ieee.es
Instituto Español de Estudios Estratégicos
1970 — 2020

Documento
Opinión

11/2021 2 de febrero de 2021

Luis Miguel Sánchez-Gil *

Repensando el concepto de ciberterrorismo

Repensando el concepto de ciberterrorismo

Resumen:

En la actualidad, no existe un consenso en la comunidad de expertos en torno al concepto de ciberterrorismo. Esto, entre otras cuestiones, deriva de la ausencia de una definición universal de terrorismo. El ciberterrorismo —como táctica— constituye una forma de terrorismo ejecutada en un escenario *online*. Este comprende una gran diversidad de actividades cuya delimitación resulta de gran importancia, ya que los grupos terroristas también emplean la red con otros objetivos mediatos. Por ello, desde el punto de vista criminológico, se trata de enfocar este fenómeno criminal y aportar algunas claves en la construcción de un concepto adecuado, más allá de las delimitaciones extensivas o estrictas del derecho, que favorezca la elaboración de legislaciones homólogas a nivel internacional en materia de lucha antiterrorista.

Palabras clave:

Ciberterrorismo, terrorismo, ciberataque, propaganda.

Reformulating the concept of cyberterrorism

Abstract:

There is currently no agreement in the expert community on the concept of cyberterrorism. This, among other issues, is due to the lack of a universal definition of terrorism. Cyberterrorism —as a tactic— is a form of terrorism carried out in an online setting. This includes a wide variety of activities whose delimitation is important, since terrorist groups also use the internet for other purposes. Consequently, from a criminological point of view, it is about addressing this criminal phenomenon to construct an adequate concept, beyond the extensive or strict delimitations of the Law, that facilitates the elaboration of homologous legislation at the international level in the fight counterterrorist.

Keywords:

Cyberterrorism, terrorism, cyber-attack, advertising.

Cómo citar este documento:

SÁNCHEZ-GIL, Luis Miguel. *Repensando el concepto de ciberterrorismo*. Documento de Opinión IEEE 11/2021.
http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO11_2021_LUISAN_RepCib.pdf
y/o enlace bie[3] (consultado día/mes/año)

Introducción

En torno al concepto de terrorismo existe un continuo debate entre la comunidad internacional, que no consigue definir —de modo consensuado— su marco esencial y sus límites. Al respecto, hay quien señala lo siguiente: «Generalmente se habla de "terrorismo" y de los "terroristas" dando por sentado el significado de estas palabras. Sin embargo, aún no disponemos de una definición de los fenómenos terroristas que concita un consenso más o menos universal. Los Estados se niegan a firmar convenios globales de cooperación antiterrorista porque no son capaces o no quieren llegar a un acuerdo sobre qué actos, individuos y organizaciones debieran ser descritos como terroristas. Los ciudadanos de a pie y los medios de comunicación difieren en los criterios con los que emplean el término "terrorista, y ni siquiera los expertos están totalmente de acuerdo al respecto».

El terrorismo es un fenómeno complejo y dinámico y —esta cuestión— lejos de ser un aspecto banal, se manifiesta en graves consecuencias como la ineficacia de los mecanismos de cooperación internacional en materia antiterrorista, la heterogeneidad normativa que se relaciona con un elevado nivel de inseguridad jurídica, la sobreexplotación del término, la división de opiniones y análisis que favorecen una visión difusa[1]. La ausencia de un acuerdo, perfectamente identificable en circunstancias como las reseñadas, deriva en la imposibilidad de establecer unos elementos esenciales que caractericen a la conducta terrorista. Esta circunstancia resulta evidente y ha sido reflejada en numerosos estudios, entre los que destaca el realizado por Bakker (2015), cuyas conclusiones sobre la falta de consenso en torno al terrorismo son: (1) ineficacia en el ámbito de la cooperación internacional en materia antiterrorista; (2) perspectiva legal heterogénea de la que derivan abusos del término; (3) inseguridad a nivel jurídico; y (4) división de opiniones y dictámenes entre los expertos y estudioso del fenómeno de la que resulta una visión difusa[2]. Otra muestra, se halla en la exposición de motivos y el

[1] SÁNCHEZ-GIL, Luis Miguel. "Terrorismo: conceptualización y consecuencias de su indefinición", *Archivos de Criminología*, Seguridad Privada y Criminalística, 18, 2017. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5813532.pdf Fecha de la consulta 30.07.2020
[2] BAKKER, Edwin. "Terrorism and counterterrorism: comparing theory and practice", *Leiden University,* 2015, Países Bajos.

objeto de las últimas directivas europeas en esta materia. Así, por ejemplo, la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017, señala: «el carácter transfronterizo del terrorismo exige una firme y coordinada respuesta y una firme cooperación en y entre los Estados miembros, así como con y entre las agencias y órganos competentes de la Unión para combatir el terrorismo, entre otros Eurojust y Europol. A tal fin, se debe hacer un uso eficaz de las herramientas y recursos de cooperación disponibles, como los equipos conjuntos de investigación y las reuniones de coordinación organizadas por Eurojust. El carácter mundial del terrorismo requiere una respuesta internacional, lo que exige que la Unión y sus Estados miembros refuercen la cooperación con los terceros países pertinentes. La respuesta firme y coordinada y la cooperación firme son también necesarias para proteger y obtener pruebas electrónicas»[3].

Además, en su objeto, el citado documento afirma que «la presente directiva establece normas mínimas relativas a la definición de las infracciones penales y las sanciones de los delitos de terrorismo, los delitos relacionados con un grupo terrorista y los delitos relacionados con actividades terroristas, así como medidas de protección, apoyo y asistencia a las víctimas del terrorismo»[4]. Este documento palia el problema de la heterogeneidad normativa en el ámbito de la Unión Europea. Sin embargo, esta cuestión permanece al traspasar sus fronteras sus fronteras, tratando de ser socavada a través de la creación de foros internacionales como los encabezados por la Naciones Unidas y otros —con presencia de España— como el Comité Interamericano contra el Terrorismo (CICTE)[5]. Naciones Unidas (2018) señalan, al respecto, que «todo instrumento regional tiene, por definición un alcance geográfico limitado, lo que hace que los instrumentos universales contra el terrorismo sean una opción más interesante como red de cooperación verdaderamente mundial cuando los Estados parte tratan de prestar asistencia a países que se encuentran fuera de su región, o de recibirla de estos»[6]. A

[3] Diario Oficial de la Unión Europea, "Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo por la que se sustituye la Decisión Marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo, Unión Europea, 2017. Disponible en: https://www.boe.es/doue/2017/088/L00006-00021.pdf Fecha de la consulta 29.11.2020.
[4] Ibid. (3).
[5] Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, "Lucha contra el terrorismo desde los Foros Internacionales", Gobierno de España, 2020. Disponible en: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Terrorismo/Paginas/LuchaContraElTerrorismoDesdeLosForosInternacionales.aspx Fecha de la consulta 29.11.2020
[6] Oficina de la Naciones Unidad contra la Droga y el Delito, "El Marco Jurídico Universal contra el Terrorismo", Naciones Unidas, Viena, 2018. Disponible en:

pesar de lo cual, no existe un instrumento global que posibilite tal realidad. Este hecho se extrapola a vocablos derivados —y estrechamente vinculados con el terrorismo— como el de ciberterrorismo.

Internet surge, en la segunda mitad del siglo XX, como un conjunto de redes que termina por convertirse en un espacio de encuentro a nivel mundial. Esta creación muestra una serie de características inéditas hasta el momento, influyendo de forma decisiva en la globalización. Internet cambia sustancialmente el formato de las relaciones humanas, los métodos comerciales, las transacciones económicas, etc. Sin embargo, no todo lo que discurre en la esfera virtual son conductas prosociales, siendo aprovechado —igual que sucede con otros instrumentos— por individuos y organizaciones criminales en beneficio de sus actividades. Debido a la naturaleza del terrorismo, Internet pronto se perfila como una herramienta que potencia en gran medida sus capacidades.

Multitud de estudiosos han identificado en el terrorismo el elemento publicitario como un rasgo esencial, al que organizaciones e individuos dedican grandes esfuerzos. En estos términos, Schmid, Jongman y otros autores[7] realizan un análisis de diversas definiciones de terrorismo, recopilando los 22 elementos que se encontraban presentes en ellas con mayor frecuencia. Entre estos —en la posición número 3— figura la propagación del terror, presente en un 51 % de las conceptualizaciones, y —en la posición 11— se fija el aspecto publicitario, recogido en un 21,5 % de los casos. No obstante, aunque estas sean dos de las actividades más reconocibles desarrolladas por los grupos terroristas en la red, estos aprovechan sus posibilidades para una gran diversidad de funciones.

Operativa de las organizaciones terroristas en Internet

Las actividades que las organizaciones implicadas en acciones terroristas desarrollan en Internet son muy diversas, pudiendo clasificarse, atendiendo a su función, en: financiación, propaganda, adoctrinamiento, adiestramiento, comunicación interna, planificación y ejecución.

https://www.unodc.org/documents/terrorism/Publications/Module%202/Module_2_Spanish.pdf Fecha de la consulta 29.11.2020.

[7] BRUCE, Gregor. “Definition of Terrorism Social and Political Effects”, *Journal of Military and Veterans*, Health, 21, 2, 2013. Disponible en: http://jmvh.org/wp-content/uploads/2013/06/Definition-of-Terrorism.pdf Fecha de la consulta 31.07.2020.

Financiación

Los grupos implicados en actividades terroristas requieren recursos económicos para su operativa y subsistencia. Los ingresos necesarios oscilan en virtud de su dimensión y pretensiones operativas. Así, es posible encontrar organizaciones como el Irish Republican Army (IRA) —que ha llegado a manejar un presupuesto anual superior a los 450 millones de dólares[8]—, pasando por otras con menor volumen, como Euskadi Ta Askkatasuna (ETA), cuyo aparato manejaba un presupuesto anual de entre 5,01 y 6,68 millones de euros[9]. Tradicionalmente, se han empleado los atracos, secuestros, la extorsión, los tráficos ilícitos y las donaciones como medios de financiación. Estas modalidades delictivas también se han trasladado a la esfera de Internet donde las estafas han adoptado la forma de *carding*, *phishing* (con sus diferentes variedades), *pharming*, *ransomware*… Además, los tráficos ilícitos han hallado en la *deep web* un espacio de mercado ideal para la comercialización de sus productos (sustancias psicotrópicas y estupefacientes, armas, etc.). Algunas organizaciones criminales encuentran en estas actividades vías sencillas de financiación, evitando tener que recurrir a otras más complejas.

Propaganda

La publicidad es uno de los objetivos que persiguen las acciones terroristas, en algunos casos —es posible afirmar— que constituye el principal objetivo. En relación con este, no puede quedar en el tintero aquella afirmación de que el terrorismo no desea causar muchas víctimas, sino tener muchos ojos mirando[10]. Bien es cierto que esta máxima ha evolucionado con el terrorismo yihadista, cuyo foco de actuación se encuentra en muchas ocasiones en lugares de poco interés mediático para Occidente. Esta realidad ha conducido a que los grupos hayan observado como la repercusión mediática de sus atentados fuera de Occidente es proporcional al número de víctimas mortales que

[8] "Así se financian los siete grupos terroristas más ricos del mundo", *La Información*, 24 de noviembre de 2015. Disponible en: https://www.lainformacion.com/asuntos-sociales/asi-se-financian-los-siete-grupos-terroristas-mas-ricos-del-mundo_RqLldBShQ7MvcOB5BwC5M3/ Fecha de la consulta 31.07.2020.
[9] AIZPEOLEA, Luis. "Las cuentas del terrorismo etarra", *El País*, 22 de febrero de 2018. Disponible en: https://elpais.com/politica/2018/02/21/actualidad/1519238990_863473.html Fecha de la consulta 31.07.2020.
[10] JENKINS, Brian. "International terrorism: a new kind of warfare", *The Rand Corporation*, junio de 1974. Disponible en: https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf Fecha de la consulta 01.08.2020.

generan, lo que —a su vez— ha provocado un incremento de la violencia. Este hecho también ha sido facilitado por la alta permisividad de las bases (seguidores y simpatizantes), respecto a la actividad de este tipo de grupos.

Por otro lado, no cabe duda de que se ha producido un cambio en el paradigma de la información. La actualidad se ha trasladado de los diarios impresos a la prensa electrónica y de la radiotelevisión a las plataformas de retransmisión por Internet. No obstante, el mayor impacto ha sido el generado por la irrupción en la función informativa de las redes sociales. Con ello, el rol periodístico ha sido asumido por la ciudadanía y la capacidad de influencia a través de la información ya no solo reside en los medios especializados, sino también en otro tipo de organizaciones e individuos. Este nuevo escenario presenta una serie de ventajas e inconvenientes que resulta importante considerar, ya que sus consecuencias pueden tener un gran impacto.

En relación con lo expuesto, las organizaciones implicadas en el terrorismo yihadista han llegado a convertirse en «una de las mejores agencias de marketing y de producción de contenidos multimedia digitales del mundo»[11]. Internet constituye un canal que facilita a estos grupos la comunicación del mensaje directamente, mediante el contacto entre emisor y receptor, convirtiendo en innecesario el papel mediador de los medios de comunicación tradicionales. Así, la organización terrorista difunde su mensaje sin ningún tipo de filtro ni condicionante, más que el de las posibilidades ofrecidas por la plataforma elegida. Además, también se suprimen las limitaciones espaciotemporales, facilitando que el mensaje alcance a más personas (capacidad de difusión global) y su exposición se prorrogue durante más tiempo (permanencia).

La finalidad de la propaganda puede ser el adoctrinamiento o la simple propagación del terror entre la ciudadanía. Entre los productos estrella de organizaciones como el Dáesh, se halla la producción de series documentales y los vídeos de ejecución. En estos «la calidad del sonido, la imagen y la edición eran propias de una serie de HBO o de Netflix»[12]. Así han intentado transformar el terrorismo en «un producto de comunicación popular comprensible, seductor, bello e imitable»[13].

[11] LESACA, Javier. *Armas de seducción masiva. La factoría audiovisual de Estado Islámico para fascinar a la generación millennial*, Ediciones Península, Barcelona, 2017.
[12] Ibid. (6).
[13] Ibid. (6).

Con similar profesionalidad, la misma organización, ha empleado las redes sociales para realizar campañas mediáticas con las que distribuir información elaborada —a través de fotogramas, infografías, etc.— sobre sus actividades violentas o publicar una gran diversidad de revistas, entre otras finalidades.

La actitud de las plataformas y de los medios de comunicación ante estas publicaciones ha sido muy cuestionada, llegando recientemente a un consenso —casi total— sobre la adecuación de censurar y eliminar gran parte de estos contenidos a la mayor brevedad posible.

La posición de los grupos respecto a las difusiones ha sido muy clarividente desde el primer momento, apostando por la mayor exposición que le facilita la Internet visible, frente a la mayor seguridad que le podría reportar la *deep web*.

Adoctrinamiento

En el adoctrinamiento podrían agruparse los procesos de radicalización violenta y reclutamiento. Se entiende por radicalización violenta «el fenómeno en virtud del cual las personas se adhieren a opiniones, puntos de vista e ideas que pueden conducirles a cometer actos terroristas»[14]. Mientras que el reclutamiento —en el contexto del terrorismo— puede ser definido como un proceso a través del cual un individuo se adhiere a un grupo guiado por una ideología radical favorecedora de la conflictividad con otros grupos y del empleo de la violencia, concurriendo la posibilidad de que la persona se implique en actos terroristas[15]. Sobre la relación cronológica entre ambos procesos también existen ciertas diferencias entre los estudiosos, motivada por la heterogeneidad de la casuística y la diversidad de enfoques.

Internet ha sido un instrumento esencial en la evolución de los procesos de radicalización y reclutamiento desde hace más de una década. A pesar de que, tal y como demuestran algunos estudios realizados en España, la radicalización exclusivamente *online* se produce —tan solo— en un porcentaje inferior al 10 %, predominando la radicalización

[14] Comisión de las Comunidades Europeas, "Comunicado de la Comisión al Parlamento Europeo y al Consejo sobre la captación de terroristas: afrontar los factores que contribuyen a la radicalización violenta", Unión Europea, 2005. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005DC0313&from=ES Fecha de la consulta 01/08/2020.
[15] MOYANO, Manuel y TRUJILLO, Humberto. "Radicalización islamista y terrorismo. Claves psicosociales", Editorial Universidad de Granada, Granada, 2013.

en entornos presenciales o metodologías mixtas[16], no obstante, resulta evidente que este medio ha potenciado las capacidades de adoctrinamiento de las organizaciones dedicadas al terrorismo, además de facilitar la movilización. Esta queda perfectamente retratada en el incremento exponencial del número de *foreign terrorist fighters* en los últimos conflictos.

Para el adoctrinamiento, los grupos emplean contenidos propagandísticos, como los ya referenciados, en los que, a menudo, adoptan una posición victimista y tratan de proyectar sus actividades como una reacción a las maniobras de sus Estados o a las intervenciones de terceros.

Los servicios que le suministra la red son muy variados, destacando las plataformas de comunicación (mensajería, chat, etc.) y de exposición (imágenes, vídeos, etc.). Al respecto, pueden diferenciarse tres modelos de comunicación entre emisor y receptor. El primer modelo (M1) son difusiones masivas de las organizaciones en las que frecuentemente aparecen figuras de relevancia en la jerarquía de estas, siendo comunicaciones unidireccionales de tipo vertical descendiente (de la cúpula hacia las bases). Un segundo tipo de modelo (M2) está engrosado por comunicaciones de tipo bidireccional, pero en las que existe una relación jerárquica entre emisor y receptor. El ejemplo más paradigmático es el de las enseñanzas compartidas por los agentes de radicalización con sus potenciales adeptos. La comunicación fluye en ambos sentidos, a través de aplicaciones de mensajería instantánea, chat, foros, etc. Sin embargo, el radicalizador se ubica jerárquicamente en un estadío superior al del potencial militante. Finalmente, el tercer modelo (M3) está formado por los denominados grupos de intercambio. Estos son grupos de iguales, que operan habitualmente en plataformas de mensajería instantánea, en los que todos los miembros poseen el mismo estatus y comparten contenidos retroalimentando su radicalización.

En estas prácticas, las organizaciones se han mostrado especialmente habilidosas, enfocando los materiales al público al que se encuentran dirigidos, al cual perfilan para vender el producto (sus narrativas), de tal forma que Dáesh ha proyectado la vida en el califato como un remanso de paz y tranquilidad en el que hacer una vida familiar libre de

[16] REINARES, Fernando; GARCÍA-CALVO, Carola y VICENTE, Álvaro. "Yihadismo y yihadistas en España", *Real Instituto Elcano*, 2019. Disponible en: http://129.35.96.157/wps/wcm/connect/7c5ffe5f-3455-4d99-b5ee-bf24da041511/yihadismo-yihadistas-espana-quince-anos-despues-11-M.pdf?MOD=AJPERES&CACHEID=7c5ffe5f-3455-4d99-b5ee-bf24da041511 Fecha de la consulta 02.08.2020.

la enfermedad social de Occidente, al tiempo que la mostraba como una experiencia repleta de aventuras trepidantes en las que manejar armamento de guerra y combatir constantemente como si de un videojuego se tratase. No han perdido la oportunidad de publicar fotografías en paradisiacos resorts o en tétricos paisajes posando con cabezas tras la decapitación de múltiples cuerpos. Todo ello adoptando una estrategia comunicativa adaptada al momento actual, alejada de los densos discursos de iconos del movimiento en cuevas recónditas.

Adiestramiento

De un modo similar al de organizaciones formativas, las organizaciones terroristas han aprovechado las posibilidades de Internet para difundir manuales y videotutoriales con los que facilitar la comisión de actos terroristas. Su difusión se ha producido tanto en materiales específicos (manuales de combate, vídeos explicativos para la confección de explosivos…) como en el interior de otros contenidos más genéricos, entre los que cabe destacar las revistas electrónicas de Al Qaeda y Dáesh. En estas últimas, se han expuesto diversas tácticas y métodos tales como las formas de ocultación de armas en aeropuertos, la confección de artefactos explosivos con sustancias y materiales de fácil acceso, las consideraciones para la comisión de un atentado con vehículo, la construcción de una pieza para el descarrilamiento de un tren, etc.

Los ejemplos enumerados en las líneas precedentes y otros muchos contenidos similares, han sido empleados por terroristas individuales y células para la comisión de atentados.

Comunicación interna

El uso de Internet para establecer comunicaciones entre actores de la organización terrorista es otro de los usos que se ha hecho de esta tecnología. La red ha revolucionado el mundo de las comunicaciones, dejando atrás las conexiones analógicas. En cambio, en relación con esta función, los grupos han manifestado especial cuidado con la seguridad y privacidad en las interacciones, a fin de evitar su detección por las fuerzas y cuerpos de seguridad y servicios de inteligencia.

La subsistencia de las organizaciones y su éxito en las acciones depende, en muchos casos, del mantenimiento del secreto de las comunicaciones. Para ello, se han empleado en la adopción de técnicas como el *dead dropping* —ya superada y en desuso— o el diseño de aplicaciones de mensajería cifrada (como Mujahideen Secrets), entre otras. Así, se han planificado y gestionado multitud de actuaciones terroristas o conexiones con fines específicos de financiación, logística, etc. En el año 2004, la célula afín a Al Qaeda del 11 de marzo empleó el *dead dropping* entre sus métodos de comunicación.

Planificación

Internet ha posibilitado el acceso a multitud de información, cuya consulta resultaba compleja hasta su llegada. Además, la irrupción de nuevas tecnologías ha permitido desarrollar contenidos novedosos e inéditos, multiplicando exponencialmente la información disponible en la red.

Entre los servicios que pueden resultar de gran utilidad a las organizaciones en la planificación de un atentado se encuentra el libre acceso a mapas —lo que facilita el establecimiento de objetivos, rutas de acceso y salida al lugar, etc.—, la construcción de un presupuesto sin necesidad de identificarse o acudir a los lugares de adquisición —accediendo, por ejemplo, al coste de alquiler de un determinado vehículo, etc.—.

Ejecución

En la función ejecutiva, se encuentran los denominados, de manera estricta, como ciberataques. Estos pueden definirse como «el uso del ciberespacio para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través de aquel. El atacante busca acceder sin autorización a información o alterar o impedir el funcionamiento de los servicios»[17].

Entre las técnicas más frecuentes de ciberataque se encuentran los *malware* (virus informáticos), el envío masivo de correo no deseado o Spam, la suplantación de remitentes de mensajes mediante *spoofing*, el envío o instalación de archivos espías o

[17] PRIETO OSÉS et al. “Guerra Cibernética: aspectos organizativos”, *Escuela de Altos Estudios de la Defensa*, XXXIII Curso de Defensa Nacional. Disponible en: https://docplayer.es/2279115-Guerra-cibernetica-aspectos-organizativos.html Fecha de la consulta 03.08.2020.

keyloggers, el uso de troyanos para el control remoto de los sistemas o la sustracción de información, el uso de archivos BOT del Internet Relay Chat (IRC) y el uso de *rootkits*. Estos pueden dar lugar a cambios en las direcciones de dominio (DNS), intrusiones no autorizadas, denegación de servicio (DDoS), saturación de cuentas de correo electrónico, interferencia electrónica de comunicaciones, BlindRadars o bloqueo del tráfico aéreo, robos de información, anulación de equipos, pulsos electromagnéticos, etc.[18].

En este ámbito, la capacidad de las organizaciones yihadistas se encuentra bastante limitada, reduciéndose los ataques a intrusiones en cuentas en redes sociales de determinadas organizaciones (como, por ejemplo, el Mando Central Militar de los Estados Unidos) o personalidades. Sin embargo, otros grupos especializados, entre los que destaca Anonymous, han sido protagonistas de importantes ciberataques como el que provocó la denegación de servicio en los servidores de PayPal en el año 2010[19].

Concepto estricto vs. concepto extensivo

Existe un debate sobre la denominación correcta de las conductas delictivas ejecutadas a través de Internet. Frente a los conceptos de ciberdelito o cibercrimen, son muchos los que optan por la etiqueta de cibercriminalidad, criminalidad cibernética o criminalidad informática. Entre los motivos principales, se señala que no constituyen tipos delincuenciales específicos, siendo únicamente formas de comisión de delitos preexistentes en el mundo offline. En virtud de ello puede entenderse el ciberterrorismo como una acción de terrorismo, con la particularidad de que no se emplea la presencialidad del individuo o individuos, sino que se comete empleando la red.

En estos términos, la doctrina desarrolla un concepto estricto y reduccionista de ciberterrorismo que se limita a las acciones de ciberataque empleadas con fines terroristas. Es decir, son ciberataques cuya motivación principal es la propagación de terror. Cabe reseñar que, con frecuencia, este tipo de acciones no presentan esta finalidad sino la de buscar un beneficio económico. En esta concepción se encuadraría

[18] URUEÑA CENTENO, Francisco J. *Ciberataques, la mayor amenaza actual*, Documento Opinión, Instituto Español de Estudios Estratégicos, 16 de enero de 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf Fecha de la consulta 03.08.2020.
[19] Ibid. (13).

la definición del Federal Bureau of Investigation (FBI) que señala que «el ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos»[20].

En definitiva, este enfoque incluiría dentro del concepto de ciberterrorismo la función de ataque —a través de los ciberataques—, excluyendo el resto de las actividades *online* de las organizaciones implicadas en actos terroristas y que se encuentren dirigidas a perseguir tales fines, como la financiación, la propaganda, el adoctrinamiento, el adiestramiento o la planificación.

Sin embargo, algunas corrientes de personalidades y organismos dentro del ámbito del terrorismo se posicionan a favor de un concepto extensivo de ciberterrorismo[21]. Desde esta perspectiva el ciberterrorismo se encontraría definido por el titular que ejecuta la conducta (el grupo terrorista), entendiéndose por tal toda actividad que un grupo o sus miembros llevan a cabo a través de Internet como fin o medio —siendo aquí donde se produce la principal diferencia con la concepción anterior— para la comisión de una acción terrorista.

A tenor de lo expuesto, aunque ambos enfoques considerarían ciberterrorismo a un ciberataque con los fines señalados, el primero extrae de dicho marco, por ejemplo, la publicación de vídeos con la decapitación de prisioneros o amenazas a los Estados apóstatas e infieles. Al mismo tiempo, el enfoque extensivo incluye como conducta ciberterrorista las estafas cibernéticas cometidas con objetivos de financiación del grupo o las conversaciones vía chat entre sus miembros.

La conciliación de ambas perspectivas puede resultar complicada desde la óptica del derecho. Sin embargo, parece un aspecto esencial en favor de alcanzar un consenso que favorezca el diseño en materia de política criminal y la operativa en el ámbito de la seguridad en la lucha contra esta fenomenología.

[20] Ibid. (13).
[21] ROMERO DONOSO, Julián. “Ciberterrorismo: Policía 3.0. En la Nueva Dimensión de la Seguridad”, *Seminario Nacional sobre Ciberterrorismo*, 27 de noviembre de 2014, Valladolid.

Hacia una construcción criminológica

Desde la Criminología, como ciencia que se encarga del estudio de las conductas transgresoras (o susceptibles de serlo), se pueden esclarecer algunas de las cuestiones planteadas en líneas precedentes, colaborando con la creación de un concepto marco de terrorismo y, por extensión, de ciberterrorismo, definiendo las características específicas de este último.

Resulta esencial establecer el objetivo de la acción (no el fin último) como elemento clave a la hora de calificarla. En consecuencia, podría fijarse como leitmotiv de los actos de terrorismo la difusión del terror entre la población con fines políticos (entre los que se incluyen las motivaciones religiosas). En estos términos hay que centrar el foco desde la perspectiva de la organización —cuando el sujeto sea un militante— o desde el individuo, cuando este carezca de una identidad grupal. Es decir, en el caso del militante puede que su objetivo y el del grupo difieran, debiéndose atender al de este último para calificar el acto. Así, por ejemplo, un miembro del Dáesh puede ejecutar un atentado para lograr reconocimiento entre sus correligionarios, verse inmerso en experiencias de acción u otras metas individuales que no se encuentran en línea con los fines estratégicos del grupo. Por ello, el objetivo del acto será entendido —en relación con el aspecto que ocupa el presente texto— desde la perspectiva de la organización. En virtud de lo cual, se puede fijar como *leitmotiv* del terrorismo la difusión del terror mediante el uso de la violencia ilícita con fines políticos (entre los que se encuentran comprendidos los de naturaleza religiosa). Por lo que el *modus operandi* del terrorismo abarcaría tanto acciones dirigidas al uso de la violencia como aquellas encaminadas a su difusión, siempre que se observe la citada finalidad.

En este marco, podrían ser consideradas acciones de ciberterroristas las actividades de ejecución (ciberataques), propaganda y aquellas acciones de adoctrinamiento cuyo objetivo sea causar terror en la población mediante manifestaciones de violencia ilícita con fines políticos. En esta concepción no entrarían las actividades de financiación, adiestramiento, planificación y aquellas de adoctrinamiento que no cumplan con dicha finalidad. Esta circunstancia no significa que las acciones carezcan de valor o significado a nivel penal o de investigación del fenómeno terrorista, sino que son actos que no pueden ser calificados como tales por sus efectos.

Reflexión final

En primer lugar, resulta necesario establecer una definición internacional de terrorismo que elimine gran parte de los problemas actuales en materia de cooperación internacional y defina los aspectos esenciales de la problemática. De esta manera, por ende, se concretarán los principales rasgos de algunas de sus formas, como el ciberterrorismo.

Además, se debe cambiar la perspectiva y dejar de referir determinadas organizaciones como grupos terroristas. Esta etiqueta (terrorista), no describe ni contiene la gran variedad de actividades —muchas de ellas criminales y violentas— que estas desarrollan. En este mundo de amenazas híbridas, se observa cómo los grupos combinan las tácticas terroristas con otras como la insurgencia, la guerra de guerrillas, el tráfico de drogas, etc. De modo que será más correcto hablar del terrorismo como táctica que convertirlo en un adjetivo por el que se defina una organización híbrida. En muchos casos, esta circunstancia ha conducido a que la sumisión del grupo en un determinado ámbito, como el militar, favorezca la sensación ilusoria de su derrota o disolución.

El ciberterrorismo debe ser concebido como una forma de terrorismo cuya comisión tiene lugar en el entorno *online*, pero cuyos efectos no difieren —en cuanto a su *leitmotiv*— de las acciones *offline*. En este, resulta más que necesario establecer definiciones universales que conduzcan a legislaciones homologas, ya que la red aumenta —aún más— la globalidad del fenómeno. La ciencia criminológica puede colaborar en esta tarea, ofreciendo análisis de las tácticas terroristas en escenarios *online*.

La irrupción de nuevas tecnologías relacionadas con Internet ha aumentado, sin lugar a duda, las capacidades de acción de los grupos terroristas y su rango de actividades, debiendo los Estados —en consonancia— adaptar sus legislaciones y herramientas de lucha contra el terrorismo.

*Luis Miguel Sánchez-Gil**
Subdirector de la Unidad de Análisis de la Conducta Criminal
Universidad de Salamanca