Opción, Año 32, No. Especial 8 (2016): 509 - 518
ISSN 1012-1587

Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista

***Miguel Ángel Poveda Criado*[1]**
***y Begoña Torrente Barredo*[2]**

[1]*Universidad Europea. Madrid, España*
Miguelangel.poveda@uem.es
[2]*Institutional Institute of Security Study (IISS). Madrid, España*
b.torrente@iisecuritystudies.es

Resumen

Es indudable que la creciente accesibilidad a internet, así como la rápida evolución de las tecnologías de la información y comunicación (TIC) han propiciado importantes progresos y ventajas para la sociedad. Sin embargo, este mundo virtual (ciberespacio) está repleto de nuevas amenazas que no sólo pueden perjudicarnos individualmente, también pueden llegar a ser capaces de poner en peligro la paz y seguridad internacionales. El uso de internet y las redes sociales por parte de grupos terroristas para llevar a cabo propósitos como financiación, propaganda, reclutamiento, etc., ha de ser considerado como una forma de ciberterrorismo.

Palabras clave: TIC, ciberterrorismo, *cybercrim*, ciberataques, financiación.

Social Networks and Cyberterrorism. ICT as a Terrorist Tool

Abstract

There is no doubt that the increased availability of Internet and the quick search evolution of Information Technology and Communication (ICT) have led to significant progress and benefits society

Recibido: 01-05-2016 • Aceptado: 01-06-2016

para. However, this virtual world (cyberspace) is packed with new threats can not only hurt us individually, can also become capable of endangering international peace and security, such as cyberterrorism. The use of internet and social networks by terrorist groups to keep out purposes like financing, propaganda, recruiting, etc., must be regarded as a form of cyberterrorism.

Keywords: ICT, cyberterrorism, cybercrime, cyberattacks, financing.

1. INTRODUCCIÓN: ENTENDIENDO EL CIBERTERROSIMO

Si resulta difícil encontrar una definición unívoca o universal del concepto de terrorismo, descubrir una interpretación común de la idea del ciberterrorismo parece una tarea imposible. Para tratar de solucionar este problema y formular en el presente apartado una definición general y certera del ciberterrorismo, es necesario tomar como referencia lo que entendemos por terrorismo. Aunque existen muchas y diferentes interpretaciones del terrorismo, hemos decidido emplear la que el Departamento de Defensa de Estados Unidos propuso en el año 2008:

> Terrorismo es el uso premeditado e ilegal (o amenaza del uso) de la fuerza o violencia en contra de individuos o propiedades para ejercer coerción o intimidar a gobiernos o sociedades, con el fin de alcanzar objetivos generalmente políticos, religiosos o ideológicos (Marín, 2011:12).

A pesar de que esta definición puede resultar incompleta, lo cierto es que reúne la mayor parte de las características esenciales que debería congregar cualquier manifestación de terrorismo. De esta manera, hemos tomado en cuenta aquellas interpretaciones de ciberterrorismo que incluyen, si no todos, algunos de los rasgos mencionados anteriormente. Una de las interpretaciones más citadas cuando se trata el tema del ciberterrorismo es la de la Dra. Dorothy Denning, profesora del Departamento de Análisis de Defensa en la universidad Naval Postgraduate School, que se resume en la siguiente idea:

> Ciberterrorismo es la convergencia entre terrorismo y ciberespacio. (…) Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar

> miedo. Ataques que deriven en muertes o personas heridas, explosiones, choques de aviones, contaminación de agua o severas pérdidas económicas pueden servir de ejemplo (Dorothy, 2000:2).

Para clarificar aún más el concepto de ciberterrorismo, debemos tener en cuenta la última descripción propuesta por la Organización de las Naciones Unidas (ONU):

> (Ciberterrorismo) es el uso de las tecnologías de la información por parte de grupos terroristas o individuos con el fin de desarrollar y promover su agenda. Se incluyen los ataques contra redes, el intercambio de información y la organización de actividades terroristas (United Nations, 2013:3).

De esta manera, podemos resumir el concepto de ciberterrorismo como el uso deliberado de tecnologías relacionadas con la informática para amenazar o atacar a personas, así como a propiedades e infraestructuras, con el fin de infundir terror para alcanzar un fin político, ideológico, social o religioso. Además, se incluye en esta definición el desarrollo de la acción terrorista en el ciberespacio a través de propaganda, financiación, reclutamiento, obtención e intercambio de información, etc. Dependiendo de la interpretación que se le dé al fenómeno del ciberterrorismo, éste poseerá unas características u otras. Aun así, podemos encontrar algunas peculiaridades que resultan inherentes a cualquier acepción de dicho fenómeno:

- **Bajo coste**: Uno de los mayores alicientes para que los terroristas usen medios informáticos con el fin de infundir terror es el bajo precio que suponen los ciberataques.
- **Premeditación**: Al igual que los ataques terroristas convencionales, los ciberataques se caracterizan por ser calculados antes de ser ejecutados con el fin de estudiar el impacto que quieran generar a través de ellos y asegurarse que su lucha política, religiosa o ideológica sea revelada a través, generalmente, de los medios de comunicación.
- **Selectividad**: No todo el mundo puede convertirse en terrorista informático de la noche a la mañana. Para llevar a cabo ataques considerables y sofisticados a través de la red es necesaria una habilidad informática que requiere unos conocimientos científicos y matemáticos muy avanzados.

- **Anonimato**: La cobardía de los ciberterroristas puede ser mayor que la de algunos terroristas convencionales, puesto que pueden llevar a cabo sus ataques sin dejar rastro alguno de su identidad o ubicación.
- **Imprevisibilidad**: No hay duda de que un ataque planeado y llevado a cabo desde la red es totalmente inesperado para el objetivo que se quiere amenazar o dañar, a no ser que sea previamente anunciado o localizado por las agencias o fuerzas de seguridad. Aun así, existen algunos sistemas informáticos que son indetectables y esto reduce considerablemente las posibilidades de que un ciberataque sea evitado.
- **Fenómeno no presencial**: Los ciberterroristas no sólo pueden amenazar o atacar a personas e infraestructuras desde lugares diferentes a dónde se encuentren éstas, también pueden desarrollar actividades como el reclutamiento y entrenamiento de terroristas, la financiación o la planificación de ataques sin necesidad de un espacio real donde llevar a cabo dichas actividades.

Es importante tener en cuenta que el concepto de ciberterrorismo no se puede confundir con el del delito informático (*cybercrime*). Si en el mundo real somos capaces de hacer una distinción entre un ataque terrorista y un delito, en el virtual ocurre lo mismo. A pesar de que un delito informático puede resultar muy nocivo, no puede entrar dentro de la interpretación de ciberterrorismo ya que se define como una actividad criminal e ilícita que utiliza los recursos informáticos como medio (cuando se realizan delitos tradicionales tales como chantaje, robo, falsificación, estafa, etc. a través de la red informática) o como fin (cuando se pretende causar algún daño a otros ordenadores, redes o sistemas electrónicos).

2. CÓMO SE MANIFIESTA EL CIBERTERRORISMO

2.1. Los ciberataques terroristas

Los ciberataques son actos criminales ejecutados a través de un ordenador u otra tecnología informática con el fin de causar algún daño o extorsión tanto físico (cuando se ataca a personas o propiedades) como tecnológico (cuando se ataca a otros equipos y sistemas informáticos). Cuando dichos ataques se llevan a cabo para tratar de lograr un fin religioso, ideológico o político se trata entonces de una manifestación de ci-

berterrorismo. Existen dos tipos de ciberataques que pueden ser ejecutados por terroristas: ataques a infraestructuras informáticas y ataques a infraestructuras físicas.

2.1.1. Ciberataques a infraestructuras informáticas.

Los terroristas pueden llevar a cabo estos ataques a través de internet u otro recurso informático para distorsionar o causar algún daño en las infraestructuras de las Tecnologías de Información y Comunicación (TIC). Se trata entonces de ataques a datos y sistemas informáticos que no pretenden causar ningún perjuicio físico en personas o propiedades, aunque al final ese daño casi siempre se produce por la conexión entre la tecnología y la realidad. Es importante destacar que la intención de estos ataques no siempre es la misma, nosotras hemos distinguido dos tipos de ciberataques a infraestructuras informáticas teniendo en cuenta su intencionalidad:

- **Ciberataques con intención de tomar el control de otros dispositivos o sistemas informáticos:** Estos ataques se suelen realizar a través de un software llamado "Bot-net" que es capaz de penetrar en otros ordenadores y servidores para controlar su funcionamiento de forma remota. Uno de los ataques más comunes es el Ataque de Denegación de Servicios, también conocido como ataque DoS (acrónimo en inglés de *Denial of Service*), cuya función principal es bloquear el funcionamiento de una red, ordenador o servidor ajeno. A través de estos ataques, los terroristas no sólo pueden perjudicar los recursos informáticos y páginas web de aquellos a quienes quieren atacar, también son capaces de enviar spam o mensajes no solicitados para hacer propaganda, exaltar su lucha, infundir terror, etc.
- **Ciberataques con intención de obtener información confidencial**: Los terroristas pueden vulnerar, de manera anónima y rápida, la confidencialidad de los datos o sistemas informáticos que deseen atacar a través distintos programas informáticos. "*Spyware*" es el software más utilizado en este tipo de ataques ya que es capaz de compilar información privada de un ordenador sin que su propietario/a se dé cuenta de ello y enviarlo después al ordenador o dispositivo de aquel que comete el ataque.

2.1.2. Ciberataques a infraestructuras físicas.

Una de las mayores amenazas para la seguridad tanto nacional como internacional es el ataque de infraestructuras críticas como las redes eléctricas, las plantas nucleares, las presas de agua, etc. a través de sistemas informáticos. No hay duda de que los efectos de un ciberataque a las redes que hoy en día permiten el control y la supervisión de procesos industriales a distancia, denominadas SCADA (*Supervisory Control And Data Acquisition*), serían realmente devastadores y se traducirían en daños terribles en el mundo real. Aunque todavía ningún grupo terrorista ha llevado a cabo un ciberataque de este calibre, lo cierto es que sí que existen ejemplos de daños ocasionados en infraestructuras físicas a través de sistemas informáticos.

2.2. La explotación de internet por parte de grupos terroristas

Aparte de los ataques terroristas que pueden llegar a ejecutarse a través de sistemas informáticos, existe otra amenaza dentro de la convergencia entre terrorismo e informática que es la presencia de organizaciones terroristas en Internet para desarrollar y promover su lucha. Las razones que hacen que los terroristas se interesen por Internet son muchas y entre ellas destaca su escasa regulación y censura, su bajo precio y la oportunidad que ofrece al poder diseminar información por todo el mundo rápidamente y de forma anónima. A continuación, analizaremos los medios que utilizan los terroristas para establecer su presencia en Internet, las actividades que desarrollan y finalmente

2.2.1. Medios utilizados por los terroristas para establecer su presencia en Internet

El Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI) distingue tres vías a través de las cuales los grupos terroristas consolidan su presencia en Internet: páginas web oficiales, páginas web no oficiales y webs de distribución.

2.2.2. Actividades terroristas en Internet

El objetivo principal de la mayoría de grupos terroristas es lograr un fin político, social, ideológico o religioso. Pero, ¿cómo pueden luchar por ese fin y desarrollarlo a través de Internet? Casi de la misma manera que en la realidad, es decir, a través de actividades como la propaganda y difusión de terror, la financiación o el reclutamiento de nuevos miembros. Veamos, por tanto, seis de esas actividades que sostienen y enriquecen la lucha terrorista:

- **Difusión de propaganda y terror.** Las organizaciones terroristas han visto en Internet un importante medio para expresarse libremente y hacer llegar su mensaje a cualquier rincón del mundo. La red ofrece multitud de plataformas, en muchas ocasiones libres de censura y control, para que los terroristas puedan presentar y glorificar sus anhelos, justificar y enaltecer sus actos violentos, demonizar al sistema establecido o a aquellos a quienes quieren atacar, promover sentimientos de violencia, etc. Todo ese material propagandístico se difunde con la intención de captar la atención de grandes multitudes y manipularlas para que apoyen su causa. De hecho, la propaganda se suele adaptar a aquellos grupos sociales más desfavorecidos y marginados y además de esto, muchas páginas web traducen su contenido a diferentes idiomas para que su impacto sea más universal.
- **Reclutamiento y activismo.** La difusión de propaganda que mencionábamos en el punto anterior es a menudo utilizada por los terroristas para reclutar nuevos colaboradores y miembros que apoyen sus ideales. Internet consigue que los simpatizantes de determinadas causas políticas, ideológicas, sociales o religiosas puedan tomar contacto y relacionarse fácilmente con aquellos grupos que las amparan. Pero el interés no sólo se lleva a cabo de simpatizante a terroristas, en gran parte de los casos son los terroristas los que recaban información de los internautas que les siguen y establecen una relación con aquellos más interesados en su lucha. Además, existen en la red foros, tablones de anuncios o chats de acceso restringido para llevar a cabo el reclutamiento de manera clandestina. El instituto SITE (*Search for International Terrorist Entities*), un grupo de inteligencia estadounidense que analiza la actividad online de grupos terroristas, confirmó la existencia de una compleja campaña de reclutamiento online que Al Qaeda desarrolló y ejecutó en 2003 para reunir a personas dispuestas a viajar a Iraq con el fin de atacar a las fuerzas estadounidenses establecidas allí. Por otra parte, los terroristas no sólo pretenden reclutar "combatientes", también se interesan por generar nuevos activistas que propaguen su mensaje allá donde vayan y en este sentido no suelen ser selectivos a la hora de elegir el público al que se dirigen.
- **Entrenamiento**. No hay duda de que Internet se ha convertido en una importante base de entrenamiento y adiestramiento para los terroristas. Existen muchas páginas web donde se puede encontrar y

publicar fácilmente las instrucciones necesarias para fabricar una bomba u otros artefactos y armas. El ejemplo más importante de este tipo de documentos es "La enciclopedia de la Yihad", un manual de más de mil páginas elaborado por Al Qaeda y disponible en Internet, que ofrece instrucciones detalladas de cómo establecer una organización clandestina o como llevar a cabo actos como la toma de rehenes.

- **Financiación.** Internet también puede ser utilizado por los terroristas como una vía rápida y discreta para financiar su mantenimiento y sus proyectos. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) distingue cinco categorías diferentes de financiación terrorista: recaudación directa, comercio electrónico, empleo de servicios de pago en línea, contribuciones a empresas fantasmas y financiación fraudulenta:
- **Coordinación y planificación.** Una de las mayores ventajas que ofrece Internet es el anonimato y la posibilidad de establecer una comunicación entre varias personas sin necesidad de que se reúnan físicamente en el mismo lugar. No hay duda de que los terroristas corren menos peligro de ser detectados o interceptados si planifican sus actos a través de la red.
- **Conexión interna y con otros grupos terroristas.** Una de las razones por las que la descentralización de algunos grupos terroristas como Al Qaeda es cada vez mayor es el acceso de las mismas a Internet. No hay duda de que la comunicación entre células asentadas en diferentes países del mundo resulta mucho más fácil a través de un ordenador. Internet no sólo facilita la interconexión de los grupos terroristas, también les permite comunicarse entre ellos para intercambiar información o expandir su influencia.

3. CONCLUSIONES

El ciberterrorismo es una amenaza real para el mantenimiento de la paz y la seguridad, no sólo por los ataques o delitos que se pueden cometer a través de los ordenadores u otras tecnologías en infraestructuras informáticas o físicas, también por el uso que hacen de Internet la mayoría de los grupos terroristas que existen en la actualidad. Hemos visto que a través de plataformas como páginas web, foros, chats, blogs, etc. los te-

rroristas pueden expandir sus capacidades y su lucha de manera rápida, gratuita y en gran parte de las ocasiones, anónima. Los gobiernos y organizaciones internacionales coinciden en el hecho de que existe una nueva amenaza en el ciberespacio, sin embargo, no son capaces de ponerse de acuerdo al determinar en qué consiste esa amenaza y por ello todavía no podemos encontrar una definición común de lo que se conoce como ciberterrorismo. Además, existe mucha confusión en torno a los conceptos de hacktivismo (convergencia entre el ciberespacio y el activismo principalmente social y político), ciberdelito (delito informático) y ciberguerra (guerra informática) y a menudo son tratados como ciberterrorismo cuando en realidad estas prácticas no se basan en lograr un fin ideológico, político, religioso o social. De lo que no hay duda es que en el ciberespacio no existen fronteras y por ello es necesario que el desarrollo de una seguridad efectiva en este mundo virtual se lleve a cabo a través de la cooperación internacional y el establecimiento de un marco legislativo internacional sin desconciertos.

En el ámbito ciber, las respuestas por parte de autoridades nacionales e internacionales han sido dispares, teniendo especial protagonismo las políticas antiterroristas –infiltración y monitorización, por parte de los servicios de inteligencia, de actividades y comunicaciones con objeto de prevenir acciones terroristas y recabar pruebas que puedan ser empleadas judicialmente– y contraterroristas, mediante la creación de mandos especializados –como el español Mando Conjunto de Ciberdefensa (MCCD) o los múltiples estadounidenses–. Asimismo, se han implementado políticas activamente enfocadas en ciberseguridad –como la creación de centros especializados tales como el *European Cybercrime Center* (EC3) o el *US Cyber Threat Intelligence Integration Center* (CTIIC).

Referencias Bibliográficas

ARQUILLA, John y RONFELDT, David. 1993. **Cyberwar is coming!** RAND corporation. Disponible en http://www.rand.org/pubs/reprints/RP223.html Consultado el 07.07.2015.

CESEDEN (Centro Superior de Estudios de la Defensa Nacional). 2012. **El ciberespacio. Nuevo escenario de confrontación**. Ministerio de Defensa de España. Disponible en http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf. Consultado el 01.07.2015.

CORNISH, Paul. LIVINGSTONE, David. CLEMENTE, Dave y YORKE, Claire. 2010. **On cyber warfare**. Análisis para Chatham House Report. Disponible en https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf. Consultado el 20.06.2015.

DENNING, Dorothy. E. 1999. **Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.** Washington. Disponible en http://nautilus.org/info-policy/workshop/papers/denning.html#axzz2mnvZzg2R. Consultado el 17.06.2015.

DENNING, Dorothy. E. 2000. **Cyberterrorism.** Disponible en http://www.cs.georgetown.edu/~denning/ Consultado el 15.06.2015.

GORDON, Sarah. Y FORD, Richard. 2003. **Cyberterrorism?** Análisis para Symantec Corporation. Disponible en http://www.symantec.com/avcenter/reference/ cyberterrorism.pdf. Consultado el 22.06.2015.

LEMOS, Robert. 2002. **What are the real risks of cyberterrorism?** Disponible en: http://www.zdnet.com/news/what-are- the-real-risks-of-cyberterrorism/124765. Consultado el 18.06.2015.

MARÍN, Rodolfo. 2011. **Definición del concepto de terrorismo.** pág. 12. Disponible en http://es.scribd.com/doc/56665123/DEFINICION-CONCEPTO-TERRORISMO. Consultado el 17.06.2015.

McCAUGHEY, Martha. y AYERS, Michael. 2003. **Cyberactivism. Online activism in theory and practice.** Ed. Routeledge. Inglaterra (UK).

POVEDA, Miguel Ángel, 2015. **Terrorismo global y crimen organizado,** Ed. Fragua, Madrid, (España).

POVEDA, Miguel Ángel, 2015. **Delitos en la red,** Ed. Fragua, Madrid (España).

THOMAS, Timothy L. 2003. **Al Qaeda and the Internet: the Danger of Cyberplaning.** Ed. Parameters. Disponible en http://strategicstudiesinstitute.army.mil/pubs/ parameters/articles/03spring/thomas.pdf. Consultado el 24.06.2015.

United Nations Office on Drugs and Crime (UNODC). 2012. **The use of internet for terrorist purposes.** Http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Consultado el 19.06.2015.

WEIMANN, Gabriel. 2006. **Terror on the Internet: The new arena, the new challenges.** United States Institute of Peace (USIP). Washington (USA).