la filosofía sobre la que se vertebra la guerra asimétrica.

El uso pasivo de Internet

Pese a las actividades que tanto los grupos terroristas como los propios Estados están realizando en internet, todavía no se ha producido ningún ataque que nos pueda inducir a proclamar el inicio de una verdadera ciberguerra o ataque ciberterrorista. Hasta el momento solo se han encontrado rastros de visitas o intentos de acceso a infraestructuras estratégicas norteamericanas en ordenadores capturados a yihadistas, pero sin mayores consecuencias. Los ataques informáticos se han limitado, en la mayoría de los casos, a colapsar los servicios de sitios web de instituciones o empresas (Ej. Estonia, 2007), inutilizar los sistemas de comunicación (Ej. Guerra del Golfo, 1991), contrainformar (Ej. Guerra Kosovo, 1999), o robar información (Ej. EUA, 2009). Por eso, podemos decir que hasta el momento unos y otros están haciendo un uso pasivo de la red.

1. El uso pasivo de internet por parte 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.[4]

Financiación. Los grupos terroristas están empleando la red, como otras organizaciones, para financiarse, es decir, como un medio para recaudar fondos para la causa. Por tal motivo los terroristas están utilizando sus páginas web para solicitar donaciones a sus simpatizantes. Por ejemplo el sitio web del IRA contenía una página en la que los visitantes podían hacer donaciones con sus tarjetas de crédito, Hamas ha recaudado dinero a través de la página web de una organización benéfica con sede en Texas, la Fundación Tierra Santa para la Ayuda, los terroristas chechenos han divulgado por la red el número de cuentas bancarias en lasque 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 en el extranjero (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.

Guerra Psicológica. También están usando el ciberespacio para librar la llamada "guerra psicológica". Existen incontables ejemplos sobre cómo se sirven de este medio sin censura para propagar informaciones equívocas, amenazar o divulgar las imágenes de sus atentados. 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, pero además han cuestionado la legitimidad y los efectos de la "Operación Libertad Iraquí".[5] De esta manera los grupos están consiguiendo transmitir una imagen interna de vigor, fortaleza y pujanza, y sus mensajes están alcanzando un impacto global.[6] Todo para intentar minar la moral de EUA y sus aliados, y fomentar la percepción de vulnerabilidad de esas sociedades.[7] 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[8] denomina "frustración delegada", es decir, la rebelión ante la injusticia que sufren otras personas, pero también para levantar la moral de los combatientes.

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."[9] 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[10], aunque internet, como reconocen los propios círculos yihadistas, también está facilitando esta labor.

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[11], la encriptación[12] y los semáforos rojos.[13] Pero también pueden colgar mensajes en el servidor corporativo privado de una empresa predeterminada para que operativos/receptores recuperen y, a continuación, eliminen el comunicado sin dejar rastro alguno; o manipular páginas electrónicas de empresas privadas u organismos internacionales para crear en ellas ficheros adjuntos con propaganda; u ocultar datos o imágenes en website de contenido pornográfico. Aunque entre todos los métodos que emplean el más creativo sea establecer comunicaciones a través de cuentas de correo electrónico con nombres de usuarios y claves compartidas. Así, una vez acordadas las claves, los terroristas se las comunican por medio de *draft messages* o borradores. La forma de comunicación es sencilla, el emisor escribe un mensaje en esa cuenta y no

Armada de EUA, Tercer Maestre Michael A. Lantron

Matt Inaki, instructor de defensores de redes computarizadas del Centro de Sistemas SPAWAR, San Diego, California, muestra al sargento segundo Daryl Graham de la Fuerza Aérea de EUA y al técnico de sistemas de información, primer maestre Martin MacLorrain, Armada de EUA cómo monitorear la actividad en una red en un curso de adiestramiento de ciberguerra en el Space and Naval Warfare Systems Center Pearl City, Hawái, 12 de julio de 2007.

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.

Coordinación y ejecución de acciones. Pero los terroristas no solo emplean la red para comunicarse, sino también para coordinarse y llevar a cabo sus acciones. La coordinación la consiguen mediante una comunicación fluida a través de internet, y la ejecución puede implicar desde un ataque lo suficientemente destructivo como para generar un temor comparable al de los actos físicos de terrorismo como cualquier otro tipo de actividades que 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.

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 ellas libres 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.

Pero, además, en la *World Wide Web* hay decenas de sitios en los que se distribuyen manuales operativos donde se explica cómo construir armas químicas y bombas, cómo huir, qué hacer en caso de detención policial, cómo realizar secuestros, o documentos críticos en los que se intenta extraer lecciones de conflictos pasados para el futuro.[14] Evidentemente, este tipo de documentos no sustituyen el adiestramiento en la vida real, pero en casos concretos pueden ser de gran utilidad.

Por ejemplo, los terroristas de los atentados de Londres, el 7 de julio de 2005, fabricaron los explosivos con fórmulas obtenidas a través de internet.[15]

Propaganda y adoctrinamiento. Internet abre enormemente el abanico para que los grupos puedan publicitar todo lo que deseen, ya que antes de la llegada de esta herramienta, las esperanzas de conseguir publicidad para sus causas y acciones dependían de lograr la atención de la televisión, la radio y la prensa. Además, el hecho de que muchos terroristas tengan un control directo sobre el contenido de sus mensajes ofrece nuevas oportunidades para dar forma a la manera en que sean percibidos por distintos tipos de destinatarios, además de poder manipular su propia imagen y la de sus enemigos.[16] 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 Hezbolá, y hasta del Ku Klux Klan, etc. Por ejemplo, el uso que hacía el IRA de internet solía ser discreto, evitando cualquier manifiesto que hiciera referencia a la lucha directa. Es más, no han tenido sitios ni publicaciones oficiales, su presencia en internet ha sido básicamente a través de su brazo político, el Sinn Fein. Otro ejemplo es el de las FARC que colgaron una página que funcionaban en seis idiomas (español, inglés, francés, italiano, alemán y portugués) para facilitar el intercambio de informaciones. En dicha página web se podía leer los partes de guerra desde 1997, poemas escritos por guerrilleros, una revista online, un programa de radio, y mensajes dirigidos a captar la atención de los jóvenes colombianos. El grupo Hezbolá, por ejemplo, ha disfrutado de tres réplicas a fin de que si una era clausurada, se pudiera acceder a las demás (www.hizbollah.org; www.hizballah.org; y www.hizbollah.tv). Estos sitios estaban escritos en árabe pero con una versión en inglés, y en ellos se ofrecían una amplia garantía de fotos, archivos de audio y video con discursos propagandísticos.

Pero además de los sitios webs 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 páginas. 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.[17] 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. Otra forma para intercambiar y transmitir información es a través de los blogs, que además suelen proporcionar enlaces con otras páginas.

2. El uso pasivo de internet por parte de los Estados

Los Estados, en primer lugar, están empleado el ciberespacio para conseguir información de sus "posibles" enemigos potenciales. Se trata de hackers o cibersoldados que se introducen en un servidor mediante un software, archivos adjuntos de correo electrónico o aprovechando las vulnerabilidades de los navegadores de internet, con el fin de poder conseguir los *passwords* necesarios para adentrarse en un determinado sistema y así poder robar información, controlar webs, tomar el mando de los ordenadores, borrar ficheros, formatear el disco duro, averiguar las actividades que está realizando el usuario, capturar pantallazos, etc. De esta manera, los Estados pueden lograr información que puede resultar muy valiosa para sus intereses, ya que les está permitiendo obtener o hacer desaparecer datos sobre los avances de otros países en cuestiones relacionadas con las operaciones defensivas y ofensivas.

Pero también están empleando la red para dañar sistemas de comunicación. Existen múltiples ejemplos que evidencia esto, incluso en casos de confrontación bélica. Por ejemplo, durante la Guerra del Golfo lo primero que hizo el ejército estadounidense fue cortar las comunicaciones iraquíes. Asimismo, los Estados están utilizando el ciberespacio para generar confusión y desinformación, y para ello están recurriendo a la difusión de noticias falsas como veraces, noticias incompletas y silencios informativos. Solo tendríamos que fijarnos en la guerra de Kosovo, donde el gobierno de Slobodan Milosevic desarrolló una campaña propagandística basada en el silencio informativo oficial y la difusión de la propaganda como información, que sólo pudo ser contrarrestada gracias a que la OTAN evitó en todo momento dañar los sistemas vitales de conexión a internet para que la población serbia tuviera la posibilidad de acceder a fuentes externas de información.

Por último, habría que mencionar la táctica de bloquear las webs de las instituciones de otros países. Esto es tan fácil que cualquiera medianamente organizado y con ciertos conocimientos informáticos podría hacerlo. Por ejemplo, sólo basta con enviar automáticamente miles de mensajes idénticos con el mismo contenido reprobatorio o con un mensaje ilegible de cientos de caracteres, o difundir un virus de carácter masivo, o habilitar páginas web para que sus seguidores con un solo movimiento de ratón pudieran contribuir a saturar un determinado servidor, etc.[18] Por ejemplo, en Chile un grupo de piratas informáticos colocaron una bandera peruana con una leyenda nacionalista en la página oficial del gobierno de Chile.

Los Estados y los grupos terroristas se preparan para la ciberguerra

Todos, Estados y grupos terroristas, se están preparando para la ciberguerra. Por tal motivo los países están dirigiendo sus acciones hacia tres frentes distintos: los sistemas de control de comunicaciones, la creación de ejércitos de cibersoldados y el establecimiento de organismos gubernamentales que eviten los posibles ataques cibernéticos; mientras que los grupos terroristas se están dedicando a buscar a expertos informáticos para la causa, al mismo tiempo que procuran que sus miembros se familiaricen con este tipo de técnicas y herramientas.

1. Los sistemas de control de comunicación

La vigilancia entre Estados siempre ha estado presente, es lo que se conoce como "guerra preventiva", lo que sucede es que ahora se ha trasladado a un entorno virtual mediante sistemas de control de comunicación como son: *Echelon*, *Enfopol*, *Carnivore* y *Dark Web*.

(Fuerza Aérea de EUA, Sgto. 2º Cecilio Ricardo)

El capitán Jason Simmons (fondo a la izquierda), Fuerza Aérea de EUA, y sargento segundo Clinton Tips (fondo a la derecha), actualizan un software anti-virus para las unidades de la Fuerza Aérea a fin de ayudar en la prevención de ataques por hackers en el ciberespacio en la Base Aérea Barksdale, Luisiana, 12 de julio de 2007.

Sistema *Echelon*. El "Sistema *Echelon*" o la "Gran Oreja", fue creado en la década de los años 70 por EUA, 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 programados 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 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.[19]

El "Enfopol". El "Enfopol"[20] es la versión europea de un sistema de control de comunicaciones. Lo que "Enfopol" 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.[21] 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.

Departamento de Defensa, Sgto 1º Adam M. Stump, Fuerza Aérea de EUA

El vicepresidente de la Junta de Jefes del Estado Mayor Conjunto, general James E. Cartwright, Cuerpo de Infantería de Marina, pronuncia un discurso en el Simposio de Ciberespacio de la Fuerza Aérea en Marlborough, Massachusetts, 19 de junio de 2008. Cartwright, en el mismo expuso la importancia de la experimentación con el uso de ciberguerra en el campo de batalla.

El "Carnivore". El "Carnivore"[22] 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 ello, se coloca un chip en los equipos de los proveedores de servicios de internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos, así cuando encuentra una palabra sospechosa, 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.[23]

El "Dark Web". El "Dark Web" 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 contenido "anónimos" online, 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.

2. La creación de ejércitos de cibersoldados

Puede que desde la era nuclear los programas militares más secretos y ambiciosos sean los que tienen que ver con el mundo del ciberespacio. Se deben estar desarrollando sofisticadas herramientas informáticas capaces de desmantelar las defensas enemigas, sembrar el caos en las comunicaciones o falsificar los datos sobre las posiciones de las tropas. 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, como, por ejemplo:

Estados Unidos ha reunido un grupo de hackers de elite que se estaría preparando para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como *Joint Functional Component Command for Network Warfare* (JFCCNW), un cuerpo que reúne personal de la CIA, FBI, Agencia Nacional de Seguridad, miembros de los cuatro ejércitos e incluso civiles y militares de los países aliados de EUA, y que tiene como función defender a todo el sistema informático de las instituciones del Estado, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información y dañar las comunicaciones rivales hasta inutilizarlas.

La Unidad Estratégica de Reconocimiento del ejército alemán está coordinando un equipo de soldados para que aprendan a infiltrarse, manipular y explotar las redes informáticas del adversario.

China ha creado una estructura de reserva especializada en telecomunicaciones, que cuenta con el apoyo de un contingente de personal altamente capacitado de expertos en computación, peritos en el monitoreo de redes y unidades de telecomunicaciones por radio. Estas fuerzas de reserva hoy en día tienen capacidad para hacer algo que queda fuera, incluso, del alcance del Ejército de Liberación Nacional (ELN) como es emplear armas electrónicas y de información para alcanzar a un adversario en otro continente[24]. Pero, además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares, ha instituido una serie de escuelas que se especializan en la guerra informática y están contratando a graduados en informática para desarrollar sus capacidades en la guerra cibernética y, así, poder configurar un ejército de hackers.

Corea cuenta con una academia militar especializada en guerra informática que está instruyendo en técnicas de creación de virus, penetrar en sistemas, programar sistemas guiados de armas, etc., a 100 cibersoldados cada año.

La OTAN ha creado un centro de excelencia para formar expertos en informática, electrónica y comunicación con el único fin de combatir el ciberterrorismo.

3. Establecimientos de organismos gubernamentales para luchar contra los posibles ataques cibernéticos

Un gran número de gobiernos están creando oficinas de seguridad informática, para que desde la presunta legalidad combatan los posibles ataques cibernéticos. Así, por ejemplo, solo por citar algunas experiencias:

Japón ha conformado un equipo antiterrorista compuesto por unos 30 especialistas informáticos y un responsable de la Oficina de Seguridad del Gobierno.

Estados Unidos ha depositado toda la responsabilidad de garantizar la seguridad de las comunicaciones estadounidenses a la Agencia de Seguridad Nacional.

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.

China y su Ejército de Liberación Popular ha constituido el Centro de Guerra de la Información para que dirija las acciones en relación con la ciberguerra.

España atribuye a la Secretaría de Estado de Seguridad la competencia de proteger las infraestructuras críticas nacionales, etc.

4. La búsqueda de expertos informáticos

Los grupos terroristas y los Estados 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. Por tanto, ya no se trata de un grupo de sujetos que buscan fama entrando en los ordenadores, ahora son personas individuales o grupos de individuos que trabajan a cambio de dinero.

5. La familiarización con las herramientas informáticas

Actualmente, los miembros de los grupos terroristas deben tener irremediablemente conocimientos básicos informáticos porque la coordinación, comunicación, instrucción, adoctrinamiento o la obtención de información se producen en la mayoría de los casos a través de la red. Por eso, en muchos de sus foros y blogs se está distribuyendo información sobre cómo comunicarse a través del correo electrónico de manera eficaz y segura, perpetuar un ataque cibernético, difundir noticias e información, etc.

Conclusiones

El ciberespacio se está convirtiendo en un nuevo escenario de conflicto. Por su propia naturaleza, internet ha pasado a ser un espacio ideal para la actividad de las organizaciones terroristas y delictivas, 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. Por tanto, la ciberguerra y el ciberterrorismo no pertenecen a la ciencia ficción, sino que es un hecho que se puede hacer realidad en cualquier instante, aunque de momento no se haya producido ningún ataque de este tipo en una infraestructura vital.

La ciberguerra es una forma de guerra asimétrica, en la que el ordenador es el arma, la red, el campo de batalla y la información, las balas. No se necesita tener armamento sofisticado y un gran ejército o estar próximos al "blanco" a batir, solo 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 riesgos. 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.

De momento, tanto Estados como grupos terroristas están haciendo un uso pasivo de la red que les está proporcionando enormes ventajas y beneficios. Los Estados, por ejemplo pueden estar obteniendo ciertas informaciones que les concedería una superioridad frente al enemigo; y los terroristas se están valiendo de la red como base para toda su infraestructura. Además, la posibilidad de una "ciberguerra" o de un ataque "ciberterrorista" ha venido a modificar las estrategias defensivas y operativas de estos actores, con todo lo que ello conlleva. Por ejemplo, en Chile se está aprobando un proyecto que autorizará el espionaje telefónico sin que sea necesario que medie orden judicial ninguna. De esta manera, el Estado podrá tener constancia de quién llama por teléfono, quién te llama, cuánto dura una llamada y desde qué lugar se realiza esta; información que hasta este momento estaba protegida y accesible sólo con autorización judicial. Ahora estará a libre disposición de cualquier fiscal del país con solo pedirla a las compañías telefónicas.

Los medios que se están empleando para intentar contrarrestar la posibilidad de un ciberataque aún no están dando los resultados esperados, ya que aunque todavía no se haya producido ningún ataque que haya ido más allá del robo de información, contrainformación, colapsar web, inutilizar sistemas de información, etc., no ha sido por su incapacidad para poder hacerlo sino por su propio interés en no realizarlo. La única solución realmente eficaz es apagar el 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, China o Corea del Norte. Aunque también existe otra posible, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto solo se puede conseguir con la ciberinteligencia.[25] El problema que se plantea es que el 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 pertenencia al grupo autorizado.[26]

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 *work station* virtual 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.[27] Para evitar estas posibles deficiencias jurídicas muchos países están tipificando gran cantidad y variedad de delitos informáticos. Por ejemplo, en Chile existe ya la Brigada Investigadora del "Cibercrimen" (BRICIB), que está adscrita a la Policía de Investigaciones de ese país. Además, según la Ley 19.974, sobre el Sistema de Inteligencia del Estado de Chile, se considera parte de la actividad de inteligencia cuya finalidad es detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional. Por si no fuera suficiente, en 1993 fue promulgada la Ley 19.223, en la cual se especifica qué conductas deben ser sancionadas por delitos informáticos. Tales como, la destrucción o inutilización de un sistema de tratamiento informático, el apoderamiento o el uso indebido de información, etc.

La ciberguerra parece estar abocada, por todo lo que ello implica y por el mundo en el que nos encontramos viviendo, a ser la guerra del siglo XXI. Todo, porque en un mundo donde, cada vez más, los sistemas de información controlan la seguridad nacional, la defensa, el tráfico aéreo, la distribución energética, las redes telefónicas, los sistemas de transmisión bancaria y de los mercados de valores, los archivos personales del sistema nacional de salud, etc., nos hace más vulnerables frente a este nuevo tipo de guerra, por no hablar de las consecuencias psicológicas y reales que podría originar un ataque de este tipo entre los ciudadanos de las sociedades occidentales.***MR***

REFERENCIAS BIBLIOGRÁFICAS

1. En: www.il-inc.com/pdf/Virtual%20criminology%2005%20spa.pdf

2. Zubir, Mokhzani. *Maritime diputes and cyber warefare. Issues and options for Malaysia*. (2006). 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.

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

4. Weimann, Gabriel. *How modern terrorism uses the internet* (United States, 2004). COHEN, Fred. "Terrorism and cyberspace", *Network Security*, nº 5, 2005.

5. Merlos García, Alfonso. "Internet como instrumento para la yihad", *Araucaria*, v. 8, nº 016, diciembre de 2006, págs. 80-99.

6. *Ibíd*.

7. *Ibíd*.

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

9. Weimann, Gabriel. *United Status Institute of Peace, How modern terrorism uses the Internet*. 2004. En: http://www.usip.org/pubs/specialreports/sr116.html.

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

11. La filosofía y las características básicas de la guerra asimétrica son claras: a) uso de técnicas que no se corresponden a las convencionales, b) el oponente puede tener una base no nacional o trasnacional, lo que dificulta su identificación y su localización, c) el terreno donde se libra la batalla es elegido por el adversario asimétrico, explotando las áreas que pueden ser más vulnerables, d) siempre se busca la sorpresa en el ataque, e) sus acciones deben tener un alto impacto con un mínimo coste, f) su estructura suele caracterizarse por tener una dirección centralizada que es complementada por unas unidades operativas descentralizadas y autónomas, lo que les permite estar presentes en todos lados, g) operan fuera de los límites marcados por el derecho internacional, h) procuran golpes directos que ponga en duda la seguridad de los Estados porque los aspectos psicológicos son fundamentales, i) ensanchan el campo de batalla al hacer partícipe a la población civil, j) sus acciones debe tener la máxima repercusión mediática, y k) los conflictos que se inician pueden tener una duración ilimitada en el tiempo.

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

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

14. 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.

15. Jordán, Javier y Torres, R. Manuel. "Internet y actividades terroristas: el caso del 11-M", *El profesional de la información*, v. 16, n. 2, marzo-abril de 2007, págs. 123-130

16. Weimann, op. Cit.

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

18. Dacha, Camilo José. "Historia de nunca acabar", *Revista Latinoamericana de Comunicación Chasqui*, nº 85, marzo de 2004, págs. 66-71.

19. A Canadá le corresponde el control del área meridional de la antigua Unión Soviética; a EUA, 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 Zelandia, la zona del Pacífico Occidental.

20. 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 europeos. 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.

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

22. Después el FBI modificó el nombre, denominándole "DCS1000".

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

24. Thomas, op. cit.

25. Ruiloba Castilla, Juan Carlos. "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, 2006, p. 53.

26. *Ibíd.*, p. 53.

27. *Ibíd.*, p. 53.