

9

EL CIBERTERRORISMO: DE LA WEB 2.0 AL INTERNET PROFUNDO

Recibido: 26/8/2015 • Aprobado: 30/9/2015

Gema Sánchez Medero
Profesora de Ciencia Política y de la Administración
Facultad de Ciencias Políticas y Sociología
Universidad Complutense de Madrid

Introducción

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

El ciberterrorismo

El *ciberterrorismo* es la convergencia del ciberespacio y el terrorismo (Orta Martínez, 2005). No obstante, no existe acuerdo acerca de una definición única. Muchos se centran en el elemento cibernético, y otros dan especial relevancia al elemento de terror (González Amado, 2007:28). Por ejemplo, el Centro de Protección de la Infraestructura Nacional nos indica que el *ciberterrorismo* es "un acto criminal perpetrado a través de computadores que resulta en violencia, muerte o/y destrucción y crea terror con el propósito de coaccionar a un gobierno a cambiar sus políticas" (González Amado, 2007: 30). Para Dan Verton (2004:32) "el *ciberterrorismo* es la ejecución de un ataque

sorpresa por parte de un grupo terrorista extranjero subnacional con objetivo político utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de un nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos". Para Jeffrey F. Addicott (2004: 32) el *ciberterrorismo* es "el empleo de varios recursos de computación para intimidar o coaccionar a otro para alcanzar objetivos específicos". En todo caso, los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en la categoría *ciberterrorismo*. Dentro de este concepto podemos hablar de tres niveles de capacidad de causar *cyberterror*, tal como se define en la Escuela de Postgrado Naval de Monterey: 1) Simple-no estructurado: la capacidad de realizar cortes básicos contra los sistemas individuales usando herramientas creadas por otra persona; 2) Avanzado-estructurado: la capacidad para llevar a cabo sofisticados ataques contra múltiples sistemas y, posiblemente, para modificar o crear herramientas básicas; y 3) Complejo-coordinado: la capacidad de hacer ataques coordinados que puedan provocar perturbaciones en masa (Jachowicz, 2003).

El ciberterrorismo en la web 2.0

Con la llegada de las nuevas tecnologías, y particularmente desde la llegada de Internet, los grupos terroristas encuentran un nuevo método de comunicación para planear y llevar a cabo sus amenazas, así como para divulgar sus ideas. Los terroristas ya no necesitan reunirse físicamente para conspirar o planificar sus ataques. Por no decir que se han convertido en una herramienta ideal para reclutar a nuevos voluntarios, recaudar fondos, dar a conocer sus hazañas y logros, conseguir información, perpetuar ataques, etc. Los grupos armados se han volcado en la red. Uno de los primeros fue el "Movimiento Sendero Luminoso"; después lo harían otros como Al Qaeda, el Ejército Republicano Irlandés (IRA), el Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Euskadi Ta Askatasuna (ETA), Hezbollah, etc. Se podría decir que, prácticamente, todos los grupos armados disponen de algún tipo de espacio (web, foro, *site*, etc.) en la red. Bien sea para divulgar la historia de la organización y de sus actividades, la información sobre sus objetivos políticos e ideológicos, las críticas de sus enemigos, o simplemente, para verter amenazas o abrir foros de debate e interactuar con sus seguidores y simpatizantes. Aunque eso sí, no siempre son fáciles de encontrar ni de acceder, ya que como cabe suponer suelen ser perseguidos por los servicios policiales y de inteligencia de los distintos gobiernos. De ahí que por norma general se mantengan poco tiempo en una misma dirección, cambiando constantemente de ubicación, o que su acceso se encuentre limitado por un administrador.

Una tipología de los sitios web de los grupos terroristas podría ser la siguiente:

1*) Sites oficiales o webs creadas y administradas directamente por miembros de la organización*. Es el grupo menos numeroso pero el más importante y el más cuidado estética y técnicamente, ya que este tipo de páginas son las principales fuentes para acceder a la difusión de nuevos vídeos, grabaciones sonoras, libros y cualquier otro material original (Torres Soriano, 2009a: 300). En la red podemos encontrar webs del Ejército Republicano Irlandés (IRA), el Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Sendero Luminoso, ETA, Hezbollah, etc. Por ejemplo, en el sitio oficial de Hamás (http://www.palestine-info.com) se ofrecen comunicados, biografías de los líderes y mártires del movimiento y relatos de momentos importantes de su historia. Además esta organización ha contado con seis sitios subsidiarios en distintos idiomas: inglés (www.palestine-info.co.uk), francés (www.palestine-info.cc), ruso (www.

palestine-info.ru), malayo (www.infopalestina.com), urdu (www.palestine-info-urdu.com), y farsi (www.palestine.persian.info). El problema de estas webs es que suelen estar muy perseguidas, lo que hace que su presencia en la red sea bastante breve, hasta que pasado un tiempo sus responsables son capaces de reubicarse en nuevo dominio (Conway, 2002).

2) *Foros*. Son páginas web donde se realizan preguntas sobre temas generales o concretos esperando abrir debates con ellas. En estos foros suelen registrarse destacados miembros del grupo, que con objeto de evitar los inconvenientes asociados a la "inestabilidad" de sus webs 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 pueden estar sometidos a la censura interna de sus administradores para evitar envíos que contradigan el mensaje que desean propagar, o que los administradores delimiten los contenidos en función de la categoría que les otorgan a los diferentes miembros en función de sus méritos dentro del foro, etc.
3) *Blogs*. Son utilizados para expresar opiniones y distribuir contenidos y realizar enlaces con otras páginas. Gracias a los blogs se puede crear un verdadero *feedback* (camino de ida y vuelta) de la comunicación, que atraviesa un modelo bidireccional (uno a uno) para acabar en un modelo multidireccional (muchos a muchos). Pero ahí está también su mayor peligro: cualquiera puede crear una identidad falsa y divulgar información falsa o contradictoria, confundiendo a los lectores.
4) *Sites de distribución*. Tienen como objetivo el sustento de la infraestructura del grupo, de manera que los miembros del mismo no queden desenganchados de la *umma* virtual, como consecuencia de los *hackeos* por parte de los servicios de inteligencia y ciberactivistas individuales (Torres Soriano, 2007:261). Además muchas de ellas son auténticos directorios actualizados, donde por ejemplo es posible encontrar reubicadas las más importantes webs yihadistas, lo que las ha convertido en un valioso recurso para aquellos individuos que se inician en el consumo de estos materiales, ofreciendo de manera sencilla y accesible toda una serie de recursos de información a través de los cuales pueden llevar a cabo una profundización en la ideología de los grupos (Torres Soriano, 2007:261).
5) *Los grupos mediáticos*. El grupo mediático más representativo es, sin duda, el llamado Global Islamic Media (GIM), transformado posteriormente en Global Islamic Media Front (GIMF). Originalmente constituía uno de los grupos o espacios virtuales que la compañía Yahoo ofrece a los usuarios de sus cuentas gratuitas de correo electrónico. Dicho grupo atesoraba las direcciones de e-mail de casi 7.500 usuarios afiliados, los cuales recibían regularmente información sobre nuevos materiales, vídeos, enlaces, etc. (Torres Soriano, 2009a:303).
6) *Las redes* sociales. El impacto de *Twitter* es enorme: una red social que permite comunicar al instante a cientos de miles de sus componentes, simplemente publicando un *"post"* que no puede superar los 140 caracteres. Los mensajes para cualquiera de estos *"microblogs"* pueden enviarse desde la web, desde un móvil vía SMS o incluso desde los sistemas de mensajería instantánea (en el caso de *Twitter*, *Aol*., *GTalk*, *Mac*, *LiveJournal* y *Jabber*), con una facilidad asombrosa, como un chasquido de dedos. En ellas, además, los usuarios pueden intercambiar de manera abierta no sólo fotografías, textos y opiniones, sino también informaciones de interés como las nuevas direcciones webs de grupos terroristas. De ahí que algunos grupos armados, como por ejemplo Sendero Luminoso, hayan creado redes sociales en

Facebook y *Hi5*. Además, desde su creación, el poder de las redes sociales no ha dejado de crecer; válganos simplemente de ejemplo la capacidad de movilización y de repercusión que han mostrado durante la guerra de Irak.

7) *Páginas de alojamientos de vídeos y archivos*. *YouTube*, *Internet Archive*, *World TV*, Megaupload o similares, esconden miles de archivos y vídeos de grupos armados. Pero además los grupos armados se están valiendo de las webs de empresas que se dedican a ofrecer a sus clientes la posibilidad de alojar en sus servidores archivos que pueden ser descargados por cualquier usuario simplemente con copiar una dirección en la barra de direcciones de su navegador, un *link* que está disponible en una serie de foros que actúan como bibliotecas virtuales de enlaces. Aunque es muy probable que esta estrategia de comunicación sea remplazada por otro tipo de páginas, que como *Megavideo* y *InternetArchive.org* permiten no sólo alojar y descargar estos archivos de gran tamaño sino también poder visionarlos *on-line*, lo que acelera el proceso de su "consumo" al tiempo que se reducen los "rastros digitales" que supone descargar y alojar estos contenidos en una computadora (Torres Soriano, 2009b).



Gracias a estos espacios los grupos terroristas difunden una ingente cantidad de información por la red que va desde vídeos, comunicados, fotografías, archivos de audio, logotipos, biografías de sus líderes y mártires, relatos de momentos importantes de su historia, recomendaciones de seguridad... hasta todo tipo de *links*. Por tanto, podemos hablar de tres tipos de materiales: los destinados a los seguidores o miembros del grupo y a la causa, a los simpatizantes y seguidores que no mantienen ningún tipo de vínculo directo con la organización, y a los adversarios. No obviemos que la guerra psicológica siempre ha sido un elemento crucial en las cruzadas de los grupos terroristas. Por eso la propaganda de guerra se dirige, en primer lugar, a la propia vanguardia para sostener la moral combatiente; luego, a la propia retaguardia que nutre de hombres y pertrechos a la vanguardia; también a los neutrales, para impedir que se alíen con el enemigo, para mantenerlos en su posición equidistante o para atraerlos hacia la causa; asimismo se dirige hacia al enemigo, tanto a su vanguardia como a su retaguardia (Pizarroso, 2008:51).

Pero los *ciberterroristas* no están empleando la red únicamente para difundir su mensaje, sino también para obtener financiación. En ella han encontrado un nuevo medio para recaudar fondos para su causa. Los terroristas están utilizando sus páginas web para solicitar donaciones a sus simpatizantes. Por ejemplo, Hamás ha recaudado dinero a través de la página web de una organización benéfica con sede en Texas, la Fundación Tierra Santa para la Ayuda. 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.

Además 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 vídeos de las torturas, las súplicas y/o el asesinato de rehenes, como los estadounidenses Nicholas Berg, Eugene Armstrong y Jack Hensley, los británicos Kenneth Bigley y Margaret Hassan, o el surcoreano Kim Sun-Il, que han circulado descontroladamente por numerosos servidores y portales de Internet, no han hecho más que reforzar la sensación de indefensión de las sociedades occidentales, pero además han cuestionado la legitimidad y los efectos de la "Operación Libertad Iraquí". De esta manera, los grupos terroristas están consiguiendo trasmitir una imagen interna de vigor, fortaleza y pujanza, y sus mensajes están alcanzando un impacto global. Todo para intentar minar la moral de los EE.UU. y sus aliados, y fomentar la percepción de vulnerabilidad de esas sociedades (Merlos, 2006).

Asimismo, la red está sirviendo para reclutar a miembros, de la misma manera que algunas personas la usan para ofrecer sus servicios. En primer lugar, porque al igual que "las sedes comerciales rastrean a los visitantes de su web para elaborar perfiles de consumo, las organizaciones terroristas reúnen información sobre los usuarios que navegan por sus sedes. Luego contactan con aquellos que parecen más interesados en la organización o más apropiados para trabajar en ella" (Weimann, 2004). En segundo lugar, porque los grupos terroristas cuentan con páginas web en las que se explica 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.

Igualmente, 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 su organización o de otras 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. Pero los terroristas no sólo emplean la red para comunicarse, sino también para coordinarse y llevar a cabo sus acciones. La coordinación la consiguen mediante una comunicación fluida a través de Internet, y la ejecución puede implicar desde un ataque lo suficientemente destructivo como para generar un temor comparable al de los actos físicos de terrorismo, como cualquier otro tipo de actividades que repercutan de manera diferente a la población pero que son igual de efectivas, como pueden ser el envío masivo de *e-mails* 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 de 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.

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 encontrar y

estudiar infinidad de cuestiones acerca de sus posibles objetivos (mapas, horarios, detalles precisos sobre su funcionamiento, fotografías, visitas virtuales...), la creación de armas y bombas, 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 en una persecución, qué hacer en caso de detención policial, cómo realizar secuestros, etc., o documentos críticos en los que se intentan extraer de conflictos pasados lecciones para el futuro.

Pero la relación de los grupos terroristas con el ciberespacio no es tan idílica como parece. La red está llena de presuntas vulnerabilidades para la difusión de los mensajes terroristas. Por ejemplo, es cierto que Internet brinda a los grupos terroristas un canal perfecto de comunicación, pero no siempre es así; por ejemplo, en los regímenes dictatoriales o aquellos en los que el Estado ejerce un excesivo control sobre su población, se combina el escaso respeto por el secreto de las comunicaciones con el más hiriente subdesarrollo material. Lo que indudablemente induce a que una buena parte de esa población, que *a priori* podría consumir este tipo de información, se retraiga de hacerlo, ante el control que se ejerce sobre estos canales, y por tanto, la posibilidad de perder el anonimato. Además, hay que tener en cuenta otro hecho: cada vez más se están desarrollando programas que pueden ser introducidos en un ordenador sin ser detectados y que permiten al controlador monitorizar todo su tráfico de datos. Por no hablar de los constantes ataques cibernéticos que sufren las webs de este tipo de grupos para conseguir inutilizarlas, por lo menos, hasta que se reubican en otro espacio; o la cantidad de páginas que están surgiendo "presuntamente" en defensa de este tipo de causas, pero que en realidad son webs tapaderas de los servicios de inteligencia; o el incremento de medidas que caminan hacia una mayor capacidad de control del ciberespacio por parte de los servicios de inteligencia; o la creación de multitud de unidades especializadas en la lucha en el ciberespacio.

El ciberterrorismo en el internet profundo

Hay una parte de internet que no es accesible a los motores de búsqueda tradicionales. Es normalmente lo que se denomina "internet profundo o invisible". Se trata de todo el contenido inaccesible desde los buscadores tradicionales por diferentes motivos, como tratarse de páginas y sitios web protegidos con contraseña, documentos en formatos no reconocibles o contenidos que requieren interrogar a su base de datos para poder acceder a la información.

Se estima que el tamaño de la internet profunda es 500 veces más grande que la web superficial; esto significa que los buscadores tradicionales no rastrean el 99% del contenido existente en internet. En el internet profundo puede encontrarse información que es válida para sistematizar en una base de datos (por ejemplo directorios telefónicos, archivos gráficos, multimedia, etc.), información que cambia de forma constante, sitios de compañías e instituciones, páginas internas de sitios muy grandes que son creadas dinámicamente, además de todo un mundo de actividades que ilícitas que buscan el anonimato. De ahí que se haya convertido en un lugar ideal para realizar todo tipo de actividades criminales. Tal es así que según el informe de Trend Micro llamado "Below the Surface: Exploring the Deep Web" más del 25% de vínculos entre la internet oculta y visible tienen fines de explotación infantil; también pueden encontrarse, por ejemplo, ofertas de unos 180.000 dólares por asesinar a una personalidad o político. Por tal motivo, los *ciberterroristas* también han encontrado en este internet profundo un lugar para seguir realizando sus actividades en la red.

El éxito de cerrar webs de grupos terroristas es relativo, ya que siendo un usuario medianamente avanzando en internet no sólo se puede consultar información nueva sino que se puede consultar el contenido antiguo. En las bibliotecas, que son aquellas webs que se dedican a archivar páginas antiguas y que dejan de estar por tanto en circulación, se pueden hallar algunos contenidos que se

creían desaparecidos, como la que fue la web oficial de Al Qaeda (www.alnelda.com), cerrada en 2002:



Fuente: http://web.archive.org/web/200201129223155/http://alneda.com/. Consultada el 22 de agosto de 2015.

En cambio, al consultar el internet superficial la web que aparece es otra:



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

Además, el internet profundo también permite navegar de forma anónima en las llamadas redes privadas virtuales (VPN). Las más populares son TOR e I2P. La primera se desarrolló con el fin de proteger las comunicaciones gubernamentales, y para ello se ocultaba la verdadera IP del ordenador, impidiendo que la ubicación del usuario fuera localizada. Además, con este servidor se puede eludir la censura, ya que tiene una opción para ayudar a que los usuarios ubicados en países que tienen un acceso restringido a internet se liberen de su vigilancia en la red. La segunda surge como alternativa a la red TOR y está pensada para proteger la comunicación de seguimiento de las redes de vigilancia y la monitorización por terceras partes, como los ISPs (proveedores de internet).

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



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

De esta manera, el anonimato supone una ventaja no sólo para la realización de actividades delictivas (violación de la propiedad intelectual, *spam*, *ciberacoso*, estafa, robo de identidad, etc.), sino también para el encubrimiento de actividades terroristas, como filtrados de información, actividades de inteligencia en fuentes abiertas, acciones de propaganda, compra de material, ciberguerra, etc. (De Salvador Carrasco, 2012:2).

Conclusiones

Internet se ha convertido en una gigantesca red de redes, en la que no manda nadie y en la que se interconectan millones de usuarios que puede enviar y recibir mensajes, consultar bases de datos desde cualquier sitio, acceder a grandes cantidades de información multimedia, relacionarse instantáneamente, etc. Un fenómeno social del que no han sido ajenos los grupos terroristas, que han encontrado en el ciberespacio un lugar ideal para producir, trasmitir y difundir sin censuras sus propios materiales, recaudar fondos, reclutar voluntarios, facilitar la comunicación, realizar ataques, etc. El único problema que han encontrado han sido las vulnerabilidades que parece presentar el ciberespacio. No obstante, el balance para los terroristas sigue siendo más positivo que negativo, de ahí que se hayan instalado en la red y la usen con profusión.

Bibliografía

ADDICOTT, J. F. (2004): *Cases and materials on terrorism law*. Ed. Lawyers and Judges Publishing Inc. Tucson.

ADHAMI, W. (2007): "La importancia estratégica de Internet para los grupos armados insurgentes en las guerras modernas". *International Review of the Red Cross*, nº 868, pp. 305-327.

CONWAY, M. (2002): *Reality Bytes: Cyberterrorism and terrorist use of the Internet*. Department of Political Science1, College Green Trinity College. En: http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf (Consultado el 12 de mayo de 2013)

DE SALVADOR CARRASCO, L. (2012): *Redes de anonimización en Internet: Cómo funcionan y cuáles son sus límites. Documento de Opinión*. Madrid, Instituto Español de Estudios Estratégicos.

ECHEVARRÍAJESÚS, C. (2009): "La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas". *Grupo de Estudios* Estratégicos y Análisis, nº 7416, pp. 1-8. También en: http://www.seguridadfip.org/boletinestudiosdefensa/boletin36estudios/Lainnovacionyahadistapropagandaciberterrorismoarmasytacticas.pdf (Consultado el 12 de mayo de 2013).

FLORES SÁNCHEZ, M. L. (2008): "Internet como herramienta del integrismo yihadista". *Boletín Información*, nº 303, pp. 23-56.

GONZÁLEZ AMADO, I. (2007): "Ciberterrorismo. Una aproximación a su tipificación como conducta delictiva". *Derecho Penal y Criminología. Revista del Instituto de Ciencias Penales y Criminológicas*, vol. 28, nº 84, pp. 13-46.

GONZÁLEZ SAN RUPERTO, M. (2005): "Grupos radicales islámicos en la red". *Revista Historia y Comunicación Social*, nº 10, pp. 117-133.

GREY, D. H. y HEAD, A. (2009): "The importance of the Internet to the post-modern terrorist and its role as form of safe haven". *European Journal of Scientific Research*, vol. 3, nº 25, pp. 396-404.

JACHOWICZ, L. (2003): *How to prevent and fight international and domestic. Cyberterrorism and cyberhooliganism*. Collegium Civitas. Foreign Policy of the United States of America.

JONGMAN, B. (2011): "Internet websites and links for terrorism research". *Perspectives on Terrorism*, vol. 5, nº 1, pp. 23-37.

MERLOS GARCÍA, J. A. (2006a): "Internet como instrumento para la Yihad". *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, nº 16, pp. 80-99.

MERLOS GARCÍA, J. A. (2006b): *Al Qaeda. Raíces y metas del terror global*. Madrid, Biblioteca Nueva.

MERLOS GARCÍA, J. A. (2008): *Terror.com. Irak, Europa y los nuevos frentes de la Yihad*. Pamplona, EUNSA.

ORTA MARTÍNEZ, R. (2005): "Ciberterrorismo". *Alfa-Redi. Revista de Derecho Informático*, nº 82. En: http://ceeseden-terrorismo.tripod.com/id71.html (Consultado el 21 de mayo de 2013).

PIZARROSO QUINTERO, A. (2008): "Aspectos de propaganda de guerra en los conflictos armados más recientes". *Redes.com*, nº 5, pp. 49-65.

SÁNCHEZ MEDERO, G. (2009a): "Ciberguerra y Ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica". En AMÉRIGO CUERVO-ARGANGO, F. y DE PEÑARANDA ALGAR, J. (comps.), *Dos décadas de Posguerra Fría. Actas de I Jornadas de Estudios de Seguridad*. Madrid, Instituto Universitario General Gutiérrez Mellado-UNED, pp. 215-241.

SÁNCHEZ MEDERO, G. (2009b): "Internet: Una herramienta para las guerras del siglo XXI". *Revista Política y Estrategia*, nº 114, pp. 63-104.

SÁNCHEZ MEDERO, G. (2009c): "Las dos nuevas perspectivas del siglo XXI: Ciberterrorismo y Ciberguerra". *Nómadas. Mediterranean Perspectives*, nº 1, pp. 683-700.

SÁNCHEZ MEDERO, G. (2010a): "Una nueva estrategia comunicativa de los grupos terroristas". *Revista Enfoques: Ciencia Política y Administración Pública*, vol. 8, nº 12, pp. 201-215.

SÁNCHEZ MEDERO, G. (2010b): "Los Estados y la ciberguerra". *Boletín de Información del CESEDEN*, nº 317, pp. 63-75.

SÁNCHEZ MEDERO, G. (2012): "Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI". *CENIPEC*, nº 31, pp. 241-267.

TIBBETTS, P. S. (2002): *Terrorist use of the Internet and related information technologies*. School of Advanced Military Studies, United States Army Command and General Staff College. Fort Leavenworth, Kansas, 2002. En: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403802&Location=U2&doc=GetTRDoc.pdf (Consultado el 12 de mayo de 2013)

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

TORRES SORIANO, M. R. (2009a): *El eco del terror. Ideología y propaganda en el terrorismo yihadista*. Madrid, Plaza y Valdés Editores.

TORRES SORIANO, M. R. (2009b): "Terrorismo yihadistas y nuevos usos de Internet: La distribución de propaganda". *Análisis del Real Instituto*, nº 110/2009.

VERTON, D. (2004): *La amenaza invisible del ciberterrorismo. Black Ice*. Madrid, McGraw Hill.

WEIMANN, G. (2004): *How modern terrorism uses the Internet*. United States Institute of Peace, Sepecial Report nº 116. En: http://www.usip.org/publications/www-terrornet-how-modern-terrorism-uses-the-internet (Consultado el 21 de mayo de 2013).