Ciberterrorismo. Concepto y aproximación al fenómeno

PID_00272036

Josep Maria Tamarit Sumalla
Mª del Carme Guirao Cid

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Josep Maria Tamarit Sumalla

Catedrático de Derecho Penal en la Universitat Oberta de Catalunya, donde es director del máster de Ciberdelincuencia. Su actividad de investigación se ha centrado básicamente en aspectos relacionados con la victimología, la justicia restaurativa y el sistema de sanciones penales. También ha escrito varias publicaciones relacionadas con la delincuencia de motivación ideológica y los delitos de odio. Es coordinador del grupo consolidado de investigación sobre el sistema de justicia penal.

Mª del Carme Guirao Cid

Graduada en Criminología por la UOC y máster de Derechos Humanos por la misma universidad. Es becaria predoctoral en la Universidad de Lleida, donde realiza su tesis doctoral sobre adoctrinamiento y victimización terrorista, un tema sobre el cual ha publicado dos artículos (2018; 2019).

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2020)

Primera edición: febrero 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

Las tecnologías de la información y la comunicación (TIC) son en la actualidad una poderosa herramienta para extremistas y grupos terroristas, que aprovechan la versatilidad de la red para promover su ideología y ampliar el círculo de sus futuras víctimas. Una de las principales amenazas del ciberterrorismo es que se produzca un ciberataque contra una infraestructura crítica, como puede ser un centro de telecomunicaciones, un aeropuerto, una central nuclear o un centro de inteligencia, por contener información sensible y estratégica. Pero no deben pasar desapercibidos otros riesgos que un adecuado estudio del fenómeno puede revelarnos.

En los próximos apartados explicaremos el ciberterrorismo centrándonos en las acciones perpetradas por organizaciones terroristas de base religiosa, como Al-Qaeda y Dáesh por ser sus máximos exponentes en la actualidad y por el temor y la inseguridad que suscita pensar que algunas de las ciberamenazas pudieran materializarse. De hecho, algunas series de ficción, como *El Príncipe*, emitida por una cadena de televisión española, han emulado la posibilidad de que un grupo de este tipo acabara cometiendo un ciberataque contra instalaciones críticas. No obstante, resulta hasta cierto punto contradictorio, o al menos paradójico, que grupos que se dedican a combatir a los países occidentales por concebirlos demasiado modernos y transgresores por medio de un discurso basado en el islam más tradicional hayan decidido utilizar las TIC para luchar contra el progreso.

El módulo se estructura en cuatro apartados. El primero está dedicado a conceptualizar el término *ciberterrorismo*, a extraer sus aspectos más característicos y a diferenciarlo de otras ciberconductas. En el segundo y tercer apartado describiremos las estructuras mediante las que actúan las organizaciones terroristas, así como las actividades que realizan en ellas. Por último, describiremos en profundidad cómo se lleva a cabo el proceso de la radicalización por la red, la ciberradicalización.

Objetivos

Los objetivos que se pretenden conseguir con el estudio del presente módulo sobre aspectos conceptuales del ciberterrorismo son los siguientes:

1. Definir el ciberterrorismo y cuáles son sus características distintivas.

2. Diferenciar el ciberterrorismo de otras modalidades cibercriminales.

3. Conocer cuáles son las estructuras mediante las que actúan las organizaciones terroristas.

4. Conocer los tipos de actividades que llevan a cabo las organizaciones terroristas en ellas.

5. Conocer en profundidad el proceso de ciberradicalización y los perfiles de los cibervictimarios y las cibervíctimas.

1. El ciberespacio: nuevas oportunidades para los delitos de terrorismo

1.1. Factores de riesgo en el ciberespacio

La creación del ciberespacio ha procurado una amplia disponibilidad de herramientas de desarrollo efectivas, y de bajo coste, que han contribuido a generar nuevas oportunidades para la comisión de delitos. En el ámbito del terrorismo, la disponibilidad de conocimiento gratuito en línea ha permitido a las organizaciones terroristas desarrollar sus métodos y realizar actividades ilegales y ataques de manera remota, causando daños a bienes jurídicos para alcanzar sus objetivos.

El entorno en línea tiene unas características que lo hacen más atractivo que el fuera de línea, al permitir al cibervictimario realizar sus actos más allá de los límites que le impone el espacio físico. Como señala Wall (2007), estos «nuevos» delitos han pasado a formar parte de las agendas políticas de los estados, ya que lo que más preocupa de ellos no es el hecho de que puedan cometerse desde ordenadores o medios portables, sino que todos están conectados al ciberespacio, un ámbito de comunicación transnacional que permite operar independientemente de las variables espaciotemporales, es decir:

> El cibervictimario puede actuar desde cualquier sitio y hacia cualquier lugar, independientemente de la distancia. Incluso puede cometer delitos simultáneamente en distintos lugares, provocando así redes distribuidas de víctimas (Miró, 2011; Jahankhani, Al-Nemrat y Hosseinian, 2014).

Como sabemos, las personas solemos actuar impulsadas por la consecución de un objetivo y sobre la base de una motivación. Sin embargo, no está garantizado que podamos alcanzar los objetivos pretendidos a causa de las barreras (tanto externas como internas) que nos lo dificultan o nos lo impiden. Autores como Suler (2004) y Agustina (2014) han estudiado el papel que tiene el entorno «ciber» para desarrollar una mayor desinhibición en los individuos. De esta manera, han identificado las siguientes características de la comunicación en el ciberespacio:

1) Anonimato disociativo: se erige como el efecto principal de la desinhibición, por ser el responsable de que podamos navegar por la red sin temor a ser descubiertos. Las características de las arquitecturas digitales han desarrollado

un conjunto de mecanismos que garantizan el anonimato al victimario, dificultando así la tarea de los cuerpos de seguridad para rastrear sus datos. Esto ha permitido crear nuevas variedades de amenazas criminales.

Una consecuencia directa que deriva del anonimato disociativo es la posibilidad que se brinda al individuo de poder separar el «yo» real del «yo» digital, permitiéndole actuar por medio de una representación virtual de él. Esto favorece que el individuo construya un segundo yo, que tampoco tiene por qué ser el único, sino que, fruto de las características que presenta la red, se le permite elaborar más de uno, lo que desencadena identidades múltiples (Becoña, 2016).

2) Invisibilidad: por una parte, permite al sujeto actuar sabiendo que difícilmente se le podrá atribuir la autoría de la conducta. Por otra parte, sabe que puede visualizar contenidos privados de otros individuos sin que estos lo sepan. Esta característica ha llevado a Jahankhani, Al-Nemrat y Hosseinian (2014) a hablar de «sinopticismo y panopticismo», refiriéndose a la capacidad de vigilancia que otorga el ciberespacio al victimario para controlar a sus víctimas de manera remota.

3) Comunicación asincrónica: si bien las TIC han permitido eliminar las variables de espacio y tiempo de la comunicación interpersonal, ello no garantiza que las reacciones a la conducta del emisor vayan a producirse de manera inmediata por parte del receptor, y pueden demorarse desde minutos a horas, o incluso días.

4) Introyección solipsista: la ausencia de interacción física favorece la consolidación de lazos y la desindividualización del sujeto a favor de una identidad grupal. Cuando la persona recibe un mensaje o lee una aportación realizada en un foro, percibe esta información como la «única» existente y veraz. A partir de ese momento, se pone en duda toda información que proviene de una fuente externa al endogrupo.

5) Minimización del estatus y de la autoridad: en el mundo fuera de línea, la autoridad y el poder son dos de las cualidades que describen un tipo determinado de personalidad que puede llegar a ser anhelada. En el ciberespacio, el peso que tienen ambos elementos se reduce, haciendo que cualquier persona tenga las mismas oportunidades de hacerse con ellos. De hecho, la máxima de internet es «todos somos iguales en la red». Todo el mundo puede compartir sus opiniones libremente con los demás (Suler, 2004).

La suma de estos factores contribuye a disminuir el umbral de riesgo percibido por el sujeto y a aumentar la probabilidad de que acabe cometiendo un delito.

Ved también

Las estructuras web utilizadas por las organizaciones terroristas serán objeto de estudio en el apartado 1 del módulo 2.

1.2. El atractivo del ciberespacio para la organización terrorista

En el apartado anterior hemos descrito las características generales del ciberespacio. Ahora, partiendo del estudio de Weimann (2017), nos centraremos en el atractivo que encuentran los ciberterroristas en su uso. Como podremos ver, algunas ya se han descrito anteriormente.

- Las aplicaciones y los medios que ofrece internet suponen un **abaratamiento** de los costes en comparación con los métodos terroristas tradicionales, puesto que lo único que se requiere es un ordenador, un móvil o una tableta con conexión a internet. Son medios que en la actualidad están a disposición de un amplísimo número de personas. No hacen falta armas o explosivos.

- El terrorismo llevado a cabo por la red permite la **circulación libre y el anonimato** a los perpetradores mediante el uso de apodos en línea o la posibilidad de conectarse con perfiles falsos, lo que dificulta a las agencias de seguridad rastrear las verdaderas identidades de los terroristas.

- La falta de límites de la red ha permitido a las organizaciones descubrir nuevos medios de adquisición de materiales para perpetrar atentados en el mundo real (materiales para fabricar explosivos, armas, drogas, etc.); por ejemplo, por medio de la ***darknet***.

- El ciberterrorista puede dirigir desde su ordenador su acción contra **multitud de objetivos**, ya sean gobiernos, individuos o servicios públicos o privados, una vez detectadas sus debilidades, siendo las más vulnerables las instalaciones de energía eléctrica a causa de la complejidad de sus infraestructuras y sistemas informáticos.

- Las características de la red permiten **ensanchar el círculo de posibles víctimas**, que pueden clasificarse en tres grupos:
  - el primero englobaría a partidarios y simpatizantes de la organización, que se tornan más vulnerables a ser reclutados y adoctrinados;
  - el segundo englobaría a instituciones y sistemas de infraestructuras críticas de la comunidad internacional; y,
  - el tercero englobaría a individuos o a colectivos tradicionalmente concebidos como «enemigos».

- Los atentados pueden ejecutarse de manera **remota**, lo que significa que al ciberterrorista ya no se le requiere entrenamiento físico, y las posibilidades de morir durante el atentado disminuyen, lo que garantiza la supervivencia de la organización.

2. Qué es el ciberterrorismo

2.1. Evolución de la presencia de organizaciones terroristas en la red

La amenaza ciberterrorista ha ido gestándose con el paso de los años. A continuación resumiremos sus inicios hasta situarnos en el momento actual.

La primera aparición de organizaciones terroristas en la red la encontramos en la segunda mitad de la década de los noventa, coincidiendo con la fundación de la organización Al-Qaeda. Es en este momento cuando aparecen los **primeros sitios web con contenidos de carácter islamista radical**, pero sin que su presencia generase ningún tipo de alarma. Más bien pasaron desapercibidos en Occidente, ya que estaban editados en árabe y el incipiente desarrollo de la red contribuyó a que las tareas de difusión se realizaran en el mundo físico.

En 2002 se inicia un nuevo período, que podríamos denominar «profesionalizador», caracterizado por el abandono progresivo (pero no la desaparición) de las webs. En este período, las organizaciones prefieren destinar sus recursos a **crear sus productoras de comunicación** con el objetivo de controlar la elaboración, la edición y la distribución del material ideologizador. Al-Qaeda funda As Sahab, y Dáesh funda Al Hayat y Al Furqan, aunque en este caso se estima que el número de productoras superaría la treintena, lo que demuestra el poder logístico de la organización. En ambos casos, el material se elabora en diversos idiomas, siendo el inglés, el francés, el alemán y el ruso los más utilizados. Este cambio de perspectiva a la hora de gestionar la difusión de su mensaje hizo que se produjera un aumento de contenido en la red, así como un incremento del número de seguidores, lo que contribuyó a un creciente interés por materiales con contenido extremista radical. Otro hecho que se produce en esta etapa es el **desarrollo de foros y de chats** destinados a promover el intercambio de información entre los usuarios, pudiendo actuar cada uno como agentes radicalizadores, que a su vez son adoctrinados por otros miembros, y derivan así en una espiral adoctrinadora. En este caso, las comunicaciones que se llevan a cabo en estos espacios son en árabe, lo que constituye un elemento de seguridad frente a posibles intromisiones por parte de las fuerzas de seguridad.

Más recientemente, desde 2007, cabe describir una tercera etapa que se corresponde con el **surgimiento o auge de las redes sociales** (p. ej. Facebook, Twitter, Instagram o Telegram), así como la mayor popularidad de plataformas audiovisuales como YouTube. Esto ha permitido a las organizaciones dotarse de mejores herramientas a la hora de difundir su mensaje y llegar a un número cada vez mayor de individuos. Incluso, como veremos con más profundidad

Ved también

Las modalidades de captación, reclutamiento y adoctrinamiento por internet serán objeto de estudio en el apartado 4 del presente módulo.

cuando analicemos el proceso de la ciberradicalización, la interacción virtual ofrece a la organización la oportunidad de dirigirse directamente, de manera selectiva, a aquellos simpatizantes que por la información que publican o las respuestas de apoyo que reciben en sus perfiles son más receptivos a su mensaje, y por lo tanto les convierte en individuos más vulnerables a la captación y a la posterior radicalización. Es lo que denominamos «radicalización pasiva». Además, y continuando con la finalidad para la que fueron creados los foros, la mayoría de las redes sociales incorporan aplicaciones de chat y de mensajería mediante las que los miembros de estos perfiles pueden interactuar entre ellos y compartir información escrita (documentos o mensajes escritos), visual (gráficos, infografías, imágenes), auditiva (p. ej. *nasheeds*) y audiovisual (vídeos).

2.2. Terrorismo, TIC y nativos digitales. Una amenaza real

El terrorismo no constituye una fenomenología criminal homogénea. En el interior de los grupos hay discrepancias que pueden fraccionarlos y dar lugar a otros nuevos. Un ejemplo de ello es el nacimiento de Estado Islámico (también denominado EIIL, EI o Dáesh) en 2010 como escisión de Al-Qaeda en plena guerra siria, que hasta entonces era el grupo hegemónico. El auge de Dáesh difícilmente puede entenderse sin analizar el papel que han tenido las nuevas tecnologías. Sin ellas seguramente no hubieran podido reclutar a tantas personas, obtener donaciones y presentarse como un desafío superior frente a enemigos militarizados y mejor capacitados que ellos. Una muestra de la importancia que dan a las TIC está en el hecho de que los miembros de la organización dedicados a su gestión reciben el título de emires y reciben un salario superior al resto, además de otros beneficios (Torres, 2016). Por todo ello, se considera que Dáesh ha sido la organización terrorista que ha alcanzado el grado más elevado de sofisticación y eficacia, pudiéndose comparar sus producciones con la estética propia de Hollywood. No obstante, tras años de guerra y la pérdida de control territorial, Dáesh ha quedado debilitado y ello ha contribuido al renacimiento de la organización Al-Qaeda con el hijo de Osama bin Laden, Hazam bin Laden, como líder.

Las productoras de comunicación

Estas productoras no solo elaboran y distribuyen el material, sino que estudian la mejor manera de difundirlo con el objetivo de que llegue al máximo número de personas.

El primer grupo terrorista que utilizó la red para sus beneficios fue Al-Qaeda, cuando en 2011 hizo un llamamiento a sus seguidores mediante el video *For Incitement and Publishing: You Are Held Responsible Only for Yourself, Parts 1 and 2*, para que cualquier musulmán con conocimientos informáticos realizara ciberataques contra sitios web y redes electrónicas de las grandes empresas «enemigas de los musulmanes». Sin embargo, la fundación de un cibercalifato capaz de realizar ciberataques no tiene lugar hasta fechas más recientes. Esto se debe, según Torres (2018), a dos motivos:

- En primer lugar, las organizaciones terroristas no se atreven a apostar por el mundo virtual hasta que perciben el éxito que son capaces de conseguir grupos hacktivistas, como Anonymous o WikiLeaks.

- En segundo lugar, para realizar este tipo de acciones se requiere del desarrollo de una determinada capacidad operativa y humana que el grupo debe ir desplegando.

Es frecuente señalar que, si bien el ciberterrorismo empieza a preocupar cada vez más a las instituciones, especialmente en los países occidentales, por el momento no se han reportado acciones terroristas significativas en el ciberespacio, lo que no significa que no se observen año tras año incrementos de estas actividades. Ni Al Qaeda ni ninguna otra organización terrorista parece haber tratado de organizar, por el momento, un ciberataque grave. Sin embargo, podemos localizar la primera acción ciberterrorista con una notable envergadura en 2007, con el ataque cibernético que sufrieron los sitios web de algunas instituciones estonias y la programación del canal francés *TV5 Monde*, cuyas emisiones quedaron interrumpidas durante dieciocho horas, incidentes que provocaron la emisión de un comunicado por parte del Parlamento Europeo. Estas acciones ponen de manifiesto la capacidad que empiezan a tener las organizaciones terroristas en la red.

Por el momento, se estima que en Europa la organización terrorista Dáesh ha conseguido captar a 35.000 individuos, mujeres y hombres, por la red. En el caso concreto de España, según datos del Ministerio del Interior publicados en el informe *Ciberamenazas y tendencias* de 2017, las organizaciones terroristas han interferido en el funcionamiento normal o incluso se han hecho con el control momentáneo de algunas empresas o instalaciones del sector público y privado, limitándose a desconfigurar los sitios web, redirigir sus direcciones o realizar pequeños actos maliciosos.

En marzo de 2019, los medios de comunicación informaron de que el califato de la organización Dáesh había sucumbido tras la pérdida del último bastión sirio que tenían en posesión. No obstante, este hecho no parece que vaya a frenar su actividad, dado que el terreno físico perdido ha sido sustituido por el virtual. Es decir, la destrucción de santuarios físicos ha ido acompañada de la creación de santuarios virtuales (Cano, 2019), una realidad que vaticinó Abdel Bari Atwan en 2015 al defender que sin la tecnología digital sería bastante improbable que organizaciones terroristas como estas pudiesen llegar a existir o subsistir. Según Cano, la mayoría de quienes se sienten atraídos por contenidos próximos al ciberterrorismo son adolescentes, lo que no sorprende si se tiene en cuenta que un 89 % de ellos tiene un comportamiento activo en la red y un 70 % usa a diario los medios sociales, pasando un total de diecinueve a veinte horas semanales conectados. Estas características suponen una ventaja para la organización, ya que sus integrantes responden al perfil de «**nativos digitales**» de Prensky (2011). El citado autor advierte que estos individuos pertenecen a una generación que ha nacido y se ha formado en las nuevas tecnologías, lo que les hace ser individuos que prefieren:

- recibir información en formato audiovisual (preferiblemente en gráficos e imágenes) y en un plazo inmediato;

- aprender de forma autodidacta y en un medio lúdico;
- trabajar en red; y
- acceder por un único documento a otros, mediante enlaces directos.

El perfil de estos jóvenes es opuesto al de los «inmigrantes digitales», sujetos que han tenido que aprender a utilizar las TIC por nacer en una época previa a ellas, y que tienden a continuar utilizando las herramientas de interacción del mundo fuera de línea. En el plano económico y de seguridad, disponer de nativos digitales resulta beneficioso para la organización. Por una parte, no se requiere invertir grandes cantidades de tiempo ni de dinero en su formación en entornos digitales, y, por otra parte, se adquiere mayor capacidad operativa respecto a la evolución tecnológica, lo que les permite escapar al rastreo de las fuerzas de seguridad.

Hay voces que lanzan alarmas de que en un futuro próximo, si las organizaciones continúan centrando sus esfuerzos en el ciberespacio, podrían consolidar la **incipiente yihad cibernética** y provocar graves perjuicios económicos, sociales y de seguridad, al poder afectar instalaciones tan sensibles como las centrales nucleares, que están controladas por dispositivos tecnológicos susceptibles de ser atacados; algunos expertos, sin embargo, consideran exageradas las alarmas dado el nivel de seguridad de los centros nucleares frente a los ciberataques (Weimann, 2004; Ruiz, 2016).

2.3. Definición y características principales

El uso de internet por parte de grupos terroristas como medio para lograr algunos de sus fines es conocido desde principios de los años noventa. En 1999, la Agencia de Inteligencia de la Defensa norteamericana avisó de su inminente irrupción. No obstante, no se habló del término *ciberterrorismo*, sino que se prefirió utilizar el de *guerra informática* (*infowarfare*). A pesar de ello, en la década de los ochenta **Barry Collin**, investigador principal del Instituto de seguridad e inteligencia de California, ya utilizó el término para hacer referencia a «la convergencia de la cibernética y el terrorismo». Es decir, la convergencia entre el mundo virtual y el real. Después de los atentados del once de septiembre, el ciberterrorismo se consideró una amenaza real y global. Por ejemplo, tras su comisión, las instituciones encargadas de velar por la seguridad tuvieron que cambiar la concepción de terrorista para adoptar otra en la que el ciberespacio tenía un papel relevante. A partir de ese momento, algunas plataformas vinculadas al yihadismo fueron objeto de ciberataques, o su contenido fue bloqueado (Torres, 2016). Aun así, hoy en día carecemos de una definición. Los motivos que explican esta realidad son principalmente tres (Brickey, 2012; Luiijf, 2014; Mayer, 2018):

- El primero reside en la propia **naturaleza del concepto**, por ser el resultado de la unión de dos términos distintos, *ciber* y *terrorismo*.

- El segundo lo encontramos en el **auge de interés** que generó su estudio entre 1997 y 2001, por parte de diferentes disciplinas, lo que derivó en una amplia gama de definiciones.

- El tercero fue la **confusión terminológica** entre el término *ciberterrorismo* y otros de naturaleza similar (profundizaremos en ello en el próximo punto).

Para entender el concepto, la mejor opción es analizar el significado de cada uno de los términos que lo conciben. De este modo, entenderemos ***ciber*** como el prefijo que se utiliza para indicar que la acción se lleva a cabo en el ciberespacio y que implica el uso de medios electrónicos o de internet; llevado al ámbito del terrorismo, nos conduce a afirmar que internet se convierte tanto en un objetivo como en un arma utilizada por parte de los terroristas, ya que usan el ciberespacio para tareas de organización, control, intercambio, planificación de información, recaudación de fondos e intentos de aumentar su apoyo, difusión de propaganda ideologizadora y para tareas de reclutamiento (Luiijf, 2014). Entendemos el ciberespacio como el dominio global dentro del entorno de la información formado por redes e infraestructuras interdependientes que incluyen internet, las redes de comunicación y los sistemas informáticos (Ruíz, 2016).

Por ***terrorismo*** debe entenderse «el uso o la amenaza de una acción dirigida a influir en el gobierno o para intimidar al público, o a una sección del público, con el propósito de promover una causa política, religiosa, racial o ideológica» (UK Terrorism Act, 2000) o «la creación y explotación deliberada del miedo mediante la violencia o la amenaza de violencia en la búsqueda del cambio político» (Hoffman, 2006).

De la unión de ambos deriva el término *ciberterrorismo*, que según Denning (2000, 2001) es

> «la convergencia del terrorismo y del ciberespacio. Se entiende que significa ataques ilegales y amenazas de ataque contra ordenadores, redes e información almacenada en ellos cuando la finalidad que se persigue es intimidar o coaccionar a un gobierno o a su gente en cumplimiento de objetivos políticos o sociales. Además, para calificar un acto de ciberterrorismo debería producirse con violencia contra personas o propiedades, o al menos causar suficiente daño para generar miedo».

Según la autora, los ataques contra infraestructuras críticas podrían ser un ejemplo de actos constitutivos de ciberterrorismo, no así los ataques que interrumpen servicios no esenciales o que causan pequeñas molestias. De esta manera, respalda a aquellos que consideran que el término *ciberterrorismo* es inapropiado, porque un ciberataque generalizado puede simplemente provocar molestias, no terror. Sin embargo, otros muchos creen que los efectos de un ataque generalizado a la red informática serían impredecibles y podrían causar

suficiente interrupción económica, miedo y muertes de civiles para considerarse adecuado calificarlos de terrorismo. Por este motivo hay dos perspectivas por medio de las que se define el término (Rollins y Wilson, 2007):

- **Según los efectos** que produce el ciberterrorismo, solo puede considerarse como tal si los daños que producen los ciberataques adquieren la magnitud suficiente para generar un miedo comparable a un acto físico (o fuera de línea) de terrorismo.

- **Según la intención**, el ciberterrorismo existiría cuando los fines que persiguen son ilegales o se realizan para intimidar o coaccionar a un gobierno o a personas, promover un objetivo político, o para causar un daño grave en la economía de un país.

Lectura obligatoria

El informe del Consejo de Europa *Ciberterrorismo: el uso de internet con fines terroristas* está disponible en el apartado «Recursos del aula». El documento es material obligado de estudio para este primer bloque de la asignatura.

Otros autores, como Lewis (2002) y Mantel (2009), definen el ciberterrorismo como el uso de las herramientas que ofrece la red por parte de determinados grupos con el fin de atacar infraestructuras críticas o para coaccionar o intimidar a un gobierno o a un individuo de la población. Por su parte, Mshvidobadze (2011) lo define como el conjunto de actos cibernéticos o ciberataques que se llevan a cabo para fomentar el terror o la desmoralización en una sociedad.

Si se examina el sentido que se ha dado al término ciberterrorismo en los documentos emanados de diversas instituciones, en 2004 el **FBI** se refiere a él como

> «un ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que pueda resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos».

En 2008, la **OTAN** definió el ciberterrorismo como

> «un ataque cibernético que utiliza o explota redes informáticas o de comunicación para causar la destrucción suficiente como para generar miedo o intimidar a una sociedad con un objetivo ideológico».

Ese mismo año, el **Consejo de Europa** publicó el informe *Ciberterrorismo: el uso de internet con fines terroristas*, y lo definió como «cualquier actividad que se realiza por parte de una célula o individuo terrorista mediante internet». En 2011, el informe de la Primera Comisión de Desarme y Seguridad Internacional de la **Asamblea General de las Naciones Unidas** lo define como las acciones realizadas mediante una red informática que pueden causar violencia o generar temor entre las personas, o provocar una destrucción grave por problemas políticos o sociales.

Entre las distintas definiciones de ciberterrorismo, adoptaremos la de Luiijf (2014) por ser la más exhaustiva y que nos lleva a entenderlo como el uso, los preparativos o la amenaza de una acción diseñada por parte de un grupo terrorista para llevarse a cabo por la red, con el fin de provocar un cambio en el orden social, crear un clima de miedo o intimidación entre el público, o influir en la toma de decisiones políticas por parte del gobierno y promover una causa política, religiosa, racial o ideológica. Ello se consigue mediante ciberataques dirigidos contra infraestructuras o sistemas, previamente seleccionados, dado el elevado valor en términos de seguridad que contienen las informaciones que estos albergan.

A partir de esta definición, podemos observar que las características básicas del ciberterrorismo son las siguientes:

- **El contexto legal**: el ciberterrorismo es la materialización de un acto delictivo o con un propósito delictivo.

- La acción, o ciberataque, es llevada a cabo por **un grupo o un individuo** perteneciente o simpatizante con una ideología que pretende la consecución de objetivos políticos por medios ilegales y **sin autoridad legal** para realizarla.

- El objetivo que se persigue es **coaccionar, controlar o provocar un daño a gran escala** contra una infraestructura crítica, que indirectamente **genera sensación de miedo, terror o inseguridad** en la sociedad.

- La acción está **motivada** por razones políticas, ideológicas, religiosas o sociales.

- El **ciberespacio** es el arma y el objetivo de las acciones perpetradas por los grupos terroristas. Los grupos terroristas aprovechan las opciones que dan las nuevas tecnologías para alcanzar sus fines.

- La **interferencia o interrupción de un sistema electrónico**.

- Los actos provocan **efectos psicológicos** de gran alcance para el público señalado como objetivo.

2.4. Ciberterrorismo y otros términos relacionados

Como hemos comentado en el anterior apartado, un motivo por el que aún no disponemos de una definición consensuada sobre qué es el ciberterrorismo es la confusión terminológica que nos lleva a confundirlo con otros términos

como *ciberguerra*, *cibercrimen*, *ciberactivismo* (o *hacktivismo*), *ciberextremismo*, *terrorismo cibernético*, *yihad virtual*, *yihad en línea* o *yihad electrónica*, que a pesar de su similitud etimológica describen realidades distintas.

Para los objetivos de esta asignatura diferenciaremos el ciberterrorismo del hacktivismo, el terrorismo cibernético y el delito cibernético.

1) Hacktivismo: hace referencia a las actividades en línea con el fin de revelar, manipular o explotar vulnerabilidades en sistemas operativos para conseguir objetivos políticos, como pueden ser promover o privilegiar una ideología política por encima de otra (Weimann, 2004), o, dicho de otro modo, utilizar los conocimientos informáticos con fines políticos. Para ello, los activistas disponen de varios medios: bloqueos virtuales, ataques de correo electrónico, piratería informática y robos informáticos, virus informáticos, o redireccionamiento de sitios web. A su vez, debemos diferenciar estas acciones del ***hacking***, que responde a la acción que lleva a cabo cualquier persona con conocimientos informáticos con el fin de introducirse, sin autorización, en sistemas ajenos para manipularlos u obtener información, entre otras acciones, con finalidades éticas, antiéticas o incluso neutrales, como la simple diversión.

Ejemplo de hacktivismo

Las acciones del grupo Anonymous.

2) Terrorismo cibernético: es un término que suele utilizarse en la prensa y en los medios de comunicación de masas para mencionar los ciberdelitos de motivación no terrorista que causan graves alteraciones en el funcionamiento de las infraestructuras de un país, y que generan temor o inquietud entre los ciudadanos. Esta tendencia a la utilización extensiva e incluso provocadora e hiperbólica del término terrorismo se detecta también cuando desde ciertos sectores se usa para referirse a conductas viales extremadamente peligrosas (terrorismo vial), para condenar acciones perniciosas contra el medio ambiente (terrorismo ecológico) o para suscitar el máximo reproche contra ciertas formas de violencia en la pareja (terrorismo doméstico).

Ejemplo de terrorismo cibernético

El espionaje o el robo de cuentas bancarias.

Por lo tanto, cuando se utiliza el concepto *terrorismo cibernético* detrás se esconde una finalidad sensacionalista que busca expandir las connotaciones peyorativas de la acción terrorista a acciones de distinta naturaleza.

3) Delito cibernético: el elemento que lo diferencia del ciberterrorismo es la motivación que se persigue con la comisión del delito. Mientras que el ciberdelito o delito cibernético persigue una finalidad, económica o de otro tipo, sin que ello suponga poner en peligro la vida de los ciudadanos, la motivación del ciberterrorismo va más allá de querer provocar un daño masivo para imponer unas creencias, ideología o gobernabilidad, además de aprovechar los beneficios de las TIC para fines de captación, reclutamiento y radicalización de individuos que, posteriormente, se muestren dispuestos a realizar atentados en el mundo real.

3. Uso de las TIC por parte de grupos terroristas

3.1. Medios de actuación

Desde la comisión de los atentados del once de septiembre de 2001 contra las Torres Gemelas y el Pentágono, se ha tenido mayor constancia del uso de las TIC por parte de las organizaciones terroristas. Si bien parte de su éxito se debe a las facilidades del medio tecnológico en términos de vulnerabilidad y escasa formación en ciberdelincuencia por parte de los agentes de seguridad, igual que sucedió con las acciones terroristas en el mundo fuera de línea, las organizaciones han sabido adaptarse al ciberespacio e ir explorando nuevas maneras de mantener y propagar su mensaje.

Para lograr sus fines, las organizaciones se dotan de distintas infraestructuras que, dado el amplio alcance de los contenidos que pueden distribuirse en ellas, han potenciado la capacidad de difusión directa del contenido por medio de internet, disminuyendo así la dependencia de los canales tradicionales de comunicación.

Mientras que antes los contenidos solo podían distribuirse por medios físicos (por ejemplo, mediante el soporte CD, VHS o DVD) a un público relativamente limitado, el uso de internet les ha permitido distribuirlos por una amplia gama de herramientas. Recordemos que la organización Al-Qaeda, en 2000, fue la primera que fundó su propia productora audiovisual, As Sahab, mediante la que ha difundido más de setecientos archivos de material audiovisual. Esta iniciativa fue y es también utilizada por otras organizaciones terroristas como Dáesh que, como se ha indicado, cuenta con más de treinta productoras que elaboran, además de vídeos, la revista oficial *Dabiq* y que gestionan un canal de televisión y una emisora de radio, *Bein HD4* y *La voz del califato*, respectivamente.

Las infraestructuras más utilizadas son las siguientes:

1) Sitios web: los sitios web fueron los primeros cauces por los que las organizaciones se dieron a conocer. En ellos, se pone a disposición del individuo un conjunto de recursos (vídeos, revistas, enlaces externos, etc.) que se pueden visualizar en línea o ser descargados. Como consecuencia del auge de las redes sociales, las webs han ido perdiendo fuerza, y ello ha permitido una descentralización de la información.

Ejemplos de webs

AQ/QA, *Al-ansar* o *Muslims news*, entre otras.

2) Redes sociales y aplicaciones de mensajería instantánea: las organizaciones han creado perfiles en las distintas redes sociales existentes, siendo Facebook y los canales de Telegram (Nikolái y Pável Dúrov) las más recurrentes; especialmente Telegram por la seguridad y la privacidad que brinda, ya que, aparte del cifrado completo, los mensajes son eliminados a las pocas horas; además, la mayoría de los terroristas arrestados en Europa lo han sido tras rastrear su actividad en esta plataforma. También coincide el hecho de que las reivindicaciones que hacen las organizaciones tras la comisión de algún atentado por parte de alguno de sus miembros se realicen por este medio, como sucedió en diciembre de 2016 tras el atentado contra un mercado navideño en Berlín.

Actualmente se considera que las redes sociales son la puerta de entrada al terrorismo, así como los medios de conexión entre las organizaciones terroristas y los simpatizantes, dado su acceso fácil y rápido y al hecho de guardar una apariencia de cierta horizontalidad entre ambas partes. Además, su uso les garantiza que un número importante de seguidores sean jóvenes. No olvidemos que estas redes son consumidas, principalmente, por este sector de la sociedad, un aspecto que las organizaciones conocen y aprovechan para impactar sobre su autoestima mediante refuerzos positivos.

Ejemplo de refuerzo positivo a seguidores jóvenes

Un individuo que participe activamente en las redes y comparta información en su cuenta personal tiene más posibilidades de recibir una insignia virtual en la que se le conceda el rango de «miembro destacado» o «miembro sénior», por ejemplo (Halopeau, 2014).

La inmediatez de la comunicación favorece que el sujeto esté informado a todas horas, así como interaccionar con otros individuos por las aplicaciones de chat de que disponen. Otro aspecto que debe resaltarse es que las redes sociales son herramientas más difíciles de controlar y de cerrar por parte de los cuerpos de seguridad, y en el caso de que así se produjera, el grupo podría crear nuevos perfiles en cuestión de escasos minutos.

3) Foros y chats: permiten al grupo mantener su información constantemente actualizada y se convierten en una potente plataforma a la que pueden acudir personas con la misma manera de pensar del grupo (independientemente de su ubicación geográfica) y compartir, entre otras cosas, métodos, técnicas o conocimientos operacionales específicos con el fin de cometer actos de terrorismo. Por este motivo, estas estructuras son consideradas auténticas «cajas de resonancia» de la ideología de la organización.

No obstante, para acceder a ellas, la mayoría requieren claves de acceso que solo son remitidas por parte de algún miembro de la organización cuando ha podido asegurarse de que el sujeto les será útil y fiel. Esta restricción de acceso (o barrera tecnológica) no solo añade un grado más de dificultad a las operaciones antiterroristas, haciendo necesario recurrir a la infiltración de alguno de sus agentes para conocer el contenido de las conversaciones que se mantienen, sino que también genera en el sujeto un sentimiento de «exclusividad» que puede contribuir a reforzar su autoestima y el deseo de pertenecer al grupo, lo que da origen a fuertes lazos de amistad que pueden acabar derivando en un microcosmos digital (Cohen-Almagor, 2017). Halopeau (2014) afirma que la manera de controlar dichos foros ha evolucionado. Si bien en el pasado

cada uno solía estar controlado por un solo administrador, en la actualidad son gestionados entre varios administradores. De esta manera, se intenta evitar que los agentes policiales puedan identificarlos y arrestarlos y que el foro deje de funcionar, ya que en caso de arrestar o condenar a uno, los otros pueden continuar con la tarea.

4) Videojuegos: por medio de las posibilidades audiovisuales que ofrecen, los videojuegos son capaces de emular o de trasladar situaciones socioculturales del mundo real al virtual, y hacer sentir al individuo como el verdadero protagonista tras la creación de su avatar. Es decir, el sujeto debe hacer de su «yo» un elemento gráfico que lo represente en el juego. Sin embargo, este no debe reproducir fielmente las características de la persona, sino que puede modificar los aspectos que menos le agradan por otros.

Si bien existen distintos tipos de videojuegos, atendiendo a diferentes variables, nos centraremos en los videojuegos masivos (*massively multiplayer online role-playing game*, MMORPG) de temática bélica, como pueden ser las series de *Call of Duty: Black Ops* o *Grand Theft Auto*. Estos videojuegos son los más utilizados por las organizaciones terroristas para captar a futuros miembros, puesto que requieren poco desgaste mental. Se ha observado que algunas organizaciones terroristas han elaborado sus propios videojuegos, o modificado los comerciales, añadiendo opciones que los hagan más próximos al estilo yihadista.

Ejemplo de opciones próximas al estilo yihadista

Ejecutar personas al grito *Allahu Akbar*, diseñar escenarios que reproducen las calles de Siria, o introducir como vestimenta el traje naranja característico de los presos de Guantánamo.

Para jugar a un MMORPG el sujeto debe interactuar con otros jugadores simultáneamente, que igual que él están conectados a la red (Carbonell, Torres y Fuster, 2016). Al tratarse de un mundo no físico, el sujeto sabe que la violación de las normas del juego no le reportará un castigo real, lo que aleja al jugador del coste real que tendría su conducta si se llevara a cabo en el mundo fuera de línea.

5) Revistas en línea: las organizaciones terroristas ven en las opciones multimedia un canal excepcional por el que difundir su ideología y captar nuevos individuos para sus filas. En estas revistas:

- se presentan manifiestos;
- se publican cartas o testamentos de muyahidines caídos en combate con el «enemigo» con el objetivo de glorificar y de banalizar la muerte;
- se realizan llamamientos contra los enemigos; o
- se explica cómo elaborar material explosivo, utilizar armas blancas o vehículos para cometer atentados en sus países de residencia.

De hecho, como señalan Lemieux, Brachman, Levitt y Wood (2014), los atentados de la maratón de Boston, en 2013, fueron planificados siguiendo las indicaciones de fabricación de explosivos que se describían en un número de la revista de Al-Qaeda, *Inspire*. Como hemos explicado anteriormente, el tratamiento visual y gráfico que se lleva a cabo de su contenido es impecable, y busca en todo momento un impacto capaz de captar la atención del lector. Sin

embargo, esta organización no ha sido la única en recorrer a la edición y difusión de revistas con el objetivo de ampliar sus bases. Dáesh, tras la autoproclamación del califato, también lo ha hecho con las revistas *Dabiq*, *Dar al-Islam*, *Istok* y *Konstantiniyye*, publicadas por Al-Hayat Media Center y redactadas en inglés, francés, ruso y turco, respectivamente. Destaca el hecho de que estas publicaciones son de fácil acceso y elaboradas en diversos idiomas, siendo el inglés, el francés y el ruso los más utilizados, a parte del árabe.

A pesar de que se dirigen a un público masculino, desde 2015 la sección femenina de Dáesh, formada por la Brigada al-Khansaa y la Brigada de Umm al-Rayan, tiene reservado un espacio en *Dabiq* bajo el título «Para nuestras hermanas» donde, recurriendo a un lenguaje coloquial, se enfatiza en el rol fundamental que tienen las mujeres en el califato, así como en desmentir la información que desde Occidente se da sobre el rol real de la mujer en la organización. Aunque este material se edita desde el Próximo Oriente, el mensaje va dirigido principalmente a chicas y a mujeres residentes en países de mayoría no musulmana con el objetivo de que se desplacen hacia el califato para servir a la organización. Todo ello se basa en la creencia de que el papel fundamental de la mujer no es otro que el de la maternidad y el cuidado del hogar, pero, lejos de la promesa de una vida plena como esposas y madres de los futuros mártires, estas acaban siendo esclavas sexuales.

La Brigada al-Khansaa y la Brigada de Umm al-Rayan

Estas brigadas están integradas por mujeres de edades comprendidas entre los dieciocho y los veinticinco años, que se dedican exclusivamente a vigilar la preservación del orden en el espacio público y a hacer cumplir (de manera expeditiva) las estrictas normas de la *sharîa* a todas las mujeres que viven en el territorio del califato. A cambio, reciben un sueldo, el acceso a servicios y una manutención.

6) *Nasheed*: con este nombre se hace referencia al género musical musulmán que consiste en cantar a capela, o con el acompañamiento de algún instrumento cuando se trata de un enlace matrimonial, un poema o parte de él. No obstante, tras el estallido de la Primavera Árabe y la autoproclamación del autodeclarado Estado Islámico por parte de Dáesh, estas formas de expresión han alcanzado un éxito que hasta entonces no tenían, y se han convertido en auténticos himnos para los simpatizantes de la ideología yihadista, así como en elementos fundamentales de su propaganda, dado que su principal función es la movilización y la radicalización de los oyentes.

A diferencia de las *nasheeds* originales, y a pesar de que su estructura está pautada (por ejemplo, su melodía no debe incitar al baile y no debe distraer al oyente de su tarea de estudiar el Corán, entre otras), las actuales son cantadas por un coro de voces masculinas que repiten reiteradamente (casi como mantras):

- narraciones de tipo bélico (*nasheeds* de batalla);
- narraciones de alegoría o de conmemoración a un mártir caído en combate con el «enemigo» (*nasheeds* de martirio); o

- narraciones de ensalzamiento de las características del muyahidín (*nasheeds* de alabanza).

Además, el idioma no siempre es el árabe, pudiéndose emplear también el francés, el inglés o el alemán (Said, 2012).

Por otro lado, la reacción que se pretende conseguir en el receptor está manipulada por programas informáticos. Es decir, la pieza musical obtenida es tratada por los productores (miembros de la organización que forman el equipo de unidad propagandístico Al-Ajnad Foundation), como si fuera un disco comercial. Estos individuos se encargan de ajustar las voces, de armonizarlas, de controlar los tiempos de aparición, y de insertar sonidos militares (por ejemplo, el sonido de pasos marchando o de armas de fuego cargándose), para finalmente distribuirla por los medios de la organización, siendo sus redes sociales y foros los canales principales, aunque también se han localizado miles de ellas en el canal YouTube, cuyas reproducciones alcanzan cifras muy elevadas. Dadas las características y el fácil acceso que cualquier persona puede tener a ellas, su control es una tarea muy complicada.

Ejemplo de producción de *nasheed*

Una de las producciones musicales más importantes, y que se ha convertido en seña de identidad del grupo, es la que lleva por título *My Ummah, Dawn has Appeared*, que cuenta con más de 220.000 reproducciones en YouTube.

3.2. Actividades principales del ciberterrorismo

Las organizaciones utilizan las distintas estructuras que acabamos de ver para conseguir fines diversos. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) señaló seis maneras como internet puede utilizarse para actividades terroristas: difusión de propaganda; captación, reclutamiento, adoctrinamiento y radicalización; financiación; formación; planificación y ciberataques.

1) Difusión de propaganda: las organizaciones terroristas usan internet con fines propagandísticos. Para ello se utiliza el término *yihad mediática*. Las organizaciones saben que con una publicidad potente que enfatice su imagen, la brutalidad en la acción y sus victorias tácticas, pueden proyectar una imagen de poder y de ambición ilimitada (Torres, 2016). La propaganda se lleva a cabo mediante comunicaciones de imagen, audio o video, por los que se difunde ideología, se promueven actividades terroristas y se proporciona una justificación. En estos materiales se muestra la capacidad del grupo para realizar operaciones (como ataques suicidas), publicar declaraciones con sus intenciones o los testamentos de terroristas, así como mostrar a los colectivos que apoyan su causa mediante la publicitación de los patrocinadores. La infraestructura les permite acceder, autopublicar y actualizar información continuamente. Sin embargo, lo que determinará que una publicación se considere, o no, propaganda terrorista y no un acto amparado por el derecho a la libertad de expresión internacionalmente reconocido, será una evaluación subjetiva. Como se sabe, el derecho a la libertad de expresión garantiza a las personas poder compartir una opinión o distribuir contenido que puede ser considerado ofensivo por otros, a reserva de ciertas excepciones limitadas previstas por

ley como son la distribución de contenido sexualmente explícito o la promoción e incitación a la violencia, algo que constituye una práctica recurrente en la propaganda de estos grupos.

2) Captación, reclutamiento o radicalización: esta utilidad está estrechamente relacionada con la anterior, ya que la organización requiere de una propaganda cuyo contenido se adapte a las características de los grupos más vulnerables, y para que internet pueda erigirse como un medio capaz de establecer relaciones con las personas más receptivas a la propaganda con el objetivo de captarlas, adoctrinarlas y radicalizarlas con el fin de que acaben cometiendo un acto terrorista. Por este motivo, el mensaje con el que se bombardea al sujeto se caracteriza por contener elevado grado de violencia (visual o verbal) y apelaciones a los sentimientos de injusticia, exclusión y humillación.

Si este proceso de por sí ya es difícil de identificar y prevenir, se vuelve mucho más complejo cuando el medio utilizado es la red. El proceso de adoctrinamiento se estructura en diversas fases, por medio de las que se generan los tres elementos necesarios que, según la teoría de la búsqueda de la significancia (*isgnificance quest theory*, SQT), se requieren para que un individuo complete la fase de radicalización en una ideología extremista y decida dar el paso hacia la acción terrorista. Estos elementos son los siguientes: la necesidad, la narrativa y la red de apoyo (Kruglanski, Jasko y LaFree, 2016; Kruglanski, Webber, Chernikova y Molinario, 2018).

En España, el año 2011 la Fiscalía General del Estado publicó la Circular n.º 2/2011, de 2 de junio, y en 2015 el Ministerio del Interior hizo público un informe en el que se estimaba que el 80 % de la captación y del adoctrinamiento se producía en lugares físicos, como mezquitas o centros universitarios, y siempre con la presencia de un agente radicalizador físico. En la actualidad, este predominio ha sido reemplazado por internet, hasta el punto de convertirse en el centro virtual del extremismo (Cano, 2008; Reinares y García-Calvo, 2017; Reinares, García-Calvo y Vicente, 2018). Sin embargo, como defiende Vicente (2018), actualmente el adoctrinamiento por medio, únicamente, del ciberespacio (sin mediar interacción física) parece poco viable. En la mayoría de los casos documentados en Europa y en América, el estadio de la radicalización requirió un contacto cara a cara con algún miembro de la organización a la que pertenecía el individuo.

La captación y radicalización por la red también se ha utilizado en el caso de las mujeres. En 2015, la Brigada al-Khansaa publicó en páginas web y foros afines a la organización terrorista Dáesh, un manifiesto de carácter propagandístico dirigido a la comunidad femenina musulmana residente en países árabes, con el fin de reclutar mujeres. Este documento, bajo el título *Las mujeres en el Estado Islámico: manifiesto y estudio de caso*, está estructurado en tres secciones en las que se pretende describir el papel de la mujer musulmana en su comunidad, así como el estilo de vida que debe llevar si quiere seguir las directrices del

Profeta. El objetivo es que cuando la mujer acabe la lectura tenga la sensación de que llevar una vida legítima y fructífera fuera del califato es imposible. De esta manera, experimenta la necesidad de abandonar su país e ir a vivir en él.

3) Preparación de atentados: la primera vez que se tuvo conciencia de este uso fue con la organización Al-Qaeda, cuando se comprobó el uso de la esteganografía para ocultar mensajes en imágenes y en películas. No obstante, la cantidad de información que puede ocultarse es muy limitada, por este motivo se cambió de método (Halopeau, 2014).

La esteganografía

Es un método de ofuscación que sirve para ocultar un mensaje dentro de otro mensaje visual (como imágenes) para que a simple vista no pueda ser detectado. Algunas de las herramientas que permiten hacer este cifrado son las siguientes: FileInyector, Our Secret o Steganographia.

Tras los atentados en el tren de Madrid el once de marzo de 2004, los detenidos revelaron que estaban usando un nuevo método para evitar la detección de sus comunicaciones. El concepto era tener una sola cuenta de correo electrónico compartida entre todos los miembros del grupo donde pudieran escribir correos electrónicos y dejarlos en la carpeta de borradores. Hoy en día, esta técnica se ha dejado de usar por ser bien conocida. Después se utilizaron otras herramientas como PGP o TrueCrypt. Pero para garantizar la privacidad de la información, en 2007 las organizaciones empezaron a desarrollar sus propias herramientas, como Mujahideen Secrets o Mujahideen Secrets 2, que fueron utilizadas por miembros de Al-Qaeda en la planificación de un atentado fallido en Francia en 2008. Más recientemente, en 2013, el Frente Islámico Global de Medios lanzó Asrar al-Dardashah, cuyo funcionamiento y apariencia recuerda a las existentes en mensajería instantánea. Otra herramienta es Pidgin, que requiere de la creación de una cuenta previa en Google Talk, MSN, Yahoo, AOL Instant Messenger y Jabber o XMPP. La importancia que da la organización a sus redes llega al extremo de emular el sistema Android. La diferencia es que sus aplicaciones no pueden ser descargadas desde una tienda oficial, sino que el usuario debe dirigirse expresamente al sitio web de la organización y seguir los pasos indicados.

4) Financiación: las organizaciones terroristas también utilizan internet como medio por el que financiar sus actos y sufragar los gastos derivados de estos como, por ejemplo, la compra de armas, los alquileres de pisos francos, la adquisición de equipo técnico, etc. Para ello pueden:

- pedir directamente a sus simpatizantes que contribuyan a la recaudación de fondos aportando donaciones personales;

- utilizar alguna sección de sus páginas webs como tienda electrónica en la que sus simpatizantes puedan adquirir material de la organización o relacionado con su ideología;

- emplear servicios de pago en línea;

- usar transferencias de fondos por transferencia bancaria electrónica, tarjeta de crédito o servicios de pago como PayPal o Skype; y

- recibir apoyo financiero por parte de organizaciones aparentemente legítimas o benéficas que desvíen parte de sus fondos a cuentas de organizaciones terroristas.

Ejemplos de organizaciones que desvían fondos a organizaciones terroristas

Algunos ejemplos contrastados son la Benevolence International Foundation, la Global Relief Foundation y la Holy Land Foundation for Relief and Development.

5) Formación: la versatilidad de internet, unida a las múltiples oportunidades que ofrece, ha propiciado que las organizaciones encuentren en él un medio ideal para formar a los reclutados, tanto en ideología como en la fabricación y la utilización de armas mediante manuales en línea de fácil acceso y en varios idiomas, ficheros de audio y video, o materiales de información y de asesoramiento con instrucciones detalladas; una auténtica biblioteca en línea que puede consultarse en cualquier momento y desde cualquier lugar. De este modo, internet se ha convertido en el sustituto de los campos de adiestramiento terrorista ubicados en lugares secretos de la geografía del país de la organización.

6) Ciberataques: no entraremos a profundizar sobre ellos, ya que los tipos de ciberataques que citaremos a continuación ya han sido materia de estudio en otras asignaturas. Como ya se sabe, un ciberataque responde a la conducta de explotación deliberada de redes informáticas con el objetivo de lanzar un ataque mediante ellas o a perturbar su funcionamiento normal. Las redes más utilizadas por parte de las organizaciones terroristas son las siguientes:

- uso de programa malicioso;

- envío de virus infectados para modificar o dañar el sistema informático;

- envío masivo de correo basura o correo no deseado;

- suplantación de remitentes de mensajes mediante Spoofing para acceder a recursos contenidos en un tercer sistema y envío o instalación de archivos espías (*keyloggers*); y

- uso de troyanos o de archivos BOT para lograr el control remoto de sistema sin el conocimiento ni consentimiento del usuario.

Otra ciberacción de interés es el uso de la técnica *blind radars*, que permite el bloqueo del tráfico aéreo por medio de interferir electrónicamente en los radares y sistemas ubicados en las torres de control de los aeropuertos y helipuertos. Todas estas acciones suelen durar poco, y tienen como finalidad contribuir a la misión de la yihad. Por lo tanto, los ciberataques tienen, a día de hoy, una finalidad instrumental.

Según Torres (2016), la posibilidad de que una organización terrorista desarrolle su propia ciberarma, aún es algo muy a largo plazo, ya que su diseño no solo implicaría un elevado coste económico, sino también tiempo para probar el *software*, comprobar su seguridad e inmunidad frente a ciberataques, así como evaluar su efectividad en relación con los objetivos buscados por la organización. La otra opción que podrían barajar sería establecer contratos de colaboración con alguna empresa profesional para que desarrollara la ciberarma. Sin embargo, y a pesar de la cuantiosa ganancia económica que ello podría reportarle, las consecuencias que pudiera tener para la empresa (el prestigio y la visibilidad social), a largo plazo lo harían inviable.

Como se puede observar, en este módulo dedicado al ciberterrorismo no entraremos a debatir o a contrastar datos epidemiológicos, ya que no existe consenso y sí grandes dificultades para determinar con certeza si un ciberataque responde a tal naturaleza o es el resultado de una acción cometida por *hackers* con cierta simpatía o inspiración yihadista, como son, por ejemplo, Islamic State Hacking Division, Sons Caliphate Army, Cyber Caliphate Army o Kalacnikov.TN, cuyo objetivo final es crear entre todos un cibercalifato (*United Cyber Caliphate*).

Medios / Estructuras	Usos / Actividades
• Páginas web	• Difusión de propaganda
• Redes sociales y aplicaciones de mensajería instantánea	• Captación, reclutamiento y/o adoctrinamiento
• Foros y chats	• Planificación de atentados
• Videojuegos	• Financiación
• Revistas en línea	• Formación
• *Nasheed*	• Ciberataques

4. El proceso de radicalización por la red

4.1. La radicalización. Definición

La radicalización se ha definido como el proceso por el que un individuo adopta actitudes y creencias que justifican, tanto utilitaria como moralmente, el terrorismo inspirado en una versión radical y extremista, que tiene lugar tras la previa captación y reclutamiento por parte de una organización terrorista (Cano, 2008; Reinares y García-Calvo, 2017). Si bien este proceso puede obedecer a distintos motivos, en el caso del terrorismo de base religiosa, tiene como objetivo socializar al individuo a una lectura e interpretación tergiversada y tendenciosa del credo islámico. Este proceso, como defienden Cano y Castro (2018), consta de dos componentes: uno de carácter **social**, dado que para que se dé el proceso se requiere de la interacción (física o no) con otro individuo, y otro **ideológico**, al ser el objetivo conseguir que un individuo sustituya su sistema de normas y valores, incluyendo su manera de pensar, por el de la organización.

Por ello es importante destacar que siempre hablamos de un proceso y no de un estado, ya que una persona difícilmente amanece convertida en terrorista, sino que se llega a este estado tras la sucesión de diversas etapas. Concretamente, y como explicaremos con mayor detalle en el próximo apartado, en cuatro etapas que son las siguientes (Silber y Bhatt, 2007):

- aproximación y primeros contactos;
- captación, adhesión y preradicalización;
- aislamiento y adoctrinamiento; y
- yihadización, que podemos renombrar como «ciberyihadización» por producirse en el entorno digital.

Advertencia sobre el adoctrinamiento

Antes de profundizar, queremos advertir que ninguna de las fases que integran el proceso debe ser entendida de manera determinista o unidireccional, al ser el adoctrinamiento un proceso que puede abandonarse en cualquiera de ellas, y evitar así su culminación. De otro modo no podríamos explicar por qué son tan pocos los casos en que alguien que ha iniciado un proceso de captación y de adoctrinamiento decide finalmente dar el paso e implicarse en una actividad de tipo terrorista.

4.2. El proceso de ciberradicalización y el perfil de las cibervíctimas

Los primeros en advertir del uso de las TIC como medio de radicalización fueron Sageman (2004) y Weimann (2004). A diferencia del adoctrinamiento fuera de línea, internet ha permitido intensificar y agilizar el proceso, y disminuir el período de tiempo necesario a solo unos meses, ya que la red posibilita estar

en contacto permanente con la ideología y con los agentes radicalizadores. Este fenómeno se ha denominado por parte de la prensa y de algunos expertos «adoctrinamiento exprés». Por lo tanto, la ciberradicalización no es un proceso que haya aparecido paralelamente a la implantación de las TIC, sino que las organizaciones han sabido redefinirlas (Grabosky, 2001).

A continuación, describiremos cada una de las cuatro fases que forman el proceso, así como el perfil de los individuos que intervienen en ellas. No obstante, para entender mejor el proceso debemos tener presente que en el ciberespacio la conducta decisional del sujeto está limitada por la ingenuidad y la impulsividad que conlleva actuar por internet (Agustina, 2014). Ello se debe a que los elementos que constituyen el entorno virtual actúan directamente en la vía emocional del sujeto (Bouzar, 2015, 2017).

Las cuatro etapas que se describirán no deben entenderse secuencialmente, sino que pueden presentarse de modo discontinuo ya que no todos los individuos alcanzan el último estadio pasando por todas las anteriores, sin olvidar los casos en que los individuos abandonan el proceso. Un reto para la investigación criminológica, de gran interés práctico, es el estudio de los factores que favorecen el desistimiento y la continuidad del proceso.

1) Aproximación y primeros contactos: a diferencia de lo que sucede en la modalidad fuera de línea, esta fase puede producirse de dos maneras, según la mayor o menor iniciativa que muestre el sujeto en el reclutamiento. Por ello diferenciamos entre una «aproximación activa» y una «aproximación pasiva» (Guirao, 2019). En la primera (aproximación activa) es el individuo quien decide ponerse en contacto con la organización por medio de alguna de sus estructuras; por ejemplo, escribiendo un mensaje en sus redes sociales. Este primer perfil responde a una persona joven que experimenta sentimientos de humillación, frustración, culpa, odio, ira o indignación, como respuesta a experiencias personales o por hechos negativos que han sucedido en su entorno. Todos estos hechos actúan como factores *push* (precipitadores o potenciadores), y facilitan que el individuo tome la iniciativa de querer ingresar en la organización. A su vez, estos factores victimógenos personales son los que indican a los ciberojeadores que ese sujeto puede ser un buen candidato a reclutar. Recordemos que la radicalización es un proceso que puede iniciarse por una multitud de causas, ya sean de tipo individual o social.

El interés que muestra el sujeto por el grupo ha podido iniciarse por mera curiosidad, es decir, el sujeto se conecta a la red y empieza a buscar información yihadista sin que esta tenga que guardar relación directa con una organización terrorista o con contenidos que se muestren proclives a la violencia yihadista. Así, estos sujetos podrían considerarse víctimas propicias pasivas a la cibervictimización terrorista, si tomamos como referencia la tipología de Cohen y Fel-

son (1979). Sin embargo, conductas aparentemente neutrales o «inocentes» como las descritas pueden ser interpretadas por los ciberreclutadores como expresivas de la voluntad de entrar a formar parte de la organización.

Cuando la conducta del sujeto va más allá de la simple curiosidad, la búsqueda no se detiene, se incrementan las horas frente al monitor y se profundiza en el contenido que alberga la red, nos encontramos ante una conducta de búsqueda casi obsesiva que le permite interiorizar los postulados yihadistas. En este punto es cuando el sujeto empieza a visitar perfiles de organizaciones y a consumir material propagandístico en el que se muestran imágenes como las de la guerra en Siria o cadáveres de mujeres y niños asesinados por el «enemigo». Estos materiales contribuyen a la elaboración de una narrativa victimista que la organización utiliza para generar en el individuo el deseo de venganza y para justificar y legitimar el uso de la violencia (Trujillo, Moyano y González-Cabrera, 2006; Kruglanski, Webber, Chernikova y Molinario, 2018).

Por otro lado, la visualización de este tipo de materiales hace que el sujeto empiece a cuestionarse tanto su estilo de vida como el sistema de creencias en el que ha sido socializado para decidir sustituirlo por el de la organización. Todo esto deriva en un pensamiento desindividualizado y dicotómico por parte del sujeto, que tiende a diferenciar entre un «nosotros» y un «ellos». Paralelamente, mientras experimenta sentimientos de rabia y de odio hacia Occidente, desarrolla empatía y solidaridad hacia la comunidad musulmana (*Umma*). De esta manera, cualquier conducta o comentario que se realiza sobre el pueblo musulmán, y que el sujeto interpreta como «injusto», «cruel» o «humillante», lo percibe como un ataque a su identidad. Esto es lo que Khosrokhavar (2003) denominó «humillación delegada».

El concepto *yihad*

Este concepto puede interpretarse de dos maneras, según la finalidad que persiga. El Corán diferencia, por un lado, una interpretación espiritual que la define como la «gran» yihad o la yihad «interior», que se refiere al esfuerzo que cada musulmán debe realizar en su día a día para llegar a ser mejor persona, mejor musulmán, alejándose de las conductas que lo puedan corromper; por otro lado, tenemos la interpretación bélica y defensiva, la yihad «menor» o «exterior». Esta interpretación permite justificar la acción violenta cometida por un individuo o grupo, cuya finalidad es eliminar al *takfir* y extender la «verdadera fe» islámica por todo el mundo.

En la segunda modalidad (aproximación pasiva), es un miembro de la organización dedicado a las tareas de captación y de reclutamiento en línea quien adopta el rol activo e inicia conversaciones con los sujetos que han mostrado de algún modo interés por la organización o por la causa que defienden. Para localizarlos se dedica a rastrear perfiles y sus conductas virtuales sobre los medios del grupo.

Todo ello nos hace tomar conciencia de que las TIC han favorecido la emergencia de una nueva relación entre nuestro cuerpo y la máquina, una nueva subjetividad digital.

2) Captación, adhesión y prerradicalización: una vez el ciberojeador ha traspasado la información al ciberreclutador (rol que suele asumir una mujer), las conversaciones entre este y el individuo pasan a establecerse en foros o en chats privados. No obstante, como hemos comentado en apartados anteriores, el sujeto debe haber recibido las claves de acceso. Estas claves suelen conseguirse una vez el individuo se ha descargado el *software* Tor (The Onion Router) en su ordenador para garantizar que su navegación no dejará huellas en el ciberespacio (*cybertrails*) susceptibles de ser rastreadas por las fuerzas de seguridad.

En las conversaciones, además de referirse a suras del Corán donde abundan las alusiones a la yihad bélica, al martirio, a la promesa de la glorificación y al acceso al paraíso para convencer al sujeto de que cometa un hecho delictivo y justificar la violencia que puedan definir sus acciones, el ciberreclutador quiere conocer sus vulnerabilidades, su estilo de vida, sus problemas familiares, su estatus socioeconómico, su nivel educacional, su profesión, su círculo de amigos, sus aficiones y otros aspectos relevantes de la vida personal. La información facilitada se trata con el objetivo de elaborar un modelo adoctrinador personalizado que pueda dar solución y respuesta a todas las necesidades y preguntas existenciales que perturban al sujeto (Guirao, 2019). Así es como el sujeto experimenta un mayor deseo de interactuar con los miembros de la organización y de aislarse del resto de la sociedad, y desarrolla en su psique una «sociedad paralela» (Khosrokhavar, 2003; Kandel, 2004). Una vez el individuo siente que ha pasado a formar parte del grupo (o cibercomunidad), desea satisfacer una nueva necesidad: la de significación social. El sujeto necesita ser reconocido y respetado por su grupo (Baumeister y Leary, 2017). Ello hace que toda información transmitida dentro del grupo se reinterprete de acuerdo con su sistema de creencias y valores. Esta dinámica favorece la consolidación del compromiso de los miembros con la organización y promueve la narrativa radical, al estar todos involucrados en un proceso de aprendizaje colectivo en el que la retroalimentación es constante (Kruglanski, Jasko, Webber y Chernikova, 2018). Cuando esto sucede, podemos entender que el sujeto ya ha iniciado el camino que le llevará a aceptar un encuentro en el mundo fuera de línea con un miembro de la organización.

3) Aislamiento y adoctrinamiento: una vez la persona ha sustituido su sistema de creencias por el salafismo radical, el siguiente paso es lograr que el cambio también se generalice en su estilo de vida fuera de línea, pero sin que ello levante sospechas en su entorno. Para ello, la organización le autorizará a usar el *taqiyya*. Este término surge de la doctrina *takfir*, y se define como el acto de disimulo mediante el que se permite al creyente esconder sus creencias religiosas ante el temor de perder la vida, las vidas de sus familiares o para la preservación de la fe. En la actualidad, su uso también se permite con el fin de evitar que el creyente sea descubierto por sus intenciones terroristas, y pasar así desapercibido en la comunidad de «infieles» para acabar sometiéndolos.

Los cambios conductuales que se pueden observar en esta fase son los siguientes:

- Abandono o cambio en determinadas actividades de ocio.

- En caso de un individuo ya musulmán, dejar de acudir a la mezquita u oratorio por considerar impura o moderada la interpretación del islam que se predica allí. También entrar en conflicto con su imán o con sus progenitores al considerar que no defienden al pueblo musulmán.

- En caso de que el sujeto sea converso, se observa que empieza a asistir a un oratorio o a mostrar interés por la rama radical del islam y por los pasajes más violentos del Corán.

Esta situación se agrava si la figura paterna está ausente o no ejerce el rol de cabeza de familia (Bouzar, 2015). De esta manera, vemos que un cambio iniciado en el entorno en línea tiene un impacto en el entorno fuera de línea, corroborando así la unidad entre ambos mundos (Agustina, 2014).

4) Ciberyihadización: en esta fase, el sujeto presenta un pensamiento completamente dicotomizado, así como una hipersensibilización ante cualquier conducta o comentario susceptible de interpretarse como un ataque contra su persona o contra la comunidad musulmana. Aquí se produce el primer encuentro cara a cara con un miembro de la organización. El encuentro tiene dos objetivos:

- en primer lugar, evaluar el nivel de fidelidad del sujeto hacia la organización; y

- en segundo lugar, acabar de convencerlo para que acepte las tareas que la organización le ordene, incluido el suicidio (Guirao, 2019).

Para ello, el ciberadoctrinador potenciará las motivaciones, los sentimientos y las justificaciones favorables a la violencia.

Resumen

El estudio de este primer módulo nos ha acercado a la realidad del ciberterrorismo. Hemos visto como a pesar de la amenaza que supone, aún no existe consenso respecto a una definición, siendo la más exhaustiva la propuesta por Luiijf (2014), y que nos lleva a entenderlo como el uso, los preparativos o la amenaza de acción diseñados por parte de un grupo terrorista, con el fin de provocar un cambio en el orden social, crear un clima de miedo o de intimidación entre el público, o influir en la toma de decisiones políticas por parte de un gobierno. El terrorismo al que nos hemos referido en este módulo está asociado a la promoción de una causa política, religiosa, racial o ideológica, lo que permite distinguirlo de otras manifestaciones, a su vez calificadas también como terrorismo, en las que un grupo organizado utiliza medios similares para alcanzar objetivos no políticos. Del mismo modo, hemos visto como los ciberataques no se llevan a cabo sobre cualquier estructura, sino que se seleccionan aquellas cuyos efectos podrían perjudicar gravemente la integridad, la confidencialidad o la disponibilidad de información de los sistemas de información y de las redes.

También hemos comprobado cómo las características que definen el ciberespacio han facilitado la inhibición conductual de los individuos, proliferando los ciberataques que van más allá del ciberterrorismo, lo que nos ha llevado a preguntarnos si de verdad se trata de nuevos delitos o simplemente son la versión 2.0 de los ya conocidos.

En el ámbito concreto del ciberterrorismo, observamos que los medios por los que las organizaciones pueden llevar a cabo sus acciones son diversos, siendo las redes sociales y las aplicaciones de mensajería instantánea sus principales aliados, sobre todo para realizar actividades relacionadas con la captación, el adoctrinamiento y la radicalización. Este proceso, cuando se lleva a cabo en el mundo virtual, recibe el nombre de ciberradicalización, y ha permitido no solo reducir costes económicos, sino también el tiempo necesario para radicalizar a un sujeto, pasando de la media de dos años a unos seis u ocho meses. Sin embargo, los estudios han demostrado que actualmente para que un sujeto alcance el estadio máximo se requiere, como mínimo, un intercambio cara a cara en el mundo real con un agente físico.

Tanto internet como las TIC han tenido, y tienen, una importancia relevante en lo referente a la propaganda y a la difusión del discurso radical de la organización. Hemos visto cómo las publicaciones responden a la voluntad de causar el mayor impacto posible en quien las consuma, para aumentar las probabilidades de que acabe entrando en contacto con la organización y se

ponga a su disposición. Una voluntad que no solo manifiestan varones, sino también mujeres. Así lo hemos visto con la tarea adoctrinadora que llevan a cabo las brigadas femeninas de las organizaciones terroristas.

Ejercicios de autoevaluación

Para que podáis comprobar el grado de consolidación alcanzado tras el estudio del material, os proponemos contestar diez preguntas tipo test cuyas soluciones están en la página siguiente. ¡Suerte!

1. Indica quién fue el primer autor que utilizó el término *ciberterrorismo*.

a) Denning
b) Barry Collins
c) Lewis
d) Mshvidobadze

2. ¿Cuál es la diferencia entre la gran yihad y la yihad menor?

a) La diferencia es cuantitativa, es decir, mientras que la gran yihad es la llevada a cabo por un grupo mayoritario, la menor es la llevada a cabo por un grupo minoritario.
b) La gran yihad es la que hace referencia al esfuerzo que cada musulmán debe realizar en su día a día para llegar a ser mejor persona, y la yihad menor es la que defiende la acción bélica.
c) No hay diferencia. Solo hay una yihad.
d) La diferencia es su aparición o no en el Corán. Mientras que la gran yihad aparece en diversas aleyas, la menor no aparece en ninguna.

3. Indica cuál de los siguientes medios ha permitido descentralizar la difusión del discurso terrorista.

a) Revistas en línea.
b) Videojuegos.
c) Ciberataques.
d) Redes sociales y aplicaciones de mensajería instantánea.

4. Indica cuál de las siguientes afirmaciones sobre el proceso de radicalización es correcta:

a) La radicalización no es un proceso, es un estado.
b) La radicalización es un proceso en el que solo interactúan el individuo y el ciberradicalizador.
c) Las fases de la radicalización son: aproximación y primeros contactos; captación, adhesión y prerradicalización; aislamiento y adoctrinamiento y ciberyihadización.
d) Los estudios han demostrado que el proceso de radicalización puede concluirse sin haber existido un encuentro cara a cara en el mundo real con un miembro de la organización terrorista.

5. Indica qué afirmación sobre las características del ciberterrorismo es incorrecta.

a) El ciberataque es llevado a cabo por un individuo perteneciente o simpatizante con una ideología extremista radical y que actúa sin autoridad legal para realizarla.
b) La acción está motivada por factores políticos, ideológicos, religiosos o sociales.
c) Los actos que realizan provocan efectos psicológicos de gran alcance para el público objetivo.
d) El ciberespacio es el arma y el objetivo de las acciones perpetradas por los grupos terroristas.

6. ¿Qué son las *nasheeds*?

a) Son un género musical musulmán que consiste en recitar un poema o una parte de él.
b) Son canciones que se han convertido en señas de identidad de los actuales grupos terroristas de base religiosa.
c) Las letras de las *nasheeds* no siempre son en árabe, también pueden ser en francés, inglés o alemán.
d) Todas las respuestas anteriores son correctas.

7. Atendiendo al mayor o menor grado de participación del sujeto en el proceso de radicalización, diferenciamos entre:

a) Aproximación cercana y lejana.
b) Aproximación proactiva y reactiva.
c) Aproximación pasiva y activa.
d) Aproximación superficial y profunda.

8. El elemento principal para la desinhibición conductual en el ciberespacio es:

a) El anonimato disociativo.
b) La invisibilidad.
c) La introyección solipsista.
d) La comunicación asincrónica.

9. Indica cuál de las siguientes afirmaciones caracteriza la propaganda terrorista difundida en la red.

a) Solo va dirigida a chicos y a hombres.
b) Su edición está muy cuidada, hasta el punto de recordarnos a producciones de Hollywood.
c) Los idiomas en que se elaboran son el árabe y el inglés.
d) Es de difícil acceso, y solo podemos visualizarla si disponemos de una clave de acceso.

10. La diferencia entre el hacktivismo y el ciberterrorismo es:

a) El hacktivismo consiste en realizar actividades en línea con un fin político. El ciberterrorismo quiere promover o privilegiar un credo religioso por encima de otro mediante la perpetración de ciberataques en instalaciones críticas de un país.
b) El hacktivismo consiste en realizar actos en la red por simple diversión, como por ejemplo hacerse con las cuentas bancarias de desconocidos. El ciberterrorismo consiste en llevar a cabo acciones en línea para influir en la toma de decisiones políticas de un gobierno nacional o internacional.
c) El hacktivismo es una forma de ciberterrorismo motivado por finalidades políticas, mientras que el ciberterrorismo puede aludir a motivos políticos, ideológicos, religiosos o sociales.
d) El hacktivismo consiste en realizar actividades en línea con un fin exclusivamente político. El ciberterrorismo puede aludir a fines políticos, ideológicos, religiosos o sociales.

Solucionario

Ejercicios de autoevaluación

1. b

2. b

3. d

4. c

5. a

6. d

7. c

8. a

9. b

10. d

Bibliografía

Agustina, J. R. (2014). «Victimización en el ciberespacio. Victimología y victimodogmática en el uso de las TIC. Desfragmentación del yo en la era digital: 'disinhibittion effect', esquizofrenia digital e ingenuidad en el ciberespacio». En: Tamarit, N.; Pereda, J. M. (2014). *La respuesta de la victimología ante las nuevas formas de victimización*. Madrid: Edisofer.

Baumeister, R.; Leary, M. (2017). *Interpersonal Development*. Londres: Routledge.

Becoña, E. (2016). «Factores de riesgo y de protección en el uso problemático de Internet». En: Echeburúa, E. (coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?* Madrid: Pirámide.

Bouzar, D. (2015). *La vie après Daesh*. París: Autrement.

Brickey, J. (2012). «Defining Cyberterrorism: capturing a broad range os activities in cyberspace». *Sentiel* (vol. 5, núm. 8, págs. 4-6). Combating Terrorism Center at West Point (CTC). Disponible en: http://bit.ly/2Wm8N1S

Cano, M. Á.; Castro, F. J. (2018). «El camino hacia la (Ciber) Yihad». *Revista electrónica de Ciencia Penal y Criminología* (núm. 20, págs. 1-36). Disponible en: http://criminet.ugr.es/recpc/20/recpc20-15.pdf

Cano, M. Á. (2019). «La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico». *Revista Científica General José María Córdova* (vol. 17, núm. 26, págs. 271-287).

Carbonell, X.; Torres, A.; Fuster, H. (2016). «El potencial adictivo de los videojuegos». En: Echeburúa, E. (coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?*. Madrid: Pirámide.

Cohen-Almagor, R. (2017). «Jihad Onlie: How Do Terrorists Use the Internet?». En: Campos, F.; Rúas, X.; Alejandro, V.; López, X. (eds.). *Media and Metamedia Management* (págs. 55-66). Dordrecht: Springer.

Cohen, E.; Felson, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach». *American Sociological Review* (vol. 44, núm. 44, págs. 588-608).

Denning, D. E. (2000). *Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*. Washington, EE. UU.: House of Representatives.

Denning, D. E. (2001). *Is Cyber Terror Next?*. Washington, EE. UU.: Social Science Research Council. Disponible en: http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm

Grabosky, P. (2001). «Virtual Criminality: Old Wine in New Bottles?». *Social & Legal Studies* (vol. 10, núm. 2, págs. 243-249).

Guirao Cid, M. C. (2019). «La ciberradicalització: una nova forma de victimització». *IDP. Revista d'Internet, Dret i Política* (núm. 29). UOC. DOI: http://doi.org/10.7238/idp.v0i29.3171

Halopeau, B. (2014). «Terrorist use of the internet». En: Babak, A.; Stainforth, A.; Bosco, S. *Cyber Crime and Cyber Terrorism. Investigator's Handbook*. Ed. Elsevier.

Hoffman, B. (2006). *Inside Terrorism*. Nueva York: Columbia University Press.

Jahankhani, H.; Al-Nemrat, A.; Hosseinian, A. (2014). «Cyber crime Classification and Characteristics». En: Babak, A.; Stainforth, A.; Bosco, F. *Cyber Crime and Cyber Terrorism Investigator's Handbook* (págs. 149-164). Ed. Elsevier.

Kandel, J. (2004). «Organisierter Islam in Deutschland und gesellschaftliche Integration». *Politisch Akademie der Friederich-Ebert-Stiftung* (págs. 1-19).

Khosrokhavar, F. (2003). *Los nuevos mártires de Alá*. Madrid: Ed. Martínez Roca.

Kruglaski, A.; Jasko, K.; LaFree, G. (2016). «Quest for Significance and Violent Extremism: The Case of Domestic Radicalization». *Political Psychology* (vol. 38, núm. 5).

Kruglaski, A.; Jasko, K.; Webber, D.; Chernikova, M. (2018). «The Making of Violent Extremist». *Review of General Psychology* (vol. 1, núm. 22, págs. 107-120).

Lemieux, T.; Brachman, J.; Levitt, J.; Wood, J. (2014). «Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model». *Terrorism and Political Violence* (vol. 26, núm. 2, págs. 354-371).

Lewis, J. A. (2002). «Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats». *Center for Strategic and International Studies*.

Luiijf, E. (2014). «Definitions of Cyber Terrorism». En: Babak, A.; Stainforth, A.; Bosco, S. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Ed. Elsevier.

Mantel, B. (2009). «Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?». *CQ Researcher* (págs. 129-152).

Miró, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminológica* (núm. 13, págs. 1-55).

Mshvidobadze, K. (2011). «State-sponsored Cyber Terrorism: Georgia's Experience». *Georgian Foundation for Strategic and International Studies* (págs. 1-7).

National Research Council (1991). *Computers at Risk: Safe Computing in the Information Age*. Washington, EE. UU.: National Academy Press.

Prensky, M. (2001). «Nativos digitales, inmigrantes digitales». *On the horizon* (vol. 9, núm. 5, págs. 1-7).

Reinares, F.; García-Calvo, C. (2016). *Estado Islámico en España*. Madrid: Real Instituto Elcano.

Reinares, F.; García-Calvo, C. (2017). «Actividad yihadista en España, 2013-2017: de la Operación Cesto en Ceuta a los atentados en Cataluña». *Documento de trabajo 13/2017*. Madrid: Real Instituto Elcano.

Reinares, F.; García-Calvo, C.; Vicente, A. (2018). «Yihadismo y prisiones: un análisis del caso español». *ARI 123/2018*. Madrid: Real Instituto Elcano.

Rollins, J.; Wilson, C. (2007). «Terrorist Capabilities for Cyberattack: Overview and Policy issues». En: Linden, E. V. (ed.). *Focus on Terrorism* (núm. 9, págs. 43-63).

Ruiz, J. (2016). «Ciberamenazas: ¿el terrorismo del futuro?». *Documento de Opinión Instituto Español de Estudios Estratégicos*. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Said, B. (2012). «Hymns (Nasheeds): A Contribution to the Study of the Jihadist Culture». *Studies in conflict & terrorism* (vol. 35, núm. 12, págs. 863-879).

Silber, M.; Bhatt, A. (2007). *Radicalization in the West: The Homegrown Threat.* Police Department City of New York.

Suler, J. (2004). «The Online Disinhibition Effect». *Cyber Psychology & Behavior* (vol. 7, núm. 3, págs. 321-326).

Torres, M. R. (2016). «Cómo contener a un califato virtual». *Cuadernos de estrategia* (núm. 180, págs. 167-194).

Torres, M. R. (2018). «El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato». *Cuadernos de estrategia* (núm. 197, págs. 197-224).

Torres Díaz, O. (2015). «La propagada del Daesh también es cosa de mujeres. De Umm Sumayyah Al-Muhajira en Dabiq al manifiesto de la Brigada Al-Khansaa en Internet». *Documento opinión* (núm. 121).

Trujillo, H. M.; Moyano, M.; González-Cabrera, J. (2006). «De la agresividad a la violencia terrorista. Historia de una patología psicosocial previsible (parte II)». *Behavioural Psychology* (vol. 14, núm. 2, págs. 289-303).

UNODC (2013). *El uso de internet con fines terroristas*. Naciones Unidas. Disponible en: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Weimann, G. (2004). «Cyberterrorism. How Real Is The Threat?». *Special Report* (núm. 119). United States Institute of Peace. Disponible en: https://www.usip.org/sites/default/files/sr119.pdf