Cómo citar este artículo:

Payá-Santos, C. A. & Delgado, J. J. (2016). El uso del ciberespacio para infringir el terror. *Estudios en Seguridad y Defensa, 11*(22),

El uso del ciberespacio para infringir el terror[1]

The Cyberspace Usage for Infringing Terror

O uso do Ciberespaço para infringir o terror

CLAUDIO AUGUSTO PAYÁ SANTOS[2]

JUAN JOSÉ DELGADO MORÁN[3]

Recibido:
25 de mayo de 2016

Aprobado:
30 de noviembre de 2016

Resumen

El terrorismo, en todas sus manifestaciones, afecta a todos. El uso de Internet para promover fines terroristas va más allá de las fronteras nacionales, lo que amplifica el efecto potencial sobre las víctimas. Las nuevas tecnologías han creado un nuevo campo de batalla, creando unos nuevos retos a los que enfrentarse. En el ciberespacio, las respuestas que han dado las autoridades nacionales e internacionales han sido diferentes, 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 utilizadas judicialmente, y contraterroristas, mediante la creación de mandos especializados como el español Mando Conjunto de Ciberdefensa. La promoción de la retórica extremista, que fomenta los actos de violencia, también es una

Palabras claves:

Terrorismo, ciberespacio, Tecnología, Seguridad Internacional

Keywords:

Terrorism, Cyberspace, Technology, International Security

Palavras Chaves:

Terrorismo, ciberespaço, tecnologia, segurança internacional

1. Artículo de reflexión vinculado al grupo de investigación "Catedra Nebrija – Santander de análisis y resolución de conflictos" de la Universidad Antonio de Nebrija, España.

2. Doctorando en Ciencias Humanas, Sociales y Jurídicas de la Universitat International de Catalunya, España, y de la Universita Luiss Guido Carli, Italia. Magíster en Inteligencia de la Universita della Calabria, Italia. Magíster en Grafoanálisis Europeo, peritaciones y análisis de la Universidad Autónoma de Barcelona, España. Magíster en Seguridad e Inteligencia de la Libera Universita Hugo Grotius, Italia. Licenciado en Criminología de la Universidad de Alicante, España. Coordinador de Área de Seguridad y Defensa de la Universidad Nebrija y Coordinador de la Catedra de Análisis y resolución de Conflictos Nebrija-Santander. Contacto: cpaya@nebrija.es

3. Candidato a doctor en Derecho de la Universidad de Murcia, España. Magíster en Derecho Penitenciario de la Universidad de Murcia, España. Magíster en Prevención de Riesgos de la Universidad Camilo José Cela de Madrid, España. Magíster en Análisis y Prevención del Terrorismo de la Universidad Rey Juan Carlos de Madrid, España. Licenciado en Criminología por la Universidad de Alicante, España. Miembro del grupo de investigación de la Cátedra Nebrija sobre "Conflictos territoriales en América Latina". Docente del área de Seguridad y Defensa de la Universidad Nebrija. Contacto: jdelgado@nebrija.es

tendencia común en toda la gama, cada vez mayor, de plataformas basadas en Internet que hospedan contenido generado por los usuarios. Contenidos que antes podrían haber sido distribuidos a un público relativamente limitado, en persona o a través de medios físicos como discos compactos -(CD)- y discos de video digital -(DVD)-, han ido pasando cada vez más hacia Internet. Los contenidos pueden distribuirse ahora usando una amplia gama de herramientas, tales como sitios web especiales, salas virtuales de charla y foros, revistas en línea, plataformas de redes sociales, como Twitter y Facebook, y sitios web populares de videos y de intercambio de ficheros, como You-Tube y Rapidshare, respectivamente. El uso de los servicios de indización, como los buscadores de Internet, también hace que sea más fácil descubrir y obtener contenido relacionado con el terrorismo. El anonimato relativo que ofrece Internet a los terroristas para promover sus causas o facilitar sus atentados, sumados a complejas cuestiones relacionadas con la ubicación, retención, incautación y presentación de los datos relacionados con Internet, hacen que la cooperación internacional eficaz y oportuna entre los organismos encargados de hacer cumplir la ley y los servicios de inteligencia, sea un factor cada vez más importante para el éxito de la investigación y el enjuiciamiento de muchos casos de terrorismo.

Abstract

Terrorism, in all its manifestations, affects us all. The use of the Internet to promote terrorist purposes goes beyond national borders, amplifying the potential effect on victims. The new technologies have created a new battlefield, creating some new challenges to face. In cyberspace, the responses given by national and international authorities have been different, with anti-terrorist policies, infiltration and monitoring by intelligence services, activities and communications in order to prevent terrorist actions and to gather evidence that can be used judicially, and counter-terrorists, through the creation of specialized controls such as the Spanish joint command of cyber defense. The promotion of extremist rhetoric, which encourages acts of violence, is also a common trend across the growing range of Internet-based platforms hosting user-generated content. Contents that may have previously been distributed to a relatively limited audience, in person or through physical media such as compact discs (CDs) and digital video (DVD) discs, have increasingly passed the Internet. Content can now be distributed using a wide range of tools, such as special websites, virtual rooms online magazines, social networking platforms such as Twitter and Facebook, and popular video and file sharing sites such as You-Tube and Rapidshare, respectively. The use of indexing services, such as Internet browsers, also makes it easier to discover and obtain content related to terrorism. The relative anonymity offered by the Internet to terrorists to promote their causes or facilitate their attacks, coupled with complex issues related to the location, retention, seizure and presentation

of Internet-related data, make effective and timely international cooperation between agencies Law enforcement and intelligence services. Is an increasingly important factor in the success of the investigation and prosecution of many cases of terrorism.

Resumo

Terrorismo, em todas suas manifestações, afeta a todos nós. O uso de Internet para promover fins terroristas vai além das fronteiras nacionais, o que amplifica o efeito potencial sobre as vítimas. As novas tecnologias criaram um novo campo de batalha, criando novos desafios para enfrentar. No ciberespaço, as respostas que têm dado as autoridades nacionais e internacionais ter sido diferentes, tomando especial destaque as políticas de combate ao terrorismo, infiltração e monitoração pelos serviços de inteligência, de atividades e comunicações, a fim de evitar ações terroristas e reunir provas que podam ser usadas judicialmente, e contra terrorista, atravesse da criação de controles especializados como o espanhol Mando Conjunto de Ciberdefensa. A promoção da retórica extremista que promove os atos de violência, também é uma tendência comum em toda a gama, cada vez maior, de plataformas baseadas na Internet que hospedam conteúdo gerado pelos usuários. Conteúdos que antes poderiam ter sido distribuído a uma audiência relativamente limitada, pessoalmente ou através de meios físicos, tais como discos compactos (CDs) e discos de vídeo digital (DVD), têm sido cada vez mais mudados para a Internet. Os conteúdos agora podem ser distribuídos usando uma ampla gama de ferramentas, como sites webs especiais, salas virtuais de bate-papo e fóruns, revistas online, plataformas de redes sociais como Twitter e Facebook, e sites de vídeo populares e de compartilhamento de arquivos como You-Tube e Rapidshare respectivamente. O uso dos serviços de indexação, tais como os motores de busca da Internet, também torna mais fácil descobrir e obter conteúdo relacionado com o terrorismo. O relativo anonimato que a Internet oferece aos terroristas para promover suas causas ou facilitar seus ataques, juntamente com questões complexas relacionadas com a localização, retenção, apreensão e apresentação de dados relacionados com a Internet, fazem que a cooperação internacional eficaz e oportuna entre agências responsável pelos serviços de aplicação da lei e de inteligência um fator cada vez mais importante para o sucesso da investigação e repressão de muitos casos de terrorismo.

Introducción

Desde finales de la década de 1980, Internet ha demostrado ser un medio de comunicación sumamente dinámico, que llega a un público cada vez mayor en todo el mundo. El desarrollo de tecnologías, cada vez más sofisticadas, ha creado una red con un alcance verdaderamente mundial y barreras al acceso relativamente bajas. La tecnología de Internet hace que resulte fácil para una persona comunicarse con

relativo anonimato, rapidez y eficacia, a través de las fronteras, con un público casi ilimitado. Sin embargo, cabe reconocer que la misma tecnología que facilita dicha comunicación puede explotarse también con fines terroristas. El uso de Internet con fines terroristas crea oportunidades y desafíos en la lucha contra el terrorismo. Los avances tecnológicos han proporcionado a los terroristas muchos medios sofisticados que les permiten servirse de Internet con fines ilícitos. Las características de los nuevos conflictos, existen multitud de teorías que aportan diferentes enfoques sobre la misma realidad. Mary Kaldor, (2001), expone que durante la década de los 80´s y 90´s, aparecieron un nuevo tipo de guerras cuyos objetivos estaban ligados a políticas de identidad. Estas nuevas guerras de la era de la globalización, surgen en un contexto de erosión o desaparición de las estructuras del Estado y, por ende, de la imposibilidad de ejercer el monopolio del uso legítimo de la fuerza. En palabras de la académica británica:

> El objetivo es controlar a la población deshaciéndose de cualquiera que tenga una identidad distinta. Por eso, el objetivo estratégico de estas guerras es expulsar a la población mediante diversos métodos, como las matanzas masivas, los reasentamientos forzosos y una serie de técnicas políticas, psicológicas y económicas de intimidación. (Kaldor, 2001)

De igual forma, en este nuevo tipo de conflictos desaparece la tradicional distinción entre lo civil y lo militar; entre combatientes y no combatientes, ya que, la guerra acaba convirtiéndose en un fin en sí mismo, puesto que en la mayoría de las ocasiones, aparecen grupos paramilitares que reclaman dinero a cambio de protección (Kaplan, 1994).

Otra de las características de los nuevos conflictos es el cambio en las armas o instrumentos utilizados para la guerra. En la actualidad, en un mundo marcado por el uso de internet, las capacidades de destrucción entre los países del "primer mundo" y los del "tercer mundo", se han equiparado de una forma inédita hasta ahora, puesto que a través de la red se podrían causar graves estragos al adversario sin que sea necesario que la parte que los causa disponga de grandes capacidades militares. Visto lo anterior, se considera de vital importancia, hacer hincapié en la posibilidad de entender al terrorismo global como un actor de este nuevo tipo de conflictos que viene marcado por una característica común que no es otra que la asimetría. El Ejército de los Estados Unidos entiende por asimetría en términos bélicos lo siguiente: "actuar, pensar, y organizarse de forma diferente al adversario en orden a maximizar nuestras fortalezas y explotar las debilidades del enemigo" (Patterson, 2002).

En esta asimetría, se basa la enorme vulnerabilidad de las sociedades occidentales frente al terrorismo yihadista. Muchos analistas creen que las razones

del éxito de ISIS son sus renovadas capacidades. Los dirigentes de Estado Islámico saben que para poder formar un califato deben actuar como un Estado. Por eso han creado una estrategia de difusión revolucionaria entre los grupos terroristas. Su estrategia de comunicación pretende imitar la comunicación institucional de un Estado. La innovación de ISIS se encuentra en comenzar a utilizar medios alojados en el ciberespacio como las redes sociales, adaptándose a sus características, como puede ser el lenguaje, en Twitter, Facebook o Instagram, adaptando su comunicación a sus propios objetivos. Realmente, hasta hace poco, no tenemos una definición general y globalmente aceptada del termino ciberterrorismo. Internet se ha convertido en un fenómeno social, cultural, económico y tecnológico que sirve para acercar a las personas y las instituciones de una manera fácil, rápida y barata. Además, la red permite evadir todas las restricciones físicas y genera incluso un volumen superior de interacciones con una comunidad global que no necesita ni de una ubicación geográfica concreta ni de un conocimiento físico entre ellos (Sánchez Medero, 2010).

En los 80´s se empezó a utilizar el término con definiciones como "convergencia del ciberespacio con el terrorismo"; o en los 90´s como "el ciberterrorismo es el ataque premeditado y políticamente motivado contra la información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras". El ciberterrorismo o terrorismo electrónico, es el uso de los medios tecnológicos, de información, de comunicación, informáticos, electrónicos o similares con el propósito de generar terror o miedo generalizados en una población o gobierno, causando con ellos una violación de la libre voluntad de las personas. Esto puede tener fines económicos, políticos o religiosos.

En los últimos años, el surgimiento y avance de la tecnología ha ido ganando mucho terreno en lo político, social y económico. Actualmente, internet es el mayor fenómeno social conocido y que ha marcado una gran influencia en el día a día de las personas. Esto permite la accesibilidad a millones de páginas web en todas las partes del mundo, con información de todo tipo, con un mecanismo ágil y global de comunicación, pero como ocurre con frecuencia entre los seres humanos, este medio también está siendo utilizado para satisfacer intereses ilícitos de individuos y grupos que han visto en internet una oportunidad muy buena de saciar sus oscuros intereses. De ahí que cada día se tengan más casos de hechos ilícitos a través de la red. Así pues, la red se muestra como una fuerza productiva, configurada como resultado una nueva generación de terroristas "a tiempo parcial", capaces de conjugar un intenso compromiso con la yihad, con una actividad profesional y una vida social perfectamente normal, donde los ciberactivistas que cooperan con los grupos terroristas sin estar necesariamente en el lugar originario de la organización (Castells, 1999).

El Ciberterrorismo, la utilización de ciberherramientas, para parar, degradar o denegar el acceso a infraestructuras críticas nacionales, como la energía, el transporte, las comunicaciones y los servicios gubernamentales, con el propósito de coaccionar o intimidar a un gobierno o a la población civil, es claramente una amenaza emergente para la que se debe desarrollar habilidades de prevención, disuasión y respuesta.

Ciberespacio como ciberamenaza

La comunicación y acción a través de internet es barata, efectiva y sencilla. Tan solo se necesita un ordenador con conexión a internet para poder acceder a los contenidos. Por ello, se valora con mucha preocupación el uso del ciberespacio como escenario de conflicto. El ciberterrorismo es una opción tan alarmante para la Comunidad Internacional como atractiva para las organizaciones terroristas. Según el autor Richard A. Clarke, la ciberguerra es cualquier penetración no autorizada por parte de, en nombre de, o en apoyo a, un gobierno en los ordenadores o las redes de otra nación, en la que el propósito es añadir, alterar o falsificar información o causar daños a, o perturbar el adecuado funcionamiento de, un ordenador, un dispositivo de red o los objetos controlados por el sistema informático (Clarke & Knake, 2010).

A partir de esta definición, surge la duda de si el terrorismo es capaz de extender sus brazos sobre este nuevo desafío global. Es evidente que la posibilidad de realizar un "mega-atentado" puede despertar el interés de grupos terroristas. Sin embargo, estas aspiraciones no son para nada fáciles de llevar a cabo. Organizaciones como Al Qaeda han experimentado, ya con estos medios sin conseguir nada fructífero. Sus acciones se han limitado a prácticas que podría hacer cualquier hacker autodidacta, no yendo más allá del sabotaje de sitios web, reconocimiento de objetivos y robo de datos personales a través de internet (Jordán, 2013).

Según el antiguo director nacional de inteligencia de Estados Unidos, Mike McConnel, los grupos terroristas alcanzarán la cibersofisticación, ya que es igual que la proliferación nuclear, pero más fácil (Nye, 2011). El ciberterrorismo, a diferencia de lo que muchos piensan, solo implica el uso del ciberespacio como un instrumento para provocar daños físicos a las personas u objetos, algo que resulta infinitamente más complejo que el hacktivismo, el uso de internet para emitir propaganda, la financiación, la obtención de información o la comunicación privada entre sus miembros (Torres Soriano, 2015).

La aparición de internet, lo extendido de su uso y el potencial que ofrece, han hecho de la red de redes tanto un instrumento de los terroristas como un campo de actuación. En palabras de Ban Ki-Moon, Secretario General de las Naciones Unidas: "Internet es un excelente ejemplo de cómo los terroristas pueden actuar de

manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional", convirtiéndose en un instrumento del terrorismo que permite, entre otras muchas posibilidades, comunicaciones "discretas" entre los criminales y el desarrollo de todo tipo de tareas logísticas y de captación. Dentro del carácter instrumental que puede tener internet para la nebulosa terrorista, no hay que olvidar que la web es en la actualidad el canal de información más ágil y global que existe y que propagar el terror entre la población es consustancial al terrorismo.

El terrorismo cibernético representa una grave amenaza para la seguridad económica y de las naciones, especialmente en un momento en el que los grupos fundamentalistas están creciendo y se propagan rápidamente en todo el mundo gracias también al uso de la red. Es un peligro para la seguridad económica puesto que en la actualidad la inmensa mayoría de las transacciones comerciales en el mundo se realizan a través de internet. Un ataque a ese "canal" significaría el colapso de la economía y la consiguiente pérdida de ingentes cantidades de dinero. Quizás este haya sido el motivo para la lucha contra el ciberterrorismo se haya centrado durante muchos años en los ataques contra la red, mientras que ha quedado demostrado en las declaraciones de multitud de terroristas yihadistas detenidos, que el uso de internet era determinante para sus tareas logísticas y de captación.

Gabriel Weiman (2004), identifica algunas formas de utilización terrorista del ciberespacio: a) *Como instrumento de guerra psicológica:* Mediante la difusión a la población enemiga de imágenes que le ocasionan terror como pueden ser las imágenes en las que se ejecutan rehenes mediante su decapitación; b) *Como instrumento de propaganda e intoxicación:* Las organizaciones terroristas pueden publicitar sus acciones en tiempo real a la totalidad del mundo una vez que hayan manipulado la información de forma que sus logros aparezcan maximizados y sus errores minimizados; c) *Como instrumento de financiación:* Trascendió en su día a la luz pública como Al Qaeda se financió gracias tanto al patrimonio de Bin Laden, como a la contribución de varias ONG. En la actualidad, expertos como Jimmy Gurulé[4] señalan a Bitcoin como el canal idóneo para la financiación del terrorismo. Actividades como el contrabando de petróleo que lidera el DAESH, pueden materializarse a través de pagos con esta cibermoneda; d) *Como instrumento de captación y movilización:* Mediante el uso de la red, el DAESH ha multiplicado el número de Foreign Fighters[5] que consiguió en su día movilizar Al Qaeda. El bombardeo a la población proclive a los postulados terroristas con imágenes y videos que muestran la cara amable de la vida de los muyahidines, así como sus éxitos contra el enemigo infiel (incluyendo la ejecución de los mismos),

4 Jimmy Gurulé, Adjunto al Fiscal General del Estado encargado de la lucha contra el terrorismo e Inteligencia Financiera

5 Término utilizado para denominar a los musulmanes que, desde distintos países se incorporan a la yihad que desarrolla el DAESH.

ha originado que el DAESH mantenga permanentemente abiertas sus "oficinas de información y reclutamiento en el mundo". Como habría de esperar, el éxito que el uso de esta tecnología ha tenido entre los jóvenes musulmanes del mundo ha sido muy considerable; e) *Como instrumento de trabajo en red y ocultación de estructuras:* La organización jerárquica de los grupos terroristas ha quedado prácticamente oculta ante el establecimiento de estructuras de comunicación y trabajo en red. Las estructuras verticales se han difuminado en favor de las horizontales por lo que células o miembros de distintos grupos terroristas pueden apoyarse, coordinarse y, en definitiva, planear ataques de una forma más segura y barata. En la red profunda, existen salas de chat donde los miembros de varias células terroristas pueden coordinarse para planear sus ataques de forma coordinada, realizar solicitudes, elevar consultas a la cúpula de la organización, etc. Al Qaeda llegó a todos los "hermanos de la yihad", utilizar PalTalk[6] al objeto de no ser detectados; f) *Como fondo documental:* En la deep web existen multitud de manuales y guías sobre fabricación de explosivos y técnicas de combate en población y tácticas guerrilleras.

La lucha contra el terrorismo dentro de la red, se ha centrado en la búsqueda de rastros de las comunicaciones entre los terroristas que han atentado o planeaban hacerlo y los responsables de esas organizaciones. En esas investigaciones, además de haberse conseguido generalmente demostrar la dependencia entre los terroristas neutralizados, ha quedado demostrada la enorme capacidad informática que poseen las organizaciones terroristas. En palabras de Jaquelyn S. Porth:[7]

> "Internet ha expandido drásticamente la capacidad de los grupos radicales de reclutar, entrenar, motivar y coordinar terroristas en vastas distancias sin tener un contacto directo. Los terroristas pueden consultar páginas webs para aprender las técnicas sobre como derribar helicópteros, ver videos de decapitaciones de rehenes, leer las cartas escritas por los kamikazes o escuchar los mensajes de los líderes militantes. Y aunque no hubiese páginas webs, Internet permite la divulgación de mensajes radicales, así como instrucciones operacionales enviadas por email.".

6. PalTalk es un programa informático de mensajería instantánea lanzado en junio de 1998. La característica principal del mismo es la posesión de salas de conversación con variedad de contenido que pueden ser creadas por los propios usuarios. En estas salas, los usuarios pueden enviar mensajes de conocimiento público o de forma privada a algún usuario en especial. Los usuarios de Paltalk también pueden tener sesiones de video chat privadas con hasta otros 15 usuarios.

7. Jaquelyn S. Porth, es la Jefa de los analistas de seguridad informática del Departamento de Estado de los EEUU.

El uso del ciberespacio para infringir el terror

Ciberespacio al servicio del terror del Daesh

El Daesh ya se ha convertido en un referente mundial e internacional de la yihad, llegando a superar en muchos aspectos a Al Qaeda. Muchos expertos en seguridad cibernética entre los que destaca Michael Rogers, Almirante de la US Navy y Director de la National Secutiry Agency[8] de los EEUU, opinan que en la actualidad, el DAESH aún no dispone de los medios apropiados para lanzar un ataque masivo contra occidente, pero también advierten que la adquisición de esas capacidades es cuestión de poco tiempo. Mientras en occidente estaba en estado de shock por los atentados contra el semanario Charlie Hebdo, miembros del DAESH consiguieron acceder a la web de Malaysia Arlines y bloquear la misma con el siguiente mensaje "Error 404- airplane not found. ISIS will win". Otra exhibición de capacidades, más grave aún si cabe, fue el pirateo de la cuenta en Twitter de uno de los operarios del USCENTCOM[9] y publicar en su nombre dos mensajes. Donde a modo de ejemplo solo se referencia dos extractos de cada uno de ellos, y donde en el segundo, se menciona el "cibercalifato" El primer mensaje fue: "Soldados americanos, estamos llegando, tened cuidado. ISIS". El contenido del segundo mensaje, comenzaba así; […] el Cibercalifato bajo los auspicios del ISIS sigue adelante con la Yihad cibernética. […]

Ese ataque sufrido por la Administración militar estadounidense mostró al mundo, no sólo la existencia de yihadistas con suficientes conocimientos informáticos, sino que el Gobierno de los EEUU no fue capaz de neutralizar el origen del ataque. Como dato a reseñar solamente en el año 2013, las pérdidas económicas de los 13.022 ataques informáticos realizados por delincuentes contra los EEUU, China y Alemania, superaron los 177 millones de euros (Symantec, 2013).

El autodenominado Estado Islámico está convirtiendo las redes sociales en una auténtica arma de guerra (Ávalos, 2016). El grupo ha usado todo tipo de redes sociales –Facebook, Whatsapp, Instagram, Twitter, Skype- y otras aplicaciones menos conocidas, como KIK o Diáspora, para extender su influencia entre todos los usuarios musulmanes e intentar reclutar nuevos simpatizantes. Diáspora es una plataforma que fue lanzada en 2010, impulsada por una campaña de *crowdfunding* creada por cuatro estudiantes de Nueva York. El equipo de soporte de Diáspora admitió que un gran número de integrantes de Estado Islámico había creado cuentas en esta plataforma tras

8 La National Security Agency (Agencia de Seguridad Nacional), es una agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información. Con este propósito en ella trabajan distintos tipos de especialistas como matemáticos criptógrafos, lingüistas, operadores de polígrafos, expertos en radiofrecuencias, programadores, hackers, etc.

9 El Mando Central de los Estados Unidos (USCENTCOM), es uno de los nueve Mandos Unificados del Departamento de Defensa de Estados Unidos. El USCENTCOM, concretamente es el Mando Unificado de Seguridad responsable de los intereses de Estados Unidos en 27 naciones y del mismo forman parte representantes del Ejército, Armada, Fuerza Aérea, Marines y Mando de Operaciones Especiales.

todas las prohibiciones llevadas a cabo tanto en Twitter, Facebook o Youtube, y que por el formato de la plataforma no es posible manipular las publicaciones, es decir, los mensajes que ellos publican no pueden ser eliminados.

Facebook, es quizá la más utilizada por los terroristas, utilizada por los fieles al régimen de Al Baghdadi para mostrar la brutalidad contra los infieles. Su objetivo es compartir imágenes de decapitaciones, bolsas llenas de extremidades, cabezas apiladas sobre la acera. En todas las publicaciones se mofan de las muertes del enemigo para lograr una radicalización mayor y una afiliación ulterior. Facebook también funciona como medio de financiación. Otra de las redes usadas es Instagram, y su finalidad es bastante similar a la de los occidentales. A pesar de que no se dedican a poner filtros y a subir fotos en playas paradisiacas, los adeptos del *Daesh* suben fotografías para mostrar su vida y dar envidia (Barrancos Larráyoz, 2014).

Esta similitud entre el uso de Instagram entre los occidentales y los yihadistas, se debe a que estos últimos, en su gran mayoría, proceden de países desarrollados. Así pues, los yihadistas intentan convencer a sus amigos occidentales, que aún no se han decidido a dar el paso, a través de fotos donde el lujo, las experiencias y la vida repleta de adrenalina, son el principal aliciente. Los terroristas utilizan Alrawi como medio para organizar sus ataques. Alrawi.apk se puede utilizar en dispositivos Android, pero no está disponible en Google Play, se descargaría de sitios web de internet. Amaq Agency es otra de las muchas aplicaciones relacionadas con el grupo terrorista que ha sido descubierta. En esta aplicación se distribuían noticias y propaganda yihadista. La aplicación se llama Amaq News y fue anunciada para Android por redes sociales cercanas a ISIS, en concreto la Agencia de noticias Amaq. 5elafabook (traducido como Califatobook). Es una plataforma creada por seguidores de Estado Islámico (El número 5, o jamsa, es utilizado en los chats en árabe para representar el sonido de la j). Empresas como Twitter ya se han movilizado para cerrar cuentas, cerrando más de 1000 cuentas en el último año, sobre todo a raíz de la publicación de videos sanguinarios donde se decapitaba a periodistas o a civiles (Marketing Directo, 2014).

Se calcula que existen hasta 46.000 cuentas de Twitter, que además emigran a otras plataformas como JustPaste, SoundCloud, VideoPres o Instagram. La propia Google, en su búsqueda de sugerencia, ha eliminado de la red la pregunta "¿Cómo unirse al estado Islámico?". El entramado digital del Daesh ya es comparado con el que pudiera usar cualquier Estado legítimo o una empresa occidental. Su facilidad para programar se evidencia en la creación de apps originales y propias como la llamada The Dawn of Glad Tidings, que estaba disponible a través de la tienda Google Play de Android.

La revista Dabiq, un magazine digital que ya cuenta con más de una decena de números y en la que se publica de forma periódica información del califato. El

ejemplar tiene una versión inglesa y francesa y está compuesta por unas 50 páginas coloridas, con ilustraciones y texto. La temática de la revista se centra en tratar los asuntos sobre los que se sustenta el pseudo Estado Islámico: 'Jamaa' (comunidad), 'Hégira' (migración), 'Manhaj' (búsqueda de la verdad), 'Tawhid' (unidad) y por supuesto 'yihad' (guerra santa) (Europa Press, 2015). El nombre de la revista está sacado de una batalla de Siria en la que ciertos mitos musulmanes vinculan con el apocalipsis. La intención de los terroristas es dar una impresión de mensaje apocalíptico, por ejemplo, la portada donde se ve colocada la bandera del Daesh sobre el obelisco del Vaticano.

Desde el punto de vista audiovisual, los videos del Daesh no tienen nada que envidiar a los creados por Hollywood. Los hay de todo tipo, desde grabaciones con smartphones hasta producciones de gran elaboración. Es evidenciable que muchos de los militantes dominan a la perfección el arte de la maquetación digital, la fotografía y la edición de video. Muchas productoras trabajan para el propio califato. Una de ellas es Al Furqan y otra es Al Hayat Media Center. Según David Barranco, analista del *think thank* especializado en ciberprotección THIBER, la propaganda de los videos del Daesh tiene cuatro objetivos: a) Infundir el miedo entre los soldados de los ejércitos enemigos; b) Fomentar el apoyo a la organización; c) Reclutar a nuevos militantes; d) Forjas nuevas alianzas con otras organizaciones terroristas (Think Thank Thiber, 2016).

Cada uno de los videos que la organización maqueta con recursos narrativos audiovisuales que se emplean con el objetivo de persuadir a la audiencia para moldear la mentalidad del receptor e influir en su pensamiento y comportamiento (Orellana, 2013). El mensaje que se prioriza en las producciones de *Al Hayat Media Center* es la llamada a la yihad. Sin embargo, esta se difunde variando la puesta en escena y mostrando diversas facetas de la organización en función del público objetivo al que se dirigen los contenidos audiovisuales. Hay cinco tipos de vídeos producidos por el Daesh: Nashid, Arenga, Mujatweet, Reportaje y Documental. A continuación, procederemos a explicarlos:

a) Nashid: Este tipo de videos se compone de imágenes que ilustran el texto de un cántico o nashid. Según Said Benham, un estudioso de estos cantares, el nashid es una música coral cantada a capela o acompañada de instrumentos de percusión. Originalmente sus textos hacían referencia a la historia y a las creencias del islam, aunque posteriormente se han ido incorporando temas políticos. El Daesh no permite el uso de instrumentos musicales, por lo que los cánticos prescinden de estos. Estos cánticos apelan no solo a la razón, sino al alma, y funcionan como un elemento seductor para los que practican la religión como nexo dentro del colectivo yihadista, creando una narración y pensamiento histórico colectivo. Los textos del nashid llaman a la

lucha, a la libertad y a recuperar la dignidad. Los primeros cánticos que la productora Al Hayat elaboró cantaban al odio, la violencia y el martirio. En estos videos siempre aparecen combatientes desfilando sonrientes y portando sus armas. La lucha en el frente por parte del Daesh se presenta como una aventura a la que sigue una fácil y rápida victoria que convierte al intrépido combatiente en un héroe. Todos los efectos que se aplican en posproducción son intencionados, con la misión de crear un ritmo vertiginoso y expectante. Por lo tanto, el nashid es un tipo de cántico incrustado en un video que se dirige con exclusividad a seguidores del grupo terrorista (Marshall, 2015).

b) Arengas: Este tipo de video es un video que se realiza al aire libre a partir de uno o varios oradores vestidos de combatientes que instan a los receptores a emprender la yihad. Aquí la imagen queda subordinada a la locución. En esta categoría de videos es donde encontramos los vídeos de asesinatos de rehenes, aunque estos no son el punto fuerte de la productora, donde los oradores lanzan amenazas al enemigo elegido y lo culpan de todo el mal. La cámara suele captar en plano detalle o primeros planos el rostro angustiado de la víctima. Normalmente se suele ralentizar el tiempo en el momento del asesinato, para así potenciar el terror que se quiere infundir en la audiencia (De La Fuente, 2016).

c) Reportaje: Este se fundamenta en potenciar la idea del califato del Estado Islámico como un lugar seguro, próspero, bien administrado y habitado pacíficamente por su sociedad, que vive bajo una Sharía armónica. Por ello, los guionistas contribuirán a remarcar las supuestas bondades del sistema, como "la ausencia de delincuencia", "la educación", "el sistema sanitario y judicial" etc. Asimismo, también tratan de demostrar la falsedad de las informaciones publicadas en distintos medios de comunicación que denuncian lo contrario. El reportaje se crea como un género objetivo, porque requiere de verosimilitud para que sea creíble. Los últimos videos de esta categoría utilizan la figura de John Cantlie para lograr una difusión mucho más amplia. Lo que se intenta así es que más familias se sientan atraídas por la supuesta comodidad del pseudo Estado y evitar que parte de la población abandone los territorios. También hay otro tipo de reportajes que no incluyen ninguna figura presentadora. En ellos, se utilizan declaraciones de personajes que actúan como testigos, muchas veces niños.

d) Mujatweets: híbrido de los términos mujahedeen y tweet. Estas piezas audiovisuales poseen una duración que oscila entre los treinta segundos y un minuto y medio. En su interior encontramos un tipo de video que trata de mostrar breves pinceladas de la vida cotidiana y mundana que se desarrolla dentro de los territorios conquistados por el Daesh. Estos no tienen nada que ver con los videos violentos que

hemos explicado antes. La atmósfera del mujatweet es amable y optimista. Se sigue llamando a la yihad, pero de una manera más sutil y cordial. Los protagonistas de estos videos tweets son personas de la población civil y sobre todo niños. Esta vez, cuando aparecen combatientes lo hacen de manera confortable y alegre: sonríen a la cámara, juegan con los niños y realizan actividades sociales. Con estos se quiere dar una imagen de amables protectores de la sociedad.

e) Documentales: Estos videos tratan de justificar las acciones del Daesh, todas ellas, incluso las que vulneran los derechos humanos. El primer documental, "Llamas de la guerra", se lanzó en 2014. Su estreno llevó una cobertura similar a la de una película de Hollywood: se emitieron trailers, banners y anuncios (De La Fuente, 2016). Estos documentales, por norma general, narran cómo la sociedad perfecta que fundó el Profeta se ha ido carcomiendo por el efecto de los cruzados e infieles. Ante esto proponen abandonar todas las costumbres corruptas y regresar al más puro origen del islam. Federico Aznar (2014), describe los argumentos de los documentales como historias que parten siempre desde una arcadia feliz que permite explicar el futuro utilizando el pasado; o para ser más exactos, reescribir el pasado en nombre del futuro (Aznar, 2014).

Ciberespacio al servicio del terror de Al Qaeda

Se calcula que, en los últimos veinte años, al menos 3800 mensajes audiovisuales fueron emitidos por parte de Al Qaeda, un total de 1.100 horas de emisión. Esto ha sido posible gracias a la famosa agencia de comunicación As Sahab, que gestiona toda la propaganda del grupo en cuestión, emitida en árabe y urdu. Al Qaeda cuenta también con una revista corporativa, la denominada Resurgence. Esta sí que está escrita en inglés para así llegar al mayor número de personas posibles. Los temas de tratamiento de este ejemplar se focalizan en la marginación, persecución y exterminio al que se ven sometidos los musulmanes alrededor del mundo. También hacen un llamamiento a los adeptos para promover la destrucción de oleoductos, gaseoductos y pasos marítimos para atacar de manera indirecta a las economías occidentales (Baños, 2014).

Al Qaeda y sus diversas ramificaciones han otorgado una enorme importancia a la Internet. A partir del ciberespacio y el código binario, los terroristas han descubierto un medio cifrado y gratuito por el que poder difundir comunicados, consignas e información técnica de adiestramiento y adoctrinamiento. De por sí, Al Qaeda es el grupo terrorista con más ramificaciones. Su estructura es según muchos autores, como un "nodo disperso que opera con cierta independencia". Las ramificaciones tienen su "empresa matriz" en Pakistán (AQ), y las diversas franquicias en diversos puntos

del globo: AQMI (Al-Qaeda en el País del Magreb Islámico); AQI (Al-Qaeda en Iraq); AQAP (Al-Qaeda al Yihad en la Isla Arábiga); AQEA (Al-Qaeda en el Este de África-Somalia); AQ y JI (Al-Qaeda y la Jemaah Islamiyah en Indonesia). Todas estas franquicias deben establecer comunicación entre ellas, y la Internet ha sido la herramienta perfecta para ello (Estallares & López, 2011).

La denominada Brecha tecnológica siempre ha jugado a favor de los de Al Zawahiri, ya que la ingente cantidad de tráfico de datos circulando a una velocidad de vértigo por la red ha sido y es imposible de analizar en su totalidad. Las agencias de seguridad fueron incapaces de interceptar los atentados del once de septiembre (11S) en los EE.UU y los ataques posteriores (Bamford, 2008).

Al-Qaeda ha desarrollado a lo largo de este siglo numerosas armas de comunicación, como correo electrónico cifrado, la esteganografía (envío de imágenes con datos ocultos) o los semáforos electrónicos (imágenes previamente reconocidas por los receptores cuyos colores de fondo cambian dependiendo del tipo de mensaje que quiera transmitirse). Los sites yihadistas más populares han sido 'Ansar Al-Jihad Network' y 'Al-Mojahden Electronic Network'. Estos son muy llamativos por la habilitación de foros en los que se puede interactuar directamente con la banda criminal e informarse de los últimos comunicados, videos y mensaje reivindicativos. Así se han conformado unos mensajes que cada vez elevan más el tono amenazante, ya no solo dirigido a los gobernantes sino también a las poblaciones civiles.

Ciberespacio al servicio del terror Talibán

Desde que los talibanes iniciaron su ofensiva contra el gobierno afgano han sabido siempre usar la comunicación. Desde un principio elaboraron periódicos y revistas mensuales, quinquenales diarios etc. Su principal arma es la revista digital Al Somood, considerada como la publicación oficial del Estado Islámico de Afganistán. Se lleva publicando desde 2006. Su agencia oficial de producción es Al Emara, aunque existen otras agencias que se encargan de la producción, difusión y edición de sus videos. Entre 2004 y 2012 emitieron 125 mensajes de audio/video, contabilizando un total de casi 74 horas de emisión. En abril de este mismo año Google retiraba una app de propaganda talibán de su Play Store. Esta aplicación trataba de aumentar la visibilidad en las redes de la organización extremista a partir de vídeos y proclamas en pastún (idioma empleado en algunas provincias de Pakistán y Afganistán). La aplicación intentaba replicar el éxito que ha tenido el Daesh con su estrategia propagandística. Actualmente los talibanes tienen un canal en el servicio de mensajería encriptado Telegram y páginas webs en varios idiomas, además de cuentas en todas las redes sociales convencionales (Baños, 2014).

Ciberespacio al servicio del terror de Al-Shabbaab

En Somalia la Fundación Al Kataib, produce y difunde videos de gran calidad en los que el mensaje principal es que Al-Shabbaab es tan solo un elemento más de un conflicto a escala planetaria en el que el islam está amenazado. Su público objetivo es tanto el pueblo somalí como la amplia diáspora repartida por todo el mundo. El grupo utiliza Twitter, con gran frecuencia para desmentir las declaraciones oficiales de las fuerzas de la Unión Africana. En diciembre de 2011 comenzó a comunicar a través de una cuenta llamada HSMPress, que logró afianzar más de 8.000 seguidores y disponen de una propia emisora de radio denominada Al Andalus, con la que llegan a los rincones más recónditos de Somalia. Algo que también llama la atención es su paradójica utilización de la música. El conocido líder de al Shabbaab Abu Mansoor Al-Amriki ganó numerosos adeptos y colocarse en el centro de atención mediático gracias a un video que subió a la red en el que interpretaba una canción de rap ensalzando la yihad (De La Corte Ibáñez, 2015).

Ciberespacio al servicio del terror de Boko Haram

Boko Haram cuyo nombre traducido al español significa "la Educación es Pecado" es el nombre de un grupo terrorista internacionalmente reconocido que actúa en el continente africano, exactamente dentro de las fronteras nigerianas. Nigeria es el país más poblado de África y el segundo más rico del continente gracias a su producción de hidrocarburos (Echevarría, 2014). Boko Haram se ha transformado en el verdadero conflicto intercomunitario en Nigeria, aprovechando la rivalidad entre cristianos y musulmanes para alimentar su combate yihadista. En 2010, fueron asesinadas 500 personas a manos de granjeros Fulani en choques intercomunitarios en Jeji, Ratsat, Nahaua y Fulani. Esta matanza fue alimentada por Boko Haram, que radicalizó a los susodichos para que mataran con cuchillos y armas. Los mensajes de incitación fueron transmitidos vía teléfono móvil. Boko Haram también utiliza masivamente la diseminación de mensajes por video, así como el apoyo que le brinda también AQMI a través de su sofisticado Instituto de Comunicación Al Ándalus. (Zenn, 2012).

Ciberespacio al servicio del terror de Jabhat al Nusrah

El Frente Al Nusrah, considerado como el brazo armado oficial de Al Qaeda en Siria, tiene también una dinámica comunicativa personal. Posee una revista que resume las actividades que lleva a cabo en la guerra y se titula: Monthly Harvest, dedicando un espacio significativo para promover la Dawwa de la organización, así como sus obras de caridad. Por ejemplo, aparecen fotos publicadas donde se muestra

a miembros de la organización realizando una campaña de vacunación contra la poliomielitis (Baños, 2014). De esta manera intentan ganarse el apoyo de la población local y demostrar que el plan del grupo beneficia a Siria. Mucha población local está intentado resistir a la implantación de la ideología de Al Qaeda y por ello están realizando este tipo de acciones. También produce videos gracias a una agencia de comunicación llamada Himam News Agency. Estos productos audiovisuales van desde reportajes hasta comunicados de calidad. También disponen de otra agencia –Al Manarah Al Bayda Foundation for Media Production-, que se encarga de distribuir los videos más recientes. Otro de los puntos fuertes de la comunicación de Al Nusra es el Twitter. El hecho de que el grupo terrorista sea poco conocido frente a la predominancia del ISIS, hace que sus mensajes pasen más desapercibidos. El grupo posee diez cuentas oficiales en la red social. De entre esas diez, una cuenta es la principal y las restantes son meramente secundarias. El diseño de la cuenta siempre es muy neutral. No utilizan símbolos de la banda ni elementos que llama la atención. Otra de sus técnicas es utilizar viejas cuentas inutilizables y cambiarles el contenido de manera cuidadosa, para así evitar las nuevas políticas de afiliación. Si bien no hay quién destrone al Daesh en contenido audiovisual, Al Nusra demuestra un uso más eficiente.

Conclusión

La investigación de los casos de terrorismo en que los presuntos terroristas han usado Internet u otros servicios conexos suele exigir el uso de tipos especializados de facultades de investigación por los organismos encargados de hacer cumplir la ley. Una respuesta eficaz ante las amenazas que plantea el uso de Internet por los terroristas exige que los gobiernos establezcan políticas y leyes nacionales claras que se ocupen, entre otras cosas, de: a) Penalización de los actos ilícitos cometidos por terroristas a través de Internet o servicios conexos; b) Otorgar facultades especiales de investigación a los organismos de seguridad encargados de las investigaciones relacionadas con el terrorismo; c) Regular de los servicios relacionados con Internet, sus proveedores y el control de su contenido; d) Alentar la cooperación internacional; e) Desarrollo de procedimientos especializados judiciales o probatorios; f) Las autoridades necesitan la cooperación de los operadores de telecomunicaciones cuando recurren a la monitorización electrónica, y técnicas de investigación electrónica.

Referencias

Ávalos, J. M. (2016). La comunicación de los grupos terroristas: Estado Islámico (Daesh). Instituto de Seguridad Global.

Aznar, F. (2014). El papel de la narrativa en el terrorismo. En Aznar, F., Baca, E. & Lázaro, J. La guerra contra la violencia. Madrid: Triacastela.

Bamford, J. (2008). The Shadow Factory. (The Ultra Secret NSA from 9/11 to the Eavesdropping on America): The Echelon Program. Doubleday.

Baños, P. (2014). Medios y modos de comunicación de los grupos extremistas. Documento digital.

Barrancos Larráyoz, D. (2014). Los community managers del terror: la propaganda online de ISIS y su ofensiva sobre Irak (Artículo de opinión). Madrid: Instituto Español de Estudios Estratégicos.

Clarke, R. & Knake, R. (2010). Cyber War. The next Threat to National Security and What to Do about It. Nueva York: Harper Collins.

Castells, M. (1999). La Era de la Información: Economía, Sociedad y Cultura. La Sociedad Red. México: Siglo XXI.

De La Corte Ibáñez, L. (2015). Al shabaab en el cuerno de África (Documento de Investigación). Madrid: Instituto Español de Estudios Estratégicos.

De La Fuente, P. (2016). La propaganda de reclutamiento del Daesh a través de sus videos (Documento de Opinión). Madrid: Instituto Español de Estudios Estratégicos.

Echevarría, J. C. (2014). El desafío terrorista de Boko Harama en Nigeria. Colección: "Grupos militantes de ideología radical y carácter violento, 1". Madrid: Instituto Español de Estudios Estratégicos.

Estallares & López, J. (2011). Los medios de comunicación de Al Qaeda y su evolución estratégica (Documento de Opinión). Madrid: Instituto Español de Estudios Estratégicos.

Jordán, J. (2013). "Manual de Estudios Estratégicos y Seguridad Internacional".

Nye, J. (2011). Nuclear lessons for Cyber Security? (18-38). Strategic Studies Quarterly, Invierno.

Kaldor, M. (2001). Las nuevas guerras. Violencia organizada en la era global. Barcelona: Tusquets.

Kaplan, R. D. (1994). The coming anarchy. The Atlantic Monthly.

Marshall, A. (2015). How Isis Got its Anthem. The Guardian.

Orellana, J. (2013). Fundamentos de narrativa audiovisual. Madrid: CEU Ediciones.

Patterson, L. (2002). Information Operations and Asymmetric Warfare…are we ready?. Pebbsylvania: US Army War College.

Sánchez Medero, G. (2010). La nueva estrategia comunicativa de los grupos terroristas. Revista Enfoques, 8(12).

Symantec. (2013). Reporte Norton 2013. Norton by Symantec. Recuperado de http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Torres Soriano, M. R. (2015). ¿Es el yihadismo una ciber-amenaza? (20-34). Revista de Occidente, 406.

Weiman, G. (2004). www. Terror. Net: How modern terrorism uses the Internet. United States Institute of Peace.