Revista de Derecho UNED, núm. 27, 2021

A VUELTAS CON EL TERRORISMO E INTERNET: HACIA UNA DEFINICIÓN DE CIBERTERRORISMO

STRUGGLING WITH TERRORISM AND THE INTERNET: TOWARDS A DEFINITION OF CYBERTERRORISM

Diego Montes Noblejas[1]

Resumen: La expansión de internet no solo ha generado innumerables beneficios y posibilidades, sino que también ha favorecido la aparición de las llamadas «ciberamenazas». Una de ellas, el «ciberterrorismo», es analizada en las siguientes páginas. El objetivo de este trabajo es ofrecer una definición propia de ciberterrorismo que pueda resultar válida desde la óptica del derecho internacional general. Para ello se sigue una aproximación inductiva.

[1] Máster en Estudios Internacionales y Europeos por la Universidad de Valencia. Diploma de Experto Universitario en Crimen Organizado Transnacional y Seguridad por la Universidad Nacional de Educación a Distancia. Graduado en Derecho y graduado en Economía por la Universidad de Castilla-La Mancha.

Primero, se proporciona una definición de terrorismo internacional obtenida después de sintetizar algunas de las nociones más relevantes en relación con dicho término. A continuación, tras exponer la importancia que tiene internet en el terrorismo internacional actual, se presenta dicha definición de ciberterrorismo. A este respecto, se opta por una concepción estricta que permite distinguir esta ciberamenaza de otras con las que habitualmente se confunde, como son «el uso de internet con fines terroristas» y el «hacktivismo». Por último, antes de presentar las conclusiones alcanzadas, se evalúan las posibilidades de que el ciberterrorismo acontezca en un futuro próximo y su consideración como una amenaza real.

Palabras clave: ciberterrorismo, uso de internet con fines terroristas, hacktivismo, terrorismo, definición.

Abstract*: The Internet growth not only has boosted countless advantages and possibilities, but also the rise of the so-called "cyberthreats". One of them, "cyberterrorism", is analysed on the following pages. This paper aims to provide an own definition of cyberterrorism which may be suitable from a general international law perspective. An inductive structure is employed to achieve it. Firstly, a definition of international terrorism is provided after having synthesised some of the most relevant insights regarding this nomenclature. Afterwards, once the significance of the Internet within current international terrorism is delineated, the sought cyberterrorism definition is presented. With regard to it, we adhere to a pure cyberterrorism definition since it helps to distinguish this cyberthreat from others which are usually confused with, such as "the use of the Internet for terrorist purposes" and "hacktivism". Finally, before expounding the conclusions, the likelihood of cyberterorism striking shortly and its considerations as a real threat are assessed.*

Key words*: cyberterrorism, use of the Internet with terrorist purposes, hacktivism, terrorism, definition.*

Recepción original: 11-12-2020

Aceptación original: 4-2-2021

I. INTRODUCCIÓN

La disruptiva aparición de internet a finales del siglo pasado como una nueva tecnología de la información y de la comunicación

(TIC) trajo consigo una inédita dimensión, el ciberespacio[2], entendido como un «entorno formado por componentes tangibles e intangibles para almacenar, modificar e intercambiar información usando redes de ordenadores»[3].

El progresivo desarrollo, extensión y perfeccionamiento de este entorno ha provocado que las oportunidades y bondades que brinda no pasen inadvertidas. Su naturaleza común, global y descentralizada lo ha erigido como punta de lanza de la globalización y del progreso tecnológico que hoy nos aprovecha. Gracias a algunas de sus características, como el fácil acceso con un reducido coste, el relativo anonimato, la gran capacidad de almacenamiento, la irrelevancia de las fronteras físicas y geográficas, o la veloz adaptación a las necesidades sociales, más de la mitad de la población mundial está presente en esta dimensión[4]. Puede decirse que, después de distintos avatares, la realidad cibernética se sitúa hoy casi en pie de igualdad con la realidad física en muchas facetas del día a día. Es ya otro lugar donde personas y comunidades enteras interaccionan, así como un espacio en el que los Estados, sus poderes públicos y las infraestructuras que los sustentan gozan cada vez de mayor presencia con el propósito de desempeñar las funciones y prestar los servicios esenciales que les son propios.

Ahora bien, dado el número de usuarios y el volumen del tráfico web, huelga decir que no todas las actuaciones sucedidas en el ciberespacio comparten los mismos intereses y motivaciones. La neutralidad[5] e incesable dinamicidad que lo caracterizan conlleva unas vulnerabilidades y unos riesgos que no siempre se puedan an-

---

[2] Aunque exista cierta tendencia a utilizarlos como sinónimos, debe conocerse que «ciberespacio» es una noción más amplia que «internet». *Vid.* YANNAKOGEORGOS, P. A., "Rethinking the Threat of Cyberterrorism", en CHEN, T. M., JARVIS, L. y MACDONALD, S. (Eds.), *Cybertorrism: Understanding, Assessment, and Response*, Springer, New York, 2014, p. 44.

[3] SCHMITT, M. N. (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber*, 2ª edición, Cambridge University Press, Cambridge, 2017, p. 564.

[4] La Unión Internacional de Telecomunicaciones (UIT) estimó que a finales de 2019 el 53,6% de la población mundial era usuaria de internet (*vid.* <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>).

[5] Según el Organismo de Reguladores Europeos de las Comunicaciones (BEREC, por sus siglas en inglés) la neutralidad de internet implica que «todo el tráfico que circula por una red es tratado de forma igual, independientemente del contenido, la aplicación, el servicio, el dispositivo o la dirección del que lo envía o lo recibe» (*vid.* <https://berec.europa.eu/eng/netneutrality/>). Sobre el origen de esta neutralidad y la necesidad de regular el estrato lógico o «código» de internet, *vid.* GARCÍA MEXIÁ, P., "El Derecho de Internet", en SEGURA SERRANO, A. y GORDO GARCÍA, F. (Coords.), *Ciberseguridad global: Oportunidades y compromisos en el uso del ciberespacio*, Editorial Universidad de Granada, Granada, 2013, pp. 77 y ss.

ticipar, repeler o subsanar. Por consiguiente, en aras de preservar y potenciar los valores esenciales de la comunidad internacional, ha de reconocerse que el ciberespacio es un terreno abonado para el florecimiento de las llamadas «ciberamenazas». De hecho, las «disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos»[6] son ya una de las principales preocupaciones institucionales[7]. Su posible materialización efectiva —en cuyo caso estaríamos más concretamente ante un ciberataque[8]— ha motivado diversas categorizaciones. Por ejemplo, es conocida aquella que distingue entre el «ciberespionaje», el «cibercrimen», la «ciberguerra» y el «ciberterrorismo»[9]. No obstante, el éxito de las mismas no puede depender de su perdurabilidad, pues la porosidad de la red de redes es tal que en ella calan continuamente otros nuevos riesgos, como el «hacktivismo» y las «amenazas híbridas»[10], lo que condena a cualquier clasificación[11] con vocación de permanencia a su infructuosidad por obsolescencia.

Comoquiera que la práctica no espera a las clasificaciones teóricas, antecedentes como los de Estonia en 2007, Georgia en 2008, *Stuxnet* en 2010 o *WannaCry* en 2017 ponen de relieve, si se permite

---

[6] Definición de ciberamenaza contenida en la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado*, 30 de abril de 2019, nº 103, p. 43442.

[7] Por ejemplo, el Foro Económico Mundial sitúa a los ciberataques como una de las siete amenazas cuya materialización es más probable, en cuyo caso se sitúaría entre las ocho que causarían un impacto más severo (*vid.* <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf>). Por ello, no es de extrañar la creciente importancia de indicadores específicos sobre ciberseguridad como el *Global Cibersecurity Index* de la UIT.

[8] La regla nº 92 del *Manual de Tallín 2.0* entiende por ciberataque «aquella operación cibernética, ya sea ofensiva o defensiva, de la que cabe esperar razonablemente que cause lesiones o la muerte de personas o el daño o la destrucción de bienes». *Vid.* SCHMITT, M. N. (Ed.), *Tallinn Manual (…)*, *op. cit.*, p. 415.

[9] NYE JR., J. S., *Cyber Power*, Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, 2010, p. 16.

[10] Sobre las amenazas híbridas se señala que «el objeto de este concepto es subrayar la mezcla de actividades coercitivas y subversivas, de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos), que pueden ser utilizados de forma coordinada por agentes estatales o no estatales para lograr objetivos específicos, manteniéndose por debajo del umbral de una guerra declarada oficialmente». *Vid. Comunicación conjunta al Parlamento Europeo y al Consejo: Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea*, JOIN/2016/018 final/3, 30 de junio de 2017.

[11] La Estrategia de Nacional de Ciberseguridad de 2019 (*vid. supra* nota 6) recoge de forma confusa una clasificación de cuatro ciberamenazas: ciberespionaje, cibercrimen, hacktivismo y amenazas híbridas. En ella la ciberguerra no se nombra y el ciberterrorismo queda catalogado como un caso de cibercrimen.

la licencia, que el partido había comenzado y algunos ni siquiera se habían bajado del autobús. Esta situación ha espoleado la respuesta de los Estados y de las Organizaciones internacionales (en adelante, OI). Por un lado, numerosos Estados cuentan ahora con sus propias estrategias nacionales de ciberseguridad[12]. Por el otro, escenarios esbozados otrora como una mera ficción se empiezan a considerar quizá no tan lejanos. De ahí, por ejemplo, que tanto el Departamento de Defensa de los Estados Unidos como la Organización del Tratado del Atlántico Norte (OTAN) hayan decidido catalogar al ciberespacio como un escenario de guerra más[13].

Todo ello ha desembocado en un contexto novedoso que bien justifica un análisis pormenorizado. Sin embargo, dada la imposibilidad de abordar todas estas ciberamenazas en una contribución de esta naturaleza, se ha optado por una de ellas, el ciberterrorismo, debido al singular interés que presentan los caracteres adquiridos por el terrorismo internacional en el presente siglo —en buena medida consolidados gracias a internet, como buena cuenta se dará en las siguientes páginas—. Dado que interesa alcanzar una definición que pueda resultar válida desde la óptica del derecho internacional general, el estudio se centra, aunque no exclusivamente sí de forma prioritaria, en la práctica desarrollada en el ámbito universal; especialmente en el seno de la Organización de las Naciones Unidas (en adelante, ONU).

Cierto es que el tema objeto de estudio se presta a otros posibles tratamientos sumamente interesantes e importantes, pero, a la par, no es menos cierto que el problema de la definición es crucial, pues sin ella no hay respuestas comunes ni eficaces frente a las implicaciones de esta amenaza. Cuestiones tales como si un ciberataque terrorista puede constituir un uso de la fuerza prohibido por el derecho internacional; si tal ciberataque desencadenaría la operatividad de las obligaciones de cooperación internacional penal propias de la lucha contra el terrorismo; si los Estados podrían recurrir a la

[12] El Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN (CCD-CoE, por sus siglas en inglés) recoge más de 70 a nivel mundial (*vid.* <https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies>).

[13] Estados Unidos lo hizo en julio de 2011 en su *Department of Defense Strategy for Operating in Cyberspace* (*vid.* pp. 6 y ss. <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>). Por su parte, la OTAN, con el documento *Cyber Defence Pledge*, resultante de la cumbre de Varsovia de 8 y 9 de julio de 2016, reconoció la «aplicabilidad del derecho internacional en el ciberespacio» por ser otro dominio en el que «sus Estados son capaces de defenderse», junto al aire, la tierra, el mar y, desde finales de 2019, también el espacio (*vid.* <https://www.nato.int/cps/en/natohq/official_texts_133177.htm>).

legítima defensa ante el ciberterrorismo; o si la participación en actividades ciberterroristas puede ser causa de denegación de una solicitud de asilo dependen en definitiva de lo que entendamos por ciberterrorismo. Así pues, dado que el debate general sobre todas esas otras cuestiones sería más fructífero si se partiese de un concepto propio de ciberterrorismo, se opta por centrar los esfuerzos en delimitar tal concepto en la medida de lo posible.

II. LA BÚSQUEDA DE UNA DEFINICIÓN PARA EL TERRORISMO INTERNACIONAL

Desde hace prácticamente un siglo se ha intentado consensuar una definición de terrorismo internacional que quedase plasmada en un instrumento legal universal[14]. Hasta la fecha, el común denominador de esos intentos ha sido la incapacidad de cumplir con dicho objetivo[15]. Es por ello por lo que, dada la parálisis en esa vía, y para arrojar luz sobre esta cuestión, en los apartados que siguen se contemplarán asimismo algunas aproximaciones doctrinales y un importante pronunciamiento judicial del Tribunal Especial para el Líbano para arrojar luz sobre esta cuestión.

II.A. El concepto jurídico de terrorismo internacional en la sociedad internacional institucionalizada

Para definir un concepto es lugar común acudir a su etimología. Así, podría entenderse el terrorismo como «aquellos actos realizados con el propósito de causar terror»; concepción que engranaría perfectamente con sus orígenes durante «El Terror» de la Revolución Francesa en las postrimerías del siglo XVIII. Pero este proceder, un

[14] Para un recorrido histórico sobre los intentos fallidos *vid.* SAUL, B., "Attempts to Define Terrorism in International Law", *Netherlands International Law Review*, vol. 52, 2005, pp. 57-83.

[15] No obstante, hay quien llama la atención sobre el hecho de que el Convenio internacional para la represión de la financiación del terrorismo de 1999, universal en un triple sentido (fuente, materia y número de ratificaciones), sí contempla una suerte de definición en su art. 2, aun cuando esta sea por una técnica mixta, *vid.* JIMÉNEZ GARCÍA, A., "Derecho Internacional Penal y Terrorismo. Historia de una relación incapaz de materializarse estatutariamente", en SOROETA LICERAS, J. (Ed.), *Cursos de Derechos Humanos de Donostia-San Sebastián. Vol. VI: Conflictos y protección de derechos humanos en el orden internacional*, Servicio Editorial de la Universidad del País Vasco, Bilbao, 2006, p. 322. Sin embargo, otros autores restan importancia a la misma, como GUILLAUME, G., "Terrorism and International Law", *International and Comparative Law Quarterly*, vol. 53, nº 3, 2004, p. 539.

tanto «ockhamiano», conduce a una tautología que casa mal con el ordenamiento jurídico internacional, el cual no aspira sino a ser un conjunto coherente y perfecto de respuestas jurídicas frente a las cuestiones, necesidades y aspiraciones presentes en el orden internacional. Y esta es precisamente la postura que debe entenderse mantenida por la sociedad internacional institucionalizada, pues, con mayor o menor decisión, ha ahondado en la búsqueda de tal definición desde antaño.

II.A.1. El terrorismo internacional en los instrumentos universales

Los primeros intentos reseñables[16] para regular jurídicamente el terrorismo internacional se albergaron en el seno de la extinta Sociedad de Naciones[17] tras el magnicidio en 1934 de Alejandro I de Yugoslavia en suelo marsellés. Sus resultados se vieron plasmados tres años más tarde en dos convenciones: la Convención para la prevención y la represión del terrorismo y la Convención para la creación de un tribunal penal internacional que conociese de los delitos contemplados en el primero de esos instrumentos.

La lectura conjunta de los tres artículos iniciales de la primera de las convenciones[18] aportaba elementos suficientes para perfilar una definición. Recogía un concepto general de actos de terrorismo como «hechos criminales dirigidos contra un Estado cuyo fin o naturaleza es la de provocar el terror en personalidades determinadas, grupos de personas o entre el público en general», acompañado de un listado que los ordenamientos internos de los respectivos Estados debían considerar actos terroristas. No obstante, quedó en letra muerta, pues ninguna de estas convenciones entraron en vigor por carecer de las ratificaciones necesarias.

En décadas posteriores la fragmentación de la sociedad internacional impediría lograr el consenso necesario, resultando en vano intentos como el ensayado en 1954 por la Comisión de Derecho In-

---

[16] Para consultar otros anteriores en el tiempo, *vid.* RAMÓN CHORNET, C., *Terrorismo y respuesta de fuerza en el marco del Derecho Internacional*, 1ª edición, Tirant lo Blanch, Valencia, pp. 42-50 y 110-123.

[17] GUILLAUME, G., "Terrorism and (…)", *op. cit.*, p. 538. Sobre lo acontecido en la Sociedad de Naciones, *vid.* SÁNCHEZ FRÍAS, A., "La propuesta de un Tribunal Internacional contra el terrorismo: retos jurídicos y políticos", *Revista de Derecho Político*, nº 103, 2018, pp. 412-416.

[18] Convención para la prevención y la represión del terrorismo, de 16 de noviembre de 1937, de la Sociedad de Naciones. Disponible en <https://dl.wdl.org/11579/service/11579.pdf>.

ternacional (CDI)[19]. Hubo que esperar a los años setenta para que el terrorismo internacional fuese objeto de especial seguimiento dentro de la ONU[20], como prueba la creación de un comité *ad hoc* por la Resolución 3034 (XXVII) de la Asamblea General de las Naciones Unidas (en adelante, AGNU), primera adoptada exprofeso sobre el terrorismo internacional. El «Comité de los 35» prolongó sus sesiones entre 1972 y 1979 y dividió su labor en tres subcomités para trabajar sobre la definición, las causas subyacentes y las medidas de prevención del terrorismo internacional. Sus reuniones, consideradas útiles ya que facilitaron cierto consenso en el tratamiento del problema del terrorismo internacional en la AGNU, permitieron esclarecer el papel del derecho internacional en relación con esta amenaza[21]. Con todo, el terreno de la definición continuó yermo.

No es de extrañar que durante ese periodo, en un contexto de proliferación de actos de terrorismo internacional[22] y de desacuerdo a la hora de alcanzar una definición convencional, los Estados abordaran el terrorismo desde una perspectiva particular mediante convenios que contemplasen aspectos específicos[23]. De esto pueden derivarse tres consecuencias: (i) la paulatina construcción de un marco jurídico convencional sustentado en la adopción de diecinueve instrumentos universales de naturaleza sectorial en materia de lucha antiterrorista regidos por el principio *aut dedere aut judicare*[24]; (ii) la

[19] El art. 2.6 del proyecto de Código de crímenes contra la paz y la seguridad de la humanidad aludía a «actos terroristas» y «actividades terroristas». *Vid.* SAUL, B., "Attempts to (…)", *op. cit.*, pp. 66-68.

[20] RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, pp. 120-121, considera que esta etapa comienza con las Resoluciones AGNU 2625 (XXV), de 24 de octubre de 1970, y 2734 (XXV), de 16 de diciembre de 1970.

[21] ALCAIDE FERNÁNDEZ, J., "Terrorismo y Derecho Internacional. Desarrollos normativos e institucionales tras el 11-S", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, nº 1, 2017, pp. 41-42.

[22] De hecho, la toma de rehenes en Entebbe (Uganda) en 1976 y el secuestro del buque de pabellón italiano *Achille Lauro* en 1985 se encuentran, respectivamente, en la génesis de la Convención internacional contra la toma de rehenes (1979) y de la Convención internacional para la represión de actos ilícitos contra la seguridad de la navegación marítima (1988), ambas de la ONU. *Vid.* SALINAS DE FRÍAS, A., "La práctica convencional multilateral de los Estados en materia de cooperación judicial internacional contra el terrorismo", *Anuario Argentino de Derecho Internacional*, XV, 2006, esp. pp. 74 y ss.

[23] BERMEJO GARCÍA, R., "Las denominadas nuevas tendencias en la lucha contra el terrorismo internacional: el caso del Estado Islámico", *Anuario Español de Derecho Internacional*, vol. 33, 2017, p. 11.

[24] Según este principio, el Estado de detención de los presuntos autores de un acto terrorista puede optar por juzgarlos él mismo o por extraditarlos a otro Estado que los reclame por tales actos. Los 19 instrumentos adoptados por la ONU y algunos de sus organismos especializados —Organización de Aviación Civil Internacional, Organización Marítima Internacional y Organismo Internacional de Energía

posposición de la búsqueda de una definición universal, ausente en dichos instrumentos, así como en las referencias que el derecho internacional humanitario dedica a la proscripción del terrorismo en el curso de los conflictos armados en los Convenios de Ginebra de 1949 y en los dos Protocolos adicionales de 1977; y (iii) el trasvase de los esfuerzos convencionales al ámbito regional para completar los instrumentos frente a esta amenaza[25].

Atómica— están disponibles en <https://www.un.org/counterterrorism/international-legal-instruments>.

[25] Sin considerar a la Unión Europea, cabe mencionar: Convención de la Organización de los Estados Americanos (OEA) para la prevención y represión de los actos de terrorismo configurados como delitos contra las personas y actos conexos de extorsión de alcance internacional de 1971; Convenio Europeo para la represión del terrorismo de 1977, tal que enmendado por su Protocolo de 2003; Convención regional de la Asociación del Asia Meridional para la Cooperación Regional (SAARC) sobre la eliminación del terrorismo de 1987 y su Protocolo adicional de 2004; Convención de la Liga Árabe sobre la represión del terrorismo de 1998 y su Enmienda de 2008; Tratado de cooperación entre los Estados miembros de la Comunidad de Estados Independientes (CEI) para combatir el terrorismo de 1999; Convención de la Organización para la Cooperación Islámica (OCI) sobre la lucha contra el terrorismo internacional de 1999; Convención de la Organización de la Unidad Africana (OUA) sobre la prevención y lucha contra el terrorismo de 1999 y su Protocolo de 2004; Convención de la Organización de Cooperación de Shanghái (OCS) para la lucha contra el terrorismo, el separatismo y el extremismo de 2001; Protocolo por el que se aprueba la ley de procedimiento para organizar y aplicar medidas conjuntas de lucha contra el terrorismo en el territorio de los Estados miembros de la Comunidad de Estados Independientes (CEI) de 2002; Convención Interamericana de la Organización de Estados Americano (OEA) contra el Terrorismo de 2002; Protocolo Adicional al Acuerdo entre los gobiernos de los Estados miembros de la Organización de Cooperación Económica del Mar Negro (OCEMN) sobre cooperación en la lucha contra la delincuencia, en particular la delincuencia organizada, relativo a la lucha contra el terrorismo de 2004; Convención de la Comunidad Económica y Monetaria del África Central (CEMAC) sobre la lucha contra el terrorismo en África Central de 2004; Convenio del Consejo de Europa para la prevención del terrorismo de 2005 y su Protocolo Adicional de 2015; Convenio del Consejo de Europa sobre el blanqueo, la investigación, la incautación y el decomiso del producto del delito y sobre la financiación del terrorismo de 2005; Convención de la Asociación de Naciones del Sudeste Asiático (ASEAN) sobre la lucha contra el terrorismo de 2007; Tratado de los Estados miembros de la Comunidad de Estados Independientes (CEI) sobre la lucha contra la legalización (blanqueo) del producto del delito y la financiación del terrorismo de 2007; Convención de la Organización de Cooperación de Shanghái (OCS) de la lucha contra el terrorismo de 2009; Convención de la Liga Árabe contra el blanqueo de capitales y la financiación del terrorismo de 2010; y Convención de la Organización de Cooperación de Shanghái (OCS) de la lucha contra el extremismo de 2017. El Informe del Secretario General de las Naciones Unidas sobre medidas para eliminar el terrorismo internacional correspondiente al septuagésimo cuarto periodo de sesiones recoge un total de 35 (A/74/151).

Ya en el último cuarto del siglo pasado[26] la ONU redobló esfuerzos y se propuso abanderar la canalización de la lucha multilateral contra el terrorismo internacional. La AGNU, nutrida de la acción de los organismos especializados, de las resoluciones del Consejo de Seguridad de las Naciones Unidas (en adelante, CSNU) y de las aportaciones realizadas por otras organizaciones universales y regionales, creó el conocido como «Comité 51/210», encargado de trabajar en nuevos instrumentos contra el terrorismo. Su éxito se traduce en los tres convenios tras cuya adopción se encuentra[27], si bien no ha logrado que fructifiquen las negociaciones iniciadas hace dos décadas para lograr un proyecto de Convenio general sobre el terrorismo internacional[28].

Pese a encontrarse en punto muerto, este nonato convenio es de interés por cuanto demuestra los puntos de entendimiento y disensión para con esta cuestión. A tal respecto, considera que cometería delito en el sentido de dicho instrumento quien amenace verosímil y seriamente con causar o cause ilícita e intencionalmente y por cualquier medio: (i) la muerte o lesiones corporales graves a cualquier persona; o (ii) daños graves u otros daños que produzcan o puedan producir un gran perjuicio económico a bienes públicos o privados, incluidos un lugar de uso público, una instalación pública o gubernamental, una red de transporte público, instalaciones de una infraestructura o el medio ambiente; y (iii) siempre que el propósito de tal acto, por su naturaleza o por su contexto, sea «intimidar a la población u obligar a un gobierno o a una organización internacional a realizar o abstenerse de realizar un determinado acto»[29].

De resultas, puede concluirse que desde 1963[30] se ha construido un marco jurídico universal contra el terrorismo que recoge todos

[26] Sobre ese periodo y la definición de terrorismo, *vid.* SAUL, B., "Attempts to (…)", *op. cit.*, pp. 68-82.

[27] Convenio internacional para la represión de los atentados terroristas cometidos con bombas, de 15 de diciembre de 1997; Convenio internacional para la represión de la financiación del terrorismo, de 9 de diciembre de 1999; y Convenio internacional para la represión de los actos de terrorismo nuclear, de 13 de abril de 2005.

[28] No parece que dicho Convenio se vaya a adoptar pronto, pues el Comité 51/210 no se reúne desde 2013 y el asunto solo se trata en el grupo de trabajo de la Sexta Comisión. Tampoco se ha convocado aún la conferencia de alto nivel bajo los auspicios de las ONU «a fin de formular una respuesta organizada conjunta de la comunidad internacional al terrorismo en todas sus formas y manifestaciones» (*vid.* A/RES/54/110).

[29] Así se recoge en el art. 2 del borrador presentado por el último informe accesible del Comité 51/210 relativo al decimosexto periodo de sesiones de este Comité especial celebrado entre el 8 y el 12 de abril de 2013 (A/68/37).

[30] Cuando se adoptó el Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de aeronaves, de 14 de septiembre de dicho año.

los instrumentos jurídicamente vinculantes adoptados a nivel mundial para que los Estados prevengan y, en su caso, combatan el terrorismo internacional. Este marco consiste en un enfoque sectorial articulado mediante una técnica enumerativa de manifestaciones terroristas que no ofrece en los instrumentos que lo conforman definición explícita alguna de terrorismo internacional, lo que puede entenderse paradójico, pues pretende afrontarlo sin delimitarlo[31]. Pero tal consideración no lleva necesariamente a concluir que esta arquitectura deba entenderse totalmente fallida[32], pues el transcurso del tiempo demuestra que «aunque no haya un concepto único, ni un tratado general, se avanza hacia una aplicación armónica de la red convencional»[33].

II.A.2. La práctica del Consejo de Seguridad de las Naciones Unidas

El tratamiento del terrorismo internacional por parte de la ONU no se ha limitado a la pujanza anterior. También constituyen un aspecto fundamental de ese marco jurídico las resoluciones del CSNU, especialmente las jurídicamente vinculantes aprobadas en virtud del Capítulo VII de la Carta de las Naciones Unidas (en adelante, Carta NU).

Fue en 1992, a raíz del caso *Lockerbie*, cuando el CSNU consideró por primera vez que los actos de terrorismo internacional constituyen una amenaza para la paz y la seguridad internacionales[34]. Después procedería a condenar inequívocamente tales actos sin necesidad de esperar a un concreto ataque[35]. Sin embargo, es a partir de los atentados del 11 de septiembre de 2001 (en adelante, 11-S), cuando el CSNU ha afrontado el terrorismo mediante una actuación «sistemática»[36], caracterizada por un tono más grave[37] y por la adop-

---

[31] GUILLAUME, G., "Terrorism and (…)", *op. cit.*, pp. 539.

[32] ALCAIDE FERNÁNDEZ, J., *Las actividades terroristas ante el Derecho Internacional contemporáneo*, 1ª edición, Tecnos, Madrid, 2000, pp. 27-78. No obstante, hay quien se cuestiona cuán satisfactoria es esta aproximación sectorial, *vid.* SAUL, B. Y HEATH, K., "Cyber terrorism", en TSAGOURIAS, N. y BUCHAN, R. (Eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, Cheltenham, 2017, p. 152.

[33] FERNÁNDEZ TOMÁS, A. F., "Terrorismo, Derecho Internacional Público, y Derecho de la Unión Europea", *Actas de los Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, 2004, p. 9.

[34] *Vid.* S/RES/731 (1992).

[35] *Vid.* S/RES/1269 (1999).

[36] SALINAS DE FRÍAS, A., "Lucha contra el terrorismo internacional: no solo del uso de la fuerza pueden vivir los Estados", *Revista Española de Derecho Internacional*, vol. 69, nº 2, 2016, pp. 234-235.

[37] BERMEJO GARCÍA, R., "Las denominadas (…)", *op. cit.*, p. 15.

ción de determinadas resoluciones que establecen «obligaciones generales y permanentes, sin relación con un asunto concreto»[38], en lo que sería una muestra de la redefinición de su papel y funciones para encarar algunos de los desafíos de la seguridad internacional[39].

Efectivamente, el 11-S motivó la adopción de las célebres Resoluciones del CSNU 1368 (2001) y 1373 (2001). La primera fue tildada de «ambigua y contradictoria»[40], ya que alude a la legítima defensa en el preámbulo y, a la par, en la parte dispositiva, califica esos ataques como una amenaza para la paz[41] y no como un ataque armado, cuando este es el resorte de la legítima defensa *ex* art. 51 Carta NU. La segunda, que asimismo establece un Comité contra el Terrorismo, también fue objeto de duras críticas. En ella, el CSNU se arroga potestades legislativas pues «actuando en virtud el Capítulo VII de la Carta *decide* […]» —empleando así un término que muestra una señal inequívoca de la obligación jurídicamente vinculante de adoptar tales medidas[42]— imponer a «todos los Estados» una parte del contenido del Convenio internacional para la represión de la financiación del terrorismo, supliendo de esta manera la voluntad soberana de los Estados[43].

Volviendo a la cuestión de la definición, que es la que nos ocupa, es obligatorio detenerse en la Resolución 1566 (2004), que colma el vacío de la Resolución 1373 (2001) en la que el CSNU evitó deliberadamente pronunciarse sobre la definición del terrorismo internacional[44]. Aprobada tras la matanza de Beslán (Rusia), en ella se insta a

---

[38] HINOJOSA MARTÍNEZ, L. M., "The Legislative Role of the Security Council in its Fight Against Terrorism: Legal, Political and Practical", *International and Comparative Law Quarterly*, vol. 57, nº 2, 2008, p. 342.

[39] *Ibid.*, p. 344.

[40] CASSESE, A., "Terrorism is Also Disrupting Some Crucial Legal Categories of International Law", *European Journal of International Law*, vol. 12, nº 5, 2001, p. 996.

[41] Dado que la calificación empleada fue la de «amenaza a la paz» se ha criticado que se evitase deliberadamente recurrir a las medidas sancionadoras que procedían, esto es, las de los arts. 41 y 42 Carta NU. *Vid.* FERNÁNDEZ TOMÁS, A. F., "Terrorismo, (…)", *op. cit.*, pp. 19-21.

[42] SÁNCHEZ FRÍAS, A., *La obligación de cooperar en la lucha contra el terrorismo: ¿hacia una nueva norma de Derecho internacional consuetudinario?* (Tesis), Universidad de Málaga, Málaga, 2019, p. 253. Con la Resolución 1373 (2001) se inaugura una línea cuya continuidad predica la Resolución 1540 (2004), que establece de nuevo obligaciones jurídicamente vinculantes para los Estados, en este caso, en relación con el acceso de grupos terroristas a armas nucleares, químicas o biológicas, y la Resolución 2178 (2014), relativa a los combatientes terroristas extranjeros.

[43] ALCAIDE FERNÁNDEZ, J., "La «guerra contra el terrorismo»: ¿una «OPA hostil» al Derecho de la comunidad internacional?", *Revista Española de Derecho Internacional*, vol. 53, nº 1 y 2, 2001, pp. 296-297.

[44] Se ha apuntado que la razón fue la voluntad de adoptar una resolución rápida y sin disensos, *vid.* ROSAND, E., "Security Council Resolution 1373, the Coun-

todos los Estados a prevenir una serie de actos de terrorismo y, en caso de que acontezcan, a cerciorarse de que sean sancionados con penas compatibles con su naturaleza. Para ello tuvo a bien presentar unos parámetros definitorios del terrorismo como «actos criminales, inclusive contra civiles[45], cometidos con la intención de causar la muerte o lesiones corporales graves o de tomar rehenes» cuando su propósito sea el de «provocar un estado de terror en la población en general, en un grupo de personas o en determinada persona, intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto, o a abstenerse de realizarlo».

A efectos de nuestro objeto de estudio, más allá de los impulsos a la cooperación contra el terrorismo internacional a golpe de resolución —no muy decididos, excepto en lo relativo a la financiación del terrorismo y a la persecución y enjuiciamiento de los combatientes terroristas extranjeros[46]—, lo importante es advertir que de esta práctica se extrapolan dos elementos definidores[47]. Por un lado, un elemento objetivo: la realización de una conducta criminal, grave y planificada consistente en el empleo de la violencia, en especial contra la población civil. Y por el otro, uno subjetivo: la finalidad de crear un estado de terror o intimidación en la población o en alguno de sus sectores para obligar a un gobierno o a una OI a hacer algo o a abstenerse de hacerlo.

II.B. Algunas propuestas doctrinales

Tradicionalmente, los impedimentos para lograr una definición jurídica sin ambigüedades y universalmente aceptada del terrorismo internacional han reposado en dos aristas: (i) las dificultades técnicas dada la tautología existente en el binomio terrorismo-terror, pues para definir al primero parece imprescindible referirse al segundo; y (ii) las tensiones políticas que planteaba la lucha de los movimientos de liberación nacional y determinadas actuaciones iden-

---

ter-Terrorism Committee, and the Fight against Terrorism", *The American Journal of International Law*, vol. 97, nº 2, 2003, p. 334, nota 7. Si ese fue realmente el motivo, este debe entenderse cumplido satisfactoriamente ya que se aprobó por unanimidad y en cinco minutos, *vid.* REMIRO BROTÓNS, A., "Terrorismo, mantenimiento de la paz y nuevo orden", *Revista Española de Derecho Internacional*, vol. 53, nº 1 y 2, 2001, esp. pp. 161-163.

[45] JIMÉNEZ GARCÍA, A., "Derecho Internacional (…)", *op. cit.*, p. 329, nota 67, apunta que es más precisa la versión en francés porque habla de actos «particularmente dirigidos contra civiles».

[46] SÁNCHEZ FRÍAS, A., *La obligación (…)*, *op. cit.*, pp. 237-280.

[47] JIMÉNEZ GARCÍA, A., "Derecho Internacional (…)", *op. cit.*, p. 331.

tificadas con el llamado «terrorismo de Estado». En realidad, como señala SOREL, lo que subyace a las continuas disensiones, guarda relación con las causas, las motivaciones y la legitimación del «hecho terrorista»[48]. Ciertamente, algunos Estados son renuentes a vincularse a una definición universal que reemplace sus propios criterios acerca de lo que ha de entenderse por terrorismo y cómo debe combatirse[49]; y más aún cuando, prospectivamente, tal definición pudiera no responder a sus intereses.

Lo anterior podría hacer que nos cuestionásemos, como hicieran CARRILLO SALCEDO y FROWEIN, si no se persigue un imposible, ya que la consecución de esa definición globalmente aceptada, lejos de acercarse, parece alejarse conforme se indaga en su búsqueda fruto de las continuas discrepancias[50]. Incluso hay quien va más allá y considera que «terrorismo» es un término carente de cualquier significado jurídico concreto y que, en todo caso, se trataría de un vocablo que resultaría útil para referirse a algunas actuaciones estatales o individuales ampliamente prohibidas porque los métodos utilizados son contrarios a derecho, porque los objetivos contra los que se dirigen están protegidos, o bien porque concurren ambos supuestos[51].

Sin embargo, también hay quien otorga valor al concepto normativo de terrorismo internacional, tanto por ser el articulador de las obligaciones internacionales en esta materia como por el relativo éxito resultante de la aproximación sectorial[52]. Además, existen otros motivos que justificarían los esfuerzos dedicados a intentar delimitar este concepto dado que: (i) la cooperación interestatal necesaria para combatirlo se ve mermada en ausencia de una definición común[53]; (ii) en los más negros escenarios la ausencia de tal definición

[48] SOREL, J.-M., "Some Questions About the Definition of Terrorism and the Fight Against Its Financing", *European Journal of International Law*, vol. 14, nº 2, 2003, p. 368.

[49] FIDLER, D. P., "Cyberspace, Terrorism and International Law", *Journal of Conflict & Security Law*, vol. 21, nº 3, 2016, p. 477.

[50] CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects juridiques du terrorisme international/The Legal Aspects of International Terrorism*, Académie de droit international de La Haye. Centre d'étude et de recherche de droit international et de relations internationales, Martinus Nijhoff Publishers, Dordrecht, 1989, pp. 19-20.

[51] HIGGINS, R., "The General International Law of Terrorism", en HIGGINS, R. y FLORY, M. (Eds.), *Terrorism and International Law*, Routledge, London, 1997, pp. 27-28.

[52] ALCAIDE FERNÁNDEZ, J., *Las actividades (…)*, *op. cit.*, pp. 43-44.

[53] CASSESE, A., "The Multifaceted Criminal Notion of Terrorism in International Law", *Journal of International Criminal Justice*, vol. 4, nº 5, 2006, p. 934.

puede facilitar una *lex talionis*[54] capaz de comprometer tanto al derecho internacional humanitario como al derecho internacional de los derechos humanos[55]; y (iii) resulta de suma importancia para dar cumplimiento al principio de legalidad penal en el derecho internacional penal[56].

Por ello es necesario conocer cuál es el denominador común que sustenta ese marco jurídico antiterrorista que los Estados consienten en abrazar, así como qué realidades son las significadas con la expresión «terrorismo internacional»[57]. Asumida por el momento la imposibilidad de resolver estas cuestiones acudiendo a la definición proporcionada por algún instrumento internacional universal, se sintetizan a continuación algunas propuestas académicas para acercarnos a los elementos integrantes que esta noción guarda tras de sí.

El terrorismo internacional puede concebirse como un acto ilícito —«criminal» siguiendo a algunos autores[58]— consistente en el uso o amenaza de uso de una violencia grave e indiscriminada[59] contra la vida o la integridad de las personas[60], contemplándose asimismo que pueda dirigirse contra propiedades públicas o privadas[61]. Es pacífico entre la doctrina entender que no se trata de una «violencia por la violencia», sino que la misma es instrumentalizada para generar un clima de pánico o de terror en la sociedad[62]

---

[54] SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 370.

[55] Que la llamada «guerra contra el terrorismo» se presta a situaciones de este tipo puede verse en SÁNCHEZ LEGIDO, Á., "«Guerra contra el terrorismo», conflictos armados y derechos humanos", en SOROETA LICERAS, J. (Ed.), *Cursos de Derechos Humanos de Donostia-San Sebastián. Vol. VI: Conflictos y protección de derechos humanos en el orden internacional*, Servicio Editorial de la Universidad del País Vasco, Bilbao, 2006, pp. 413-470.

[56] JIMÉNEZ GARCÍA, A., "Derecho Internacional (…)", *op. cit.*, p. 310.

[57] ALCAIDE FERNÁNDEZ, J., *Las actividades (…)*, *op. cit.*, p. 43.

[58] GOL, J., "Coordination européenne de la prévention du terrorisme", *Studia Diplomatica*, vol. 41, nº 1, 1988, p. 5; CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op. cit.*, pp. 21 y 57.

[59] GOL, J., "Coordination (…)", *op. cit.*, pp. 4-6; CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op. cit.*, pp. 21 y 57; SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 371. Hay quien además exige que la violencia sea planificada, *vid.* GUILLAUME, G., "Terrorism and (…)", *op. cit.*, p. 540.

[60] CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op. cit.*, pp. 21 y 57; SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 371; GUILLAUME, G., "Terrorism and (…)", *op. cit.*, p. 540.

[61] SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 371. Aunque sin afirmarlo expresamente, parece no descartarse esta posibilidad por GUILLAUME, G., "Terrorism and (…)", *op. cit.*, p. 540.

[62] GLASER, S., "Le terrorisme international et ses divers aspects", *Revue internationale de droit comparé*, vol. 25, nº 4, 1973, p. 826; GOL, J., "Coordination (…)", *op. cit.*, pp. 5-6; CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op.*

—ya sea en individuos, en grupos o en comunidades enteras— con el propósito de lograr posteriormente un determinado objetivo. En este sentido, se ha apuntado que el terror es una forma «extranormal de violencia»[63] que genera una reacción a nivel social, en tanto que miedo o ansiedad fruto de la violencia indiscriminada y/o dirigida contra inocentes, que es palpablemente superior a los daños físicos o materiales acaecidos[64]. El objetivo último de ese clima de terror es influir en la agenda política[65] de un Estado o de una OI, lo que generalmente implicaría hacer concesiones favorables a los intereses de los terroristas[66].

Respecto a la nota de internacionalidad, es decir, «las condiciones en que cabe hablar del terrorismo como fenómeno internacional»[67], se ha señalado que el terrorismo es internacional cuando se atenta contra el orden social internacional, y más específicamente contra la paz o la seguridad de la humanidad[68]. Otros autores apuntan que el elemento internacional se refiere a que, por un motivo u otro, el acto o la actividad terrorista trasciende las fronteras de un Estado[69], lo que puede ocurrir porque el acto se planifique o cometa a través de una frontera internacional, porque los objetivos sean nacionales extranjeros, porque los autores se refugien en otro país o porque la conducta en cuestión caiga bajo alguna de las categorías reguladas en los tratados[70]. En cambio, a esta concepción se le ha puntualizado que traspasar fronteras nacionales es sinónimo de transnacionalidad, pero no garantía de internacionalidad, ya que esta solo tiene lugar cuando se pretende subvertir el *statu quo* regional o mundial, lo que requiere que los actores terroristas, individua-

cit., p. 21; RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, p. 72; SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 371; GUILLAUME, G., "Terrorism and (…)", *op. cit.*, pp. 540-541.

[63] RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, esp. pp. 70-72 y 80-81, indica que esta «extranormalidad» en los actos terroristas se hace patente en una ausencia de límites que se manifiesta en la no discriminación o arbitrariedad de tales acciones y en su imprevisibilidad.

[64] REINARES NESTARES, F., "¿A qué llamamos terrorismo internacional?", en MARTÍNEZ DE PISÓN CAVERO, J. Mª. y URREA CORRES, M. (Coords.), *Seguridad internacional y guerra preventiva: análisis de los nuevos discursos sobre la guerra*, Perla Ediciones, Logroño, 2008, p. 90.

[65] SOREL, J.-M., "Some Questions (…)", *op. cit.*, p. 371.

[66] CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op. cit.*, pp. 21 y 57; y GUILLAUME, G., "Terrorism and (…)", *op. cit.*, p. 541.

[67] RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, p. 131, nota 203. El elemento internacional es profundamente analizado en las pp. 131 y ss.

[68] GLASER, S., "Le terrorisme (…)", *op. cit.*, p. 826.

[69] ALCAIDE FERNÁNDEZ, J., *Las actividades (…)*, *op. cit.*, p. 53.

[70] CARRILLO SALCEDO, J. A. y FROWEIN, J. A., *Les aspects (…)*, *op. cit.*, pp. 21 y 57.

les y colectivos, extiendan sus actividades por un número relevante de países o áreas geopolíticas[71].

En paralelo se encuentra la interpretación de quienes, como hiciera CASSESE, defienden la existencia de una norma de derecho consuetudinario respecto a los elementos objetivos y subjetivos del terrorismo internacional en tiempos de paz[72]. Para con el elemento objetivo[73], tal definición contempla: (i) una conducta normalmente prevista y castigada por los ordenamientos penales nacionales; (ii) transnacional por naturaleza, es decir, no limitada al territorio de un único Estado en cuanto a sus acciones o implicaciones; y (iii) cuyas víctimas sean la población en general, civiles concretos o personalidades públicas. En cuanto al elemento subjetivo[74], la finalidad principal y esencial es siempre ejercer coerción sobre una autoridad pública —esto es, un gobierno o una OI— o una institución privada transnacional —por ejemplo, una empresa multinacional— para que realice o se abstenga de realizar una determinada acción o política. Dicho elemento subjetivo requiere: (i) un *dolus generalis* correspondiente a la voluntad que subyace al delito cometido —por ejemplo, un asesinato o un secuestro—; y (ii) un *dolus specialis* consistente en forzar a una autoridad relevante, pública o privada, a que haga o deje de hacer algo. Finalmente, esta conducta no debe estar guiada por un interés privado, sino por una motivación política, ideológica o religiosa[75].

II.C. La noción utilizada por el Tribunal Especial para el Líbano

En este espectro de propuestas conceptuales sobresale el pronunciamiento del Tribunal Especial para el Líbano (en adelante, TEL) establecido por el CSNU mediante la Resolución 1757 (2007). Haciéndose eco de las divergencias existentes, la Sala de Apelaciones del TEL[76] hizo suya la postura del propio CASSESE, quien lo presidía.

---

[71] REINARES NESTARES, F., "¿A qué (…)", *op. cit.*, p. 92.
[72] CASSESE, A., "The Multifaceted (…)", *op. cit.*, pp. 935 y ss.
[73] *Ibid.*, p. 938
[74] *Ibid.*, pp. 939 y 940.
[75] *Ibid.*
[76] Special Tribunal for Lebanon (STL), *The Prosecutor v. Ayyash et al.*, Appeals Chamber, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case No. STL-11-01/I, 16 February 2011. *Vid.* esp. § 83-113. Disponible en <https://www.stl-tsl.org/sites/default/files/documents/legal-documents/stl-casebooks/STL_Casebook_201_EN.pdf>.

Afirmó la existencia de una norma de derecho consuetudinario en la comunidad internacional, al menos en tiempo de paz, con respecto al crimen internacional de terrorismo que resultaría avalada por una práctica internacional sobre la materia plasmada en los tratados, las resoluciones de la ONU y en la práctica legislativa y jurisprudencial de los Estados, evidenciando todo ello la formación de una *opinio iuris* general[77].

El delito de terrorismo internacional se integraría por[78]: (i) la comisión o amenaza de comisión de un acto criminal, entre otros, el asesinato, el secuestro, la toma de rehenes o los incendios provocados; (ii) el propósito de difundir el miedo entre la población o de ejercer coerción directa o indirecta sobre una autoridad nacional o internacional para que realice una acción o se abstenga de realizarla; y (iii) la presencia de un elemento transnacional, lo que comúnmente será consecuencia de una conexión entre dos o más países por medio de las víctimas, los autores o los medios empleados, o porque sea previsible que un ataque terrorista planeado y cometido en un territorio suponga, al menos para los países limítrofes, una amenaza para la paz y la seguridad internacionales[79].

Pese a la controversia suscitada[80] este pronunciamiento de la Sala de Apelaciones del TEL posee la virtud de realizar un esfuerzo compilador de las nociones de terrorismo existentes a distintos niveles —universal, regional y nacional— sobre las que sustenta la presentada en su decisión, lo que permite advertir los puntos de entendimiento sobre una parte del contenido de la varias veces pospuesta definición universal sobre el terrorismo internacional. Así, puede apreciarse cierto consenso sobre el elemento subjetivo e intencio-

[77] *Ibid.*, § 85.
[78] *Ibid.*
[79] *Ibid.*, § 90.
[80] *Vid.* AMBOS, K., "Creatividad judicial en el Tribunal Especial para el Líbano: ¿es el terrorismo un crimen internacional?", *Revista de Derecho Penal y Criminología*, 3ª época, nº 7, 2012, pp. 143-173.

nal (*mens rea*) a nivel universal[81] y regional[82]; tanto en la intención especial «general» —es decir, la finalidad de atemorizar o amedrentar a la población o a sectores de esta— como en la intención especial «especial»[83] —esto es, el propósito de coaccionar a un Estado o a una OI para que realice una concreta acción o abstención—. Por oposición, parece más dudoso que exista tal concordancia de criterios en cuanto a los elementos objetivos (*actus reus*), dado que en estos no se aprecia un nivel de precisión similar, lo que pondría de relieve «la falta de consenso de la comunidad internacional en

[81] Cfr. art. 2.1 del proyecto de Convenio general sobre terrorismo internacional de la ONU (*vid. supra* p. 708, nota 29) y la definición dada por el CSNU en la S/RES/1566 (2004) (*vid. supra* p. 711). De igual modo, la AGNU en sus resoluciones sobre terrorismo alude a que «los actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general, en un grupo de personas o en determinadas personas son injustificables cualesquiera que sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquiera otra índole que se hagan valer para justificarlos» (entre otras, A/RES/49/60; A/RES/54/110; A/RES/71/151; A/RES/73/221). Asimismo, el art. 2.1.b) del Convenio internacional para la represión de la financiación del terrorismo de 1999 recoge en su «protodefinición» el mismo *dolus specialis* que el identificado por el TEL, considerando que comete delito en el sentido de dicho convenio quien financie en los términos del art. 2.1 «cualquier otro acto destinado a causar la muerte o lesiones corporales graves a un civil o cualquier otra persona que no participe directamente en las hostilidades en una situación de conflicto armado, cuando, el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o abstenerse de hacerlo».

[82] Por ejemplo, la Convención de la Liga Árabe sobre la represión del terrorismo de 1998 en su art. 1.2 recoge: «por "terrorismo" se entenderá todo acto de violencia o de amenaza del uso de la violencia […] que tenga por objeto sembrar el pánico entre la población, amenazarla con causarle daños o poner en peligro su vida, su libertad o su seguridad […]». Similar definición es la contemplada en el art. 1.2 del Convenio de la Organización para la Cooperación Islámica sobre la lucha contra el terrorismo internacional de 1999: «por "terrorismo" se entenderá cualquier acto o amenaza de violencia […] con el fin de ejecutar un plan delictivo individual o colectivo para aterrorizar a las personas o amenazar con hacerles daño o poner en peligro su vida, honor, libertad seguridad o derechos […]». Por su parte, la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo relativa a la lucha contra el terrorismo califica como delitos de terrorismo los actos intencionados enumerados en el art. 3.1 cuando se cometan con el fin de «intimidar gravemente a una población; obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo; desestabilizar gravemente o destruir las estructuras políticas, constitucionales, económicas o sociales fundamentales de un país o de una organización internacional».

[83] La terminología está tomada de AMBOS, K., "Creatividad judicial (…)", *op. cit.*, p. 171.

cuanto a los detalles de la definición de un crimen internacional de terrorismo»[84].

II.D. Una propuesta sintética

No obstante, sintetizando las ideas previas, puede considerarse que sí existen elementos suficientes para ofrecer una definición de terrorismo internacional de cara a ser utilizada posteriormente en nuestro intento de conceptualizar el ciberterrorismo. De este modo, el terrorismo internacional podría definirse como «(i) la comisión o amenaza de comisión de un acto criminal capaz de afectar al orden internacional por su gravedad[85]; (ii) dirigido contra la vida o la integridad de las personas o contra bienes, instalaciones o propiedades públicas o privadas; (iii) cuando el propósito de tal acto sea diseminar el miedo entre la población o sectores concretos de esta, o coaccionar directa o indirectamente a un gobierno o a una OI para que realice o se abstenga de realizar una acción concreta».

En cualquier caso, la plasmación convencional de propuestas de esta índole se atisba prácticamente imposible mientras que no se depuren completamente las diferencias existentes en la sociedad internacional, pues si algo está claro en la mesa de negociaciones del terrorismo internacional es que «nada queda acordado hasta que todo esté acordado»[86].

III. DEFINIENDO EL CIBERTERRORISMO

Dedicar las páginas precedentes a un tema tan manido como el concepto de terrorismo internacional se justifica precisamente por la ausencia de tal concepto. Pero, sobre todo, por el interés que presenta sintetizar algunas de las nociones existentes para así gozar de

[84] *Ibid.*, p. 173.

[85] Un parámetro para poder concretar dicha gravedad sería atender al nivel de violencia o de fuerza que requiere su comisión y no al medio que se utilice. RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, p. 63 señala en el sentido de lo que acaba de decirse «que lo que permite hablar de terrorismo no es que el tipo de instrumento utilizado para sembrar el terror se encuentre dentro de un catálogo determinado, ya que éstos pueden ser casi innumerables (asesinato, chantaje, secuestro, sabotaje, etc) con tal de que presenten como característica común el uso de la fuerza o de la violencia».

[86] Lema usado en las negociaciones del proyecto de Convenio general sobre terrorismo internacional. *Vid.* informe del Coordinador de las consultas oficiosas de tal proyecto adjunto a la carta de fecha 3 de agosto de 2005 dirigida al Presidente de la AGNU por el Presidente de la Sexta Comisión (A/59/894).

cierta seguridad de cara a la definición del ciberterrorismo que se persigue y de la que nos ocupamos de ahora en adelante.

III.A. Aproximación contextual

La idea según la cual la magnitud de la barbarie del 11-S supuso un punto de inflexión en la manera de afrontar la lacra del terrorismo internacional por parte de los Estados y las OI es ampliamente compartida[87]. Pero lo cierto es que también marcó un antes y un después para los propios terroristas —en especial para Al-Qaeda, los Talibanes y sus afiliados—, quienes vieron retornar el bumerán virulentamente lanzado. Con una sociedad internacional imbuida por convicción o por inercia en la lucha antiterrorista, el progresivo cercamiento que sufrían estos actores no estatales les obligó a reinventarse.

III.A.1. Los perfiles del terrorismo internacional tras el 11-S: breves apuntes

La mutación experimentada se proyecta al menos en cuatro características propias de la configuración actual del terrorismo internacional: (i) el incremento del uso de internet y, por ende, de su presencia en el ciberespacio; (ii) el recurso a nuevos métodos de articulación de la guerra psicológica; (iii) la expansión de las fuentes de financiación; y (iv) la creciente interconexión con la delincuencia organizada. Como es lógico, nuestra atención recae sobre la primera de ellas. No obstante, son oportunas un par de pinceladas generales.

Para no faltar a la verdad, lo primero es poner de relieve que el origen de estos rasgos no se encuentra en el 11-S como tal. Aunque esta fecha se emplea como bisagra para diferenciar entre un «viejo» y un «nuevo» terrorismo, lo cierto es que tras ese luctuoso día más que a cambios repentinos asistimos a la consolidación gradual de tendencias ya existentes[88]. El uso de internet por los grupos terroristas, incluido el dirigido a obtener financiación, era una realidad

[87] SALINAS DE FRÍAS, A., *Counter-terrorism and human rights in the case law of the European Court of Human Rights*, Council of Europe Publishing, Strasbourg, 2012, p. 11; FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 483; o BERMEJO GARCÍA, R., "Las denominadas (…)", *op. cit.*, pp. 13 y ss.

[88] SCHMID, A. P., *Revisiting the Relationship between International Terrorism and Transnational Organised Crime 22 Years Later*, The International Center for Counter-Terrorism Research Paper, The Hague, 2018, p. 12.

antes del cambio de milenio[89]. Tampoco la simbiosis entre el terrorismo y la delincuencia organizada, capaz de engendrar sustantividades propias como el narcoterrorismo, puede catalogarse en puridad como una novedad[90]. De igual forma, las estrategias utilizadas para propagar el terror se han transformado continuamente, antes y después de internet, ya sea en los medios empleados, en los sujetos involucrados o en los objetivos señalados[91].

Lo segundo es advertir que entre esos caracteres puede intuirse fácilmente cierto ligamen. Por ejemplo, la interrelación con la delincuencia organizada obedece, amén de otras razones, a la obtención de nuevas vías de financiación[92]. Igualmente, el mundo virtual es donde se generan y al mismo tiempo se satisfacen algunas necesidades consustanciales al terrorismo. Basta con comprobar que el púlpito más elevado para predicar un particular credo, el techo más amplio para dar cobijo a todos los que prueben su lealtad y las cajas fuertes más seguras para guardar las contribuciones anónimas para la «causa» se encuentran ahora en el ciberespacio. Puestas las unas al lado de las otras, estas razones permiten explicar con bastante precisión por qué la web se ha erigido rápidamente como un recurso predilecto para estos grupos[93].

---

[89] DENNING, D. E., "Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy", en ARQUILLA, J. y RONFELDT, D. (Eds.), *Networks and netwars. The future of terror, crime and militancy*, Rand Corporation, Santa Monica, 2001, p. 252; SÁNCHEZ MEDERO, G., "Ciberterrorismo. La guerra del siglo XXI", *El viejo topo*, nº 242, 2008, p. 16; JACOBSON, M., "Terrorist Financing and the Internet", *Studies in Conflict & Terrorism*, vol. 33, nº 4, 2010, pp. 353-354.

[90] Antes del 11-S existían algunas «*violent hybrid organizations*», como las FARC colombianas o el Grupo Abu Sayyaf filipino. *Vid.* SCHMID, A. P., *Revisiting the (…)*, *op. cit.*, p. 13. Sobre la hibridación y los porqués de la cooperación entre ambos fenómenos, *vid.* MARRERO ROCHA, I., "Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas", *Revista Española de Derecho Internacional*, vol. 69, nº 2, 2017, pp. 145-169. Sin embargo, es cierto que será después del 11-S cuando la preocupación se asiente en el seno de la ONU, *vid.*, entre otras, S/RES/1973 (2001) y S/RES/2195 (2014).

[91] Para una síntesis reciente de las distintas oleadas en el terrorismo, *vid.* GAZAPO LAPAYESE, M. J., *Daesh: terrorismo global y local a medio camino entre lo físico y lo virtual* (Tesis: Ed. electrónica), Universidad Complutense de Madrid, Facultad de Ciencias Políticas y Sociología, Departamento de Relaciones Internacionales e Historia Global, 2019, pp. 79-85.

[92] SCHMID, A. P., *Revisiting the (…)*, *op. cit.*, pp. 17-18.

[93] En 1998 los sitios web terroristas eran una docena, *vid.* WEIMANN, G., *How Modern Terrorism Uses the Internet*, Special Report 116, United States Institute of Peace, Washington D. C., 2004, p. 2. Hace una década eran más de 10.000 según SÁNCHEZ MEDERO, G., "El ciberterrorismo: De la web 2.0 al internet profundo", *Ábaco*, nº 85, 2016, p. 100. En lo referente a páginas web ya se habían identificado más de 300.000 con este contenido hace quince años, como muestran REID, E. *et al.*, "Collecting and Analyzing the Presence of Terrorists on the Web: A Case Study

Todo lo anterior prueba que el terrorismo internacional es un leviatán, si bien esto no puede ser una desmotivación a la hora de afrontarlo. Antes al contrario, debe servir para incentivar mejores análisis del recorrido terrorista, es decir, de dónde venimos y a dónde vamos en este ámbito. Solo así podremos comprender esta ignominia camaleónica, capaz de adaptarse a los cambiantes contextos con tal de sobrevivir. En lo que a esta contribución respecta, si en palabras de ALCAIDE FERNÁNDEZ «la internacionalización del terrorismo ha venido acompañada no solo por un aumento de los actos terroristas, sino por una nueva configuración cualitativa del fenómeno»[94], poca duda cabe de que en esa nueva configuración del terrorismo a nivel internacional la red de redes ha tenido un rol crucial gracias a su acentuada capacidad transformativa[95].

III.A.2. ¿Por qué internet?

Internet, y en especial la *World Wide Web* (WWW), ha permitido a los terroristas establecer nuevos lazos de comunicación para interactuar con miembros y con terceros, adoctrinar y reclutar a simpatizantes, intercambiar información, mercadear con productos y datos, difundir propaganda, recaudar fondos, incitar a la comisión de actos terroristas, coordinar ataques, reivindicar sus actuaciones y, en fin, desarrollar en otra dimensión la guerra psicológica[96] que libran estos grupos.

La revolución virtual ha desempeñado —y desempeñará— un papel fundamental en la metamorfosis del terrorismo internacional. Una metamorfosis continua, pero también incompleta, pues a na-

---

of Jihad Websites", en KANTOR, P. *et al.* (Eds.), *Intelligence and Security Informatics*, vol. 3495, Springer, Berlin, Heidelberg, 2005, p. 406. Hoy en día las cifras son desorbitadas si además se incluyen los perfiles en redes sociales. Se estima que son publicados entre 100.000 y 200.000 tuits diarios relacionados de algún modo con *Daesh*, *vid.* BROADHURST, R. *et al.*, *Cyber Terrorism: Research Review*, Australian National University, Cybercrime Observatory, Canberra, 2017, p. 69.

[94] ALCAIDE FERNÁNDEZ, J., *Las actividades (…)*, *op. cit.*, pp. 30-31.

[95] FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 477.

[96] CHICHARRO LÁZARO, A., "Respuesta internacional al desafío de la estrategia mediática del Estado Islámico", *Revista Electrónica de Estudios Internacionales*, nº 29, 2015, p. 7, nota 27 indica que esta guerra psicológica pasa por crear un alarmismo colectivo causado por el miedo, la conmoción, la excitación o la psicosis generalizada para ejercer una presión psicológica subjetiva, la cual forma parte de estrategias más amplias para la consecución de sus objetivos. Dicha guerra se empieza a ganar cuando la comisión de un acto terrorista pasa de concebirse como una mera posibilidad a asumirse como una realidad a nivel social, siendo la incertidumbre del dónde y el cuándo acontecerá lo que genera ese pavor.

die se le escapa que, aunque las organizaciones terroristas «tradicionales» aún perviven, no son ya los únicos actores sobre el escenario. Coexisten con y se nutren de los «lobos solitarios», quienes encuentran más rápida y fácilmente en el mundo virtual que en el real las diatribas radicales, las propuestas de reclutamiento, los campamentos de adiestramiento y el colmo de sus vacíos sentimentales, identitarios y existenciales. Incluso dentro de esta metamorfosis parece que el rema de los últimos atentados de trascendencia internacional se han visto influidos por la espectacularidad, la inmediatez y el difícil control de los contenidos en la red.

El terrorismo ha sabido explotar con versatilidad las herramientas disponibles en cada época[97]. En un inicio recurrieron a rudimentarias páginas web[98]. Después se sirvieron de foros como *PalTalk*, plataformas de contenido multimedia del estilo de *YouTube* y redes sociales como *Facebook* o *Twitter*. Con posterioridad se conoció su predilección por aplicaciones cifradas que permiten alcanzar con mayor seguridad un público casi ilimitado, entre ellas *Telegram* o *TrueCrypt*, si bien las recientes restricciones impuestas en dichas aplicaciones han ayudado al desarrollo de otras tendencias, como la experimentación en las plataformas *RocketChat*, *ZeroNet* o *Riot*, propias de la «web descentralizada» (*DWeb*)[99], cuya principal ventaja es que ofrece un mayor dominio sobre la información y el contenido que en ella se alojan[100].

Del mismo modo, es conocido el desplazamiento de los terroristas hacia la *deep web*, esa parte de internet unas quinientas veces más grande que la web superficial[101] a cuyo contenido no se puede acceder mediante los buscadores comúnmente conocidos, como *Google*, *Yahoo!* o *Bing*; y más concretamente a sus profundidades, la llamada *dark web*, intencionalmente oculta y solo accesible a partir de

[97] Sobre cómo los terroristas se han mudado de una a otra, *vid.* WEIMANN, G., "Terrorist Migration to the Dark Web", *Perspectives on Terrorism*, vol. 10, nº 3, 2016, pp. 40-44 y WEIMANN, G., "Terror on Facebook, Twitter, and Youtube", *The Brown Journal of World Affairs*, vol. 16, nº 2, 2010, pp. 45–54.

[98] TORRES SORIANO, M. R., *Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda* (ARI nº 110/2009), Real Instituto Elcano, 2009, pp. 3 y ss.

[99] No obstante, Europol indica que *Telegram* sigue siendo la herramienta predilecta de Al-Qaeda y Daesh para comunicarse. Ahora bien, este tipo de tendencias «demuestra la voluntad y la preocupación de estos grupos por indagar en las nuevas tecnologías". *Vid.* EUROPOL, "European Union Terrorism Situation and Trend Report", Europol, The Hague, 2019, p. 39.

[100] KING, P., "Islamic State group's experiments with the decentralised web (Conference Paper)", *3rd Conference of the European Counter Terrorism Centre (ECTC) Advisory Networks*, 9-10 April, 2019, The Hague, pp. 1-9.

[101] SÁNCHEZ MEDERO, G., "El ciberterrorismo:(…)", *op. cit.*, p. 105.

softwares específicos como *Tor* o *I2P*. Si a ello se le unen los conocimientos cada vez más sofisticados que estos individuos poseen[102], la monitorización y el seguimiento de sus actividades se presenta como un reto de creciente exigencia para los Estados, los servicios de inteligencia y las agencias de seguridad[103]. Ante este panorama hay quien ha apuntado la paradoja de que la proliferación de usuarios y contenido terrorista en la web, la más innovadora red de comunicación creada por el mundo occidental, sirva precisamente a los intereses del terrorismo internacional, gran amenaza de aquel[104].

Si se quiere entender el singular atractivo que lo cibernético presenta para los terroristas, lo primero es recordar que estos sujetos también son usuarios de redes. Dado que en menos de tres décadas el número de usuarios en la red ha pasado de un millón a casi cuatro mil millones y medio[105], puede entenderse que el incremento y la sofisticación del uso de internet por los terroristas es una consecuencia natural de la masiva migración a un continente virtual en el que, si todo tiene cabida, el terrorismo no iba a ser una excepción.

Pero también hay razones específicas, radicadas en las ventajas que les reporta la configuración de la dimensión virtual, que explican por qué los terroristas se sienten especialmente cómodos en este espacio. Características como la transnacionalidad, la descentralización, la deslocalización, el alcance y la neutralidad de internet se adaptan mejor a la morfología de las organizaciones terroristas que a la de los Estados que las sufren[106]. Asimismo, se trata de una herramienta singularmente provechosa ya que es barata y anónima, de fácil accesibilidad y permite incrementar los potenciales objetivos[107]. A esto se une que lo «ciber» posee algunas ventajas sobre otros medios de ataque. Entre ellas se encuentra su mayor maleabilidad con menor peligro frente a otros materiales —como los nucleares, químicos o biológicos[108]—, así como su manejo a distancia[109] sin tener

---

[102] Más profundamente sobre esta cuestión, *vid.* MALIK, N., *Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies*, The Henry Jackson Society, London, 2018.

[103] WEIMANN, G., "Terrorist Migration (…)", *op. cit.*, p. 43.

[104] WEIMANN, G., "Terror on (…)", *op. cit.*, p. 53. KLEIN, J. J., "Deterring and Dissuading Cyberterrorism", *Journal of Strategic Security*, vol. 8, nº 4, p. 23 contempla una idea parecida.

[105] *Vid.* NYE JR., J. S., *Cyber (…)*, *op. cit.*, p. 3 y *supra* p. 701, nota 4.

[106] MORÁN BLANCO, S., La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo, *Revista Española de Derecho Internacional*, vol. 69, nº 2, 2017, p. 202.

[107] KLEIN, J. J., "Deterring and (…)", *op. cit.*, pp. 27-28.

[108] FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 476.

[109] KLEIN, J. J., "Deterring and (…)", *op. cit.*, p. 28.

que manipular explosivos o cometer ataques suicidas[110], lo que supone un incentivo para aquellos simpatizantes que, siendo aversos a la muerte, muestran su interés en contribuir a la «causa». Además, dado que internet se ha asentado más sobre los pilares de la libertad que sobre los de la seguridad, los ataques por esta vía poseen ventajas estratégicas sobre las estructuras defensivas erigidas en la red[111]. De esta forma, los beneficios de un potencial conflicto asimétrico, que son los preferidos por los terroristas y los propios de este escenario, resultan superiores para estos actores no estatales, pues ahí son menos vulnerables y cuentan con ventajas relativas[112]. Por consiguiente, el ciberespacio se ha ido configurando como un lugar idóneo para ejercer una presión constante de cara a la consecución de sus objetivos.

Teniendo en cuenta este contexto, considerar al ciberterrorismo una amenaza de nuestro tiempo es, más que oportuno, imprescindible. A partir de ahí, su desbaratamiento pasa por una respuesta adecuada capaz de garantizar la seguridad en el mundo real y en el virtual, lo cual solo se antoja posible en la medida en que dicha amenaza resulte correctamente delimitada.

III.B. Aproximación conceptual

Para abordar el ciberterrorismo[113] puede partirse de dos premisas. La primera es que, al igual que sucede con el terrorismo, tampoco existe una definición universal. La segunda es que, en tanto que «ciber», su relación con las redes informáticas y el mundo digital constituye un rasgo esencial, si bien el ciberterrorismo es algo más que la simple añadidura de un prefijo a un lexema[114]; máxime cuando este lexema es objeto de disensiones.

---

110 DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 281.

111 NYE JR., J. S., *Cyber (…)*, *op. cit.*, p. 5.

112 *Ibid.*, esp. pp. 4 y 13.

113 El primer uso de este término se ha atribuido a Barry C. Collin en los años 80, *vid.* BROADHURST, R. *et al.*, *Cyber Terrorism (…)*, *op. cit.*, p. 2. No obstante, otros autores señalan que se formuló algún año antes en Suecia, *vid.* OLEKSIEWICZ, I., "Challenges of EU Security on the Example of Cybterterrorism Policy", *Journal of International Trade, Logistics and Law*, vol. 1, nº 1, 2015, p. 25 y SMOLAREK, M. y WITKOWSKI, M., "Threat Analysis in the Network-Centric Environment", *International Conference Knowledge-based Organization*, vol. 22, nº 3, 2016, p. 552.

114 YANNAKOGEORGOS, P. A., "Rethinking the (…)", *op. cit.*, p. 44.

A pesar de la multiplicación de esfuerzos académicos en los últimos años[115], todavía existe cierta confusión en torno al ciberterrorismo. Hay quien apunta que dicha confusión se ha visto favorecida en parte por la expansión de su noción hasta el punto de confundir, mezclar o absorber otras realidades, como el uso de internet con fines terroristas o el hacktivismo[116]. Entonces, ¿qué es el ciberterrorismo?

Una estrategia en tres pasos es óptima para responder. El primero es perfilarlo pragmáticamente como el espectro de confluencia entre el ciberespacio y el terrorismo[117]. El segundo es la identificación de los actos y actividades terroristas que tienen o pueden tener lugar en el ciberespacio. Para ello tomamos en consideración las seis categorías expuestas por la Oficina de las Naciones Unidas contra la Droga y el Delito (en adelante, UNODC, por sus siglas en inglés)[118]: (i) propaganda; (ii) adiestramiento; (iii) financiación; (iv) planificación; (v) ejecución; y (vi) ciberataques. Tras un breve análisis de cada una de ellas, el tercer y último paso consiste en diferenciar lo que no es ciberterrorismo de lo que sí lo es.

Como se ha señalado que para los terroristas el principal atractivo de internet reside en todo lo que rodea a un ataque excepto en su utilización como medio de ataque en sí mismo[119], se tomará esta idea como punto de partida. En el siguiente apartado se tratan las cinco primeras categorías recién enunciadas. La sexta se deja para un apartado posterior en el que se responderá a la pregunta formulada anteriormente.

---

[115] En 2014 ya se habían contabilizado unos 31.000 artículos académicos sobre terrorismo y ciberespacio, *vid.* TORRES SORIANO, M. R., "¿Es el yihadismo una ciber-amenaza?", *Revista de Occidente*, nº 406, marzo 2015, p. 22.

[116] KENNEY, M., "Cyber-Terrorism in a Post-Stuxnet World", *Orbis*, vol. 59, nº 1, 2015, pp. 111-128, esp. pp. 112 y 125; TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 21.

[117] COLLIN, B. C., "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge" (Paper), *11th Annual International Symposium on Criminal Justice Issues*, The University of Illinois at Chicago, 1996.

[118] UNODC, *El uso de internet con fines terroristas*, Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Nueva York, 2013, pp. 3-13.

[119] SÁNCHEZ FRÍAS, A., "¿Cazador o presa en la telaraña del terror?: La UE en la lucha contra el ciberterrorismo" (Ponencia), *II Seminario internacional UC3M sobre criminalidad organizada transnacional y terrorismo*, 2016, p. 5; MORÁN BLANCO, S., "La ciberseguridad (…)", *op. cit.*, p. 204.

III.B.1. Una cosa es el «uso de internet con fines terroristas»

En primer lugar, en cuanto a la preparación y difusión de propaganda, internet posibilita una estrategia de comunicación cuyo atractivo reside en la eliminación de las asimetrías informativas[120]. En la web existe un dominio completo sobre el qué, el cómo y el cuándo de la propaganda, sin cortapisas en la radio, la televisión o la prensa escrita que moldeen el mensaje y resten difusión[121]. De este modo se consigue una comunicación directa con una audiencia muy variada: miembros, colaboradores, simpatizantes, público neutral, víctimas, objetivos, gobiernos y comunidad internacional. Para conseguirlo los soportes más utilizados son[122]: mensajes, imágenes, infografías, revistas, audios o vídeos difundidos por diferentes vías[123]; entre ellas, páginas web, foros, redes sociales, videojuegos, revistas, plataformas de intercambio de ficheros o aplicaciones de distinta naturaleza[124].

Estas herramientas permiten generar más fácilmente la sensación de pertenencia a una comunidad; sensación que llevada al extremo puede derivar en otros fenómenos como la radicalización, el reclutamiento o la incitación a la comisión de ataques terroristas. Esto es así porque el material disponible en la web ha facilitado enormemente la rapidez con la que se suceden las distintas fases de la radicalización, en virtud de las cuales un sujeto en inicio carente de inclinación alguna hacia la perpetración o el apoyo de actos terroristas se convierte en alguien con dicha pulsión[125]. Como resultado, puede señalarse que el número de individuos con estas inquietudes, dispuestos a engrosar las filas de un grupo, y, en consecuencia, aprovechables para la «causa», aumenta gracias a la globalización que internet favorece[126]. Todo ello acelera y facilita la labor de los reclutadores, quienes tienen un mayor número de blancos potenciales a un solo clic.

---

120 SÁNCHEZ MEDERO, G., "La nueva estrategia comunicativa de los grupos terroristas", *Revista Enfoques: Ciencia Política y Administración Pública*, vol. 8, nº 12, 2010, p. 211.

121 DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 246. También hay quien apunta que esa «era dorada» de dominio casi absoluto que les permitía granjearse miles de seguidores podría haber acabado, *vid.* TORRES SORIANO, M. R., *El estado de la yihad online un año después de los atentados de Barcelona y Cambrils*, Informe del Instituto de Seguridad y Cultura, 2018, p. 18.

122 GAZAPO LAPAYESE, M. J., *Daesh: terrorismo (…)*, *op. cit.*, pp. 151 y ss.

123 BROADHURST, R. *et al.*, *Cyber Terrorism (…)*, *op. cit.*, pp. 67-77.

124 Además, existen otras como *Whatsapp*, *Messenger*, *Tumblr*, *Viper*, *Reddit.com*, *Bestgore.com* y un largo etcétera. *Vid.* GAZAPO LAPAYESE, M. J., *Daesh: terrorismo (…)*, *op. cit.*, pp. 159-160.

125 YANNAKOGEORGOS, P. A., "Rethinking the (…)", *op. cit.*, pp. 47-49.

126 GAZAPO LAPAYESE, M. J., *Daesh: terrorismo (…)*, *op. cit.*, p. 84.

En segundo lugar, el adiestramiento se ha visto enormemente facilitado por la cantidad y diversidad de material existente en la red; dando lugar incluso a la idea de una «universidad abierta» para el terrorismo[127]. En internet pueden encontrarse guías para la comisión de atentados con detalladas instrucciones sobre cómo preparar bombas y utilizar diversas armas[128]. Igualmente, abundan en foros y chats los vídeos y las explicaciones con métodos e instrucciones para fabricar explosivos a partir de distintos materiales, entre ellos, por ejemplo, el conocido triperóxido de triacetona[129].

La creciente preocupación por el recrudecimiento y la intensificación del terrorismo internacional —concretamente, el de corte yihadista— se explica en parte porque estos materiales están presentes en la web de forma abundante y con un fácil acceso, tal y como ha sido advertido por el CSNU[130]. De hecho, la preocupación expuesta por la ONU ha sido compartida, sin ir más lejos, por nuestro legislador mediante la tipificación de los delitos de adoctrinamiento y adiestramiento pasivos, incluidos el autoadoctrinamiento y autoadiestramiento[131].

En tercer lugar, las formas de obtener financiación a través de internet se pueden agrupar en cuatro categorías[132]. La primera es la solicitud directa de fondos, por ejemplo, adjuntando los números de cuentas bancarias[133]. La segunda es el comercio electrónico legal[134] e ilegal —como es la venta de petróleo o antigüedades expoliadas[135], e

---

[127] TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 25.

[128] No es difícil hacerse con ejemplares de este tipo, incluso en la *surface web*, como son *The Anarchist Cookbook* y *The Big Book of Mischief*. Otros manuales que circulan por la red son *The Mujahadeen Poisons Handbook* o *The Terrorist's Handbook*, *vid.* WEIMANN, G., *How Modern (…)*, *op. cit.*, pp. 9-10.

[129] El TATP, también llamado «la madre de Satán», ha sido empleado, por ejemplo, en los ataques de París en 2015, Bruselas en 2016, Manchester en 2017 o en la explosión de Alcanar en 2017 en la víspera de los sucesos de Barcelona y Cambrils.

[130] *Vid.* S/RES/2178 (2014).

[131] Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. *Boletín Oficial del Estado*, 31 de marzo de 2015, nº 77, pp. 27177-27185. Sobre ellos, la STS 354/2017, de 17 de mayo de 2017, señala en su FJ 2º «la falta de cobertura en los instrumentos internacionales mencionados en el Preámbulo de la LO 2/2015 de las modalidades de adoctrinamiento pasivo y de autoadoctrinamiento del art. 575.1 y 2 CP».

[132] UNODC, *El uso (…)*, *op. cit.*, p. 7.

[133] WEIMANN, G., *How Modern (…)*, *op. cit.*, p. 7.

[134] EUROPOL, "European Union (…)", *op. cit.*, p. 17, recuerda que la mayoría de las organizaciones terroristas poseen negocios legales desde los que desvían sus fondos a actividades ilegales.

[135] *Vid.* Carta de fecha 13 de noviembre de 2014 dirigida al Presidente del CSNU por el Presidente del Comité del Consejo de Seguridad dimanante de las Resolucio-

incluso el tráfico de órganos humanos[136]—. La tercera es el empleo de servicios de pago utilizando la llamada banca en línea y otras plataformas como *PayPal*[137]. La cuarta es el uso de fundaciones o asociaciones pantalla, aparentemente lícitas y sin ánimo de lucro, que posteriormente desvían sus fondos a estos grupos[138]. Sin embargo, lo cierto es que, excepto en el segundo caso, en el que sí existe una contraprestación, los otros son básicamente donaciones maquilladas como una suerte de apadrinamiento de combatientes[139] o campañas de *crowfunding*[140] para el avituallamiento, habitualmente a partir de criptomonedas como *Bitcoin* o *Monero*[141].

En cuarto lugar, estaría la planificación, que debe entenderse referida a todas las actividades preparatorias de un acto terrorista. Dentro de este grupo de actuaciones tiene singular importancia la comunicación entre los terroristas, ya sea recurriendo a métodos con trayectoria conocida[142], como el «buzón muerto» o la esteganografía, o a otros más modernos facilitados por el uso aplicaciones cifradas, entre ellas *Telegram* o *Zello*[143]. Además, la web se presenta como una gran biblioteca con fondos de inmensa utilidad como los datos personales[144], que permiten un mejor conocimiento de los objetivos marcados. También es de ayuda para la planificación de esos ataques la información gráfica de cualquier punto de la geografía

---

nes del CSNU 1267 (1999) y 1989 (2011) relativas a Al-Qaida y las personas y entidades asociadas (S/2014/815); o las Resoluciones también del CSNU 2199 (2015) y 2347 (2017).

136 NASTITI, A. y WIMMER, A., "Darknet, Social Media, and Extremism: Addressing Indonesian Counterterrorism on the Internet", *Deutsches Asienforschungszentrum Asian Series Commentaries*, vol. 30, 2015, p. 4.

137 UNODC, *El uso (…)*, *op. cit.*, p. 7.

138 JACOBSON, M., "Terrorist Financing (…)", *op. cit.*, pp. 355-356.

139 ZERZRI, M., *The Threat of Cyber Terrorism and Recommendations for Countermeasures*, Center for Applied Policy Research, 2017, p. 3.

140 EUROPOL, "European Union (…)", *op. cit.,* p. 17, alude a *SadaqaCoins*, un mercado de micromecenazgo en la *dark web* para comprar rifles, silenciadores o vehículos 4x4 para los muyahidines.

141 MALIK, N., *Terror in (…)*, *op. cit.*, pp. 37-44.

142 UNODC, *El uso (…)*, *op. cit.*, p. 11.

143 TORRES SORIANO, M. R., *El estado (…)*, *op. cit.*, p. 21.

144 Es cierto que en muchas ocasiones somos los usuarios mismos quienes nos excedemos involuntariamente facilitando nuestra información confidencial en la red, pero también existen otros supuestos en los que somos hackeados para tal fin. Por ejemplo, en 2015 se robó la información de unos 1.300 miembros de las fuerzas armadas y de personal del gobierno estadounidense para posteriormente filtrarlo al *Daesh*, que la publicó en la web animando a cometer ataques contra ellos (*vid.* <https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison>).

disponible en *Google Earth* o *Google Maps*, entre otras[145]. Por último, no se puede obviar el amplio abanico de posibilidades que la *dark web* ofrece para las actividades preparatorias en lo referente a la adquisición de documentación falsificada o robada[146] y armas de distinta naturaleza[147].

En quinto y último lugar, al hablar de la ejecución, la utilización de internet debe entenderse en un sentido logístico, es decir, como instrumento de acompañamiento durante la perpetración del acto terrorista. A tal respecto puede ser utilizado para coordinarse y comunicarse *in situ*[148] o para conseguir una retroalimentación instantánea sin limitaciones físicas o temporales[149]. Finalmente, tampoco sería una novedad utilizar macabramente y sin censura plataformas como *Facebook Live*, para retransmitir un ataque en directo[150], o *Twitter*, para mostrar los resultados de este[151].

Pues bien, lo que todas las cinco categorías anteriores tienen en común es que existen igualmente en el mundo *offline*. La propaganda, el adiestramiento, la financiación, la planificación y la ejecución, aunque fuesen más laboriosas, ya existían antes de internet. Son, adoptando la terminología anglosajona, «*cyber-enabled crimes*»[152], es decir, actividades que las TIC, y en particular internet,

---

[145] Uno de los primeros usos conocidos de estas aplicaciones con dicho propósito fue el de la organización terrorista Lashkar-e-Tayyiba, que utilizó *Google Earth* para planificar la cadena de ataques que se sucedieron en Bombay (India) a finales de noviembre de 2008 (*vid.* <https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html>).

[146] MALIK, N., *Terror in (…)*, *op. cit.*, pp. 32-34.

[147] PERSI PAOLI, G., "The Trade in Small Arms and Light Weapons on the Dark Web: A Study", *United Nations Office for Disarmament Affairs (UNODA) Occasional Papers*, nº 32, October 2018.

[148] YANNAKOGEORGOS, P. A., "Rethinking the (…)", *op. cit.*, p. 52 alude a este uso durante los citados ataques de 2008 en Bombay (*vid. supra*, nota 145). También lo hacen SAUL, B. y HEATH, K., "Cyber (…)", *op. cit.*, p. 150, nota 16.

[149] BROADHURST, R. *et al.*, *Cyber Terrorism (…)*, *op. cit.*, p. 69 alude a este uso de internet durante los atentados del centro comercial *Westgate* de Nairobi (Kenia) en 2013.

[150] Así sucedió en los ataques a las mezquitas de Al Noor y Linwood de Christchurch (Nueva Zelanda) en 2019 en un vídeo de unos 17 minutos de duración emitido a través de este servicio de *streaming*. También se usó tras el asesinato de una pareja de policías en Magnanville (Francia) en 2016. Todavía hoy pueden visualizarse ambos vídeos en la web sin necesidad de una búsqueda exhaustiva. Recientemente se utilizó en el ataque en Nakhon Ratchasima (Tailandia) el 8 de febrero de 2020.

[151] Así lo hizo el asesino del Profesor Samuel Paty mostrando su cabeza decapitada en una fotografía subida a dicha red social el 16 de octubre de 2020.

[152] MCGUIRE, M. y DOWLING, S., *Cybercrime: A review of the evidence. Summary of key findings and implications (Research Report 75)*, Home Office, London, 2013, p. 5. La terminología ha sido recogida por la UNODC, *vid.* <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>.

han potenciado —y en parte modificado—, facilitando su comisión y aumentando tanto el alcance como la magnitud de sus efectos; cumpliéndose así los peores temores de la ONU hace dos décadas[153].

Es por ello por lo que, en nuestro intento de definir el ciberterrorismo, y para evitar posibles confusiones a la hora de abordar la amenaza que este supone, coincidimos con quienes señalan que todas las actuaciones descritas precedentemente —más allá de que se agrupen o no siguiendo taxativamente dichas categorías— son manifestaciones del uso con fines terroristas que estos sujetos hacen de internet, pero no son ciberterrorismo[154].

III.B.2. Y otra es el «ciberterrorismo»

En línea de principio, el ciberterrorismo ha de ser necesariamente un concepto más restringido bajo cuya etiqueta no se incluya el uso de internet con fines terroristas, por mucho que este sea preocupante y digno de una especial atención. En esta tesitura no resta sino delimitar en la medida de lo posible este concepto, siendo conscientes de que, tal y como se dijo, no existe una definición indiscutida en el ámbito internacional.

Para tal fin de nuevo es útil acudir a la terminología anglosajona. Por contraposición a los «*cyber-enabled crimes*», el ciberterrorismo se acomoda dentro de los «*cyber-dependent crimes*», es decir, de aquellos actos cuya comisión no puede tener lugar sin un elemento o tecnología «ciber»[155]. A este respecto se ha apuntado que este tipo de tecnología puede ser utilizada como medio, como objetivo o como

[153] *Vid.* A/RES/53/70.

[154] Entre otros, DENNING, D. E., "Cyberterrorism: The Logic Bomb versus the Truck Bomb", *Global Dialogue*, vol. 2, nº 4, 2000, p. 30; CONWAY, M., "Reality bytes: Cyberterrorism and Terrorist 'Use' of the Internet", *First Monday*, vol. 7, nº 11, 2002, esp. p. 6; WEIMANN, G., "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism*, vol. 28, nº 3, 2005, p. 131; CHARVAT, J. P. I. A. G., "Cyber Terrorism: A New Dimension in Battlespace", en CZOSSECK, C. y GEERS, K., *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 2009, pp. 77-87. También hace esta diferenciación CANDAU ROMERO, jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, *vid. Diario de sesiones de las Cortes Generales, Comisiones Mixtas, XII Legislatura*, nº 105, 2018, sesión nº 18 celebrada el martes 18 de septiembre de 2018 en el Palacio del Senado, p. 6 (disponible en <http://www.congreso.es/public_oficiales/L12/CORT/DS/CM/DSCG-12-CM-105.PDF>).

[155] MCGUIRE, M. y DOWLING, S., *Cybercrime: A (…)*, *op. cit.*, p. 5.

ambos[156]. Pero ¿cómo ha de ser empleada? ¿Como medio? ¿Como objetivo? ¿O como ambos?

No es raro que el ciberterrorismo se describa como la comisión de actos terroristas por medios «ciber» o contra objetivos «ciber», sin optar por una o por otra[157]. Llegado el caso, parece que para la catalogación de un acto como ciberterrorista tiene mayor peso que lo «ciber» sea el medio y no el objetivo[158]. No obstante, si esto es así, cabría preguntarse por qué otros medios novedosos en su momento e igualmente utilizados por el terrorismo, como la telefonía móvil, no dieron pie a una preocupación internacional semejante, suscitando debates, por ejemplo, sobre un «móvilterrorismo»[159].

En esta contribución, partiendo de que un «*cyber-dependent crime*» es principalmente una actuación contra ordenadores, redes o sistemas[160], se prefiere optar por lo que podría ser considerado un concepto de ciberterrorismo «puro»[161] en el que tanto el medio como el objetivo sean necesariamente «ciber»[162]. Y esto sin obviar que tal ataque debe alcanzar un determinado nivel de gravedad y presentar consecuencias tangibles para que pueda escalar a la categoría de ciberterrorismo. Es más, la contemplación del uso dual de esta tecnología como medio de ataque y como objetivo del propio ataque parece ser la que subyace en el documento de la UNODC cuando identifica la última de sus categorías, los ciberataques, con «la explotación deliberada de redes informáticas como medio para lanzar un ataque […] destinado a perturbar el funcionamiento normal de los blancos elegidos, como los sistemas de computadoras, servidores o la infraestructura subyacente»[163].

---

156 DEVOST, M. G. *et al.*, "Information Terrorism: Political Violence in the Information Age", *Terrorism and Political Violence*, vol. 9, nº 1, 1997, pp. 77-78.

157 SAUL, B. y HEATH, K., "Cyber (…)", *op. cit.*, pp. 150 y 151; WEIMANN, G., "Cyberterrorism: The (…)", *op. cit.*, p. 133.

158 JARVIS, L. y MACDONALD, S., "What is Cyberterrorism? Findings From a Survey of Researchers", *Terrorism and Political Violence*, vol. 27, nº 4, 2015, pp. 672-673.

159 FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 477.

160 MCGUIRE, M. y DOWLING, S., *Cybercrime: A (…)*, *op. cit.*, p. 5.

161 DEVOST, M. G. *et al.*, "Information Terrorism: (…)", *op. cit.*, p. 78.

162 KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, p. 126.

163 UNODC, *El uso (…)*, *op. cit.*, p. 12. En consecuencia, quizá hubiera sido mejor otro título para la citada publicación. No obstante, la UNODC parece discernir entre el uso de internet con fines terroristas y el ciberterrorismo, e incluso el hecho de descartar el tratamiento en dicha publicación de esos «ciberataques» confirmaría nuestra argumentación.

Retomando la idea de la convergencia entre el mundo virtual y el mundo físico[164], sabemos que el ciberterrorismo, tal y como se ha orientado, abarca aquellos actos de terrorismo dirigidos contra los ordenadores, las redes o la información contenida en unos y en otras, siempre que sean ejecutados a través de los mismos. En la medida en que anteriormente se propuso una definición de terrorismo[165], basta con aunarle a aquella las ideas recién desarrolladas para estar, ya sí, en disposición de ofrecer una definición de ciberterrorismo.

Puede entenderse que el ciberterrorismo que interesa al derecho internacional consiste «(i) en el uso de un medio "ciber" para cometer o amenazar con cometer un acto contra un objetivo "ciber"; (ii) siempre que tal acto sea capaz de afectar al orden internacional debido a las consecuencias provocadas sobre la vida o la integridad de las personas, o a los estragos causados en bienes, instalaciones o propiedades públicas o privadas; (iii) siendo necesario por lo tanto que exista una proyección o un riesgo de traslación desde el mundo virtual hasta el real de tales consecuencias o estragos; y (iv) que el propósito de dicho acto sea expandir el miedo entre la población o sectores concretos de esta, o coaccionar directa o indirectamente a un gobierno o a una OI para que realice o se abstenga de realizar una determinada acción».

Se ha advertido que para evitar que el ciberterrorismo se convierta en un cajón de sastre que englobe bajo una etiqueta errónea cosas que no se corresponden con este fenómeno, es necesario diferenciarlo de las demás figuras próximas a él[166]. Por ello, una definición estricta como la defendida[167], la cual sustrae del concepto aquellos casos en los que el objetivo no es «ciber», ayuda a disipar la confusión entre el ciberterrorismo y el uso de internet con fines terroristas, lo que redunda positivamente en el análisis de los riesgos e implicaciones de esta amenaza y de las políticas para contrarrestarlo[168]; posibilitando que la sociedad internacional pueda avanzar hacia una respuesta acompasada y eficaz.

---

[164] DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 241.

[165] *Vid.* p. 718.

[166] POLLITT, M. M., "Cyberterrorism — Fact or Fancy?", *Computer Fraud & Security*, vol. 1998, nº 2, 1998, p. 9.

[167] La definición alcanzada es próxima a la ofrecida por DENNING, D. E., "Cyberterrorism: The (…)", *op. cit.*, p. 29.

[168] KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, p. 126.

III.B.3. Que no debe confundirse con el «hacktivismo»

Si lo anterior marca la línea divisoria entre el ciberterrorismo y el uso de internet con fines terroristas, no hace lo propio en lo que se refiere a su distinción con respecto al hacktivismo, el cual también es confundido asiduamente con el ciberterrorismo. Brevemente, se intentará establecer la diferencia esencial entre ambas ciberamenazas.

De la idea según la cual el hacktivismo es la «convergencia del hackeo con el activismo»[169] pueden derivarse las dos razones que provocan dicha confusión con el ciberterrorismo. Dado que se recurre al hackeo, es decir, a la explotación de vulnerabilidades de seguridad en sistemas informáticos o en redes para acceder a la información ahí contenida y emplearla con fines de dudosa licitud, vemos la primera similitud: el medio utilizado, al igual que el objetivo, es «ciber». Asimismo, puesto que el activismo «en general» posee determinadas motivaciones, generalmente ideológicas o políticas, que buscan propiciar un cambio en la agenda de los poderes establecidos en un concreto tiempo y lugar, se aprecia en este rasgo la segunda similitud con el ciberterrorismo: dicha actividad también pretende que determinadas instituciones públicas o privadas cambien el curso de sus acciones, haciendo o dejando de hacer algo.

Eso sí, las similitudes acaban ahí. Cuando los hacktivistas se sirven, entre otras técnicas, de ataques de denegación de servicio (DoS) o de denegación de servicio distribuido (DDoS)[170], del *ransomware*[171] o del *phising*[172], o bien se proyectan mediante un *website defacement*[173] o haciéndose con el control de perfiles en redes sociales, no parecen perseguir la vida o la integridad de las personas o querer destruir bienes, instalaciones o propiedades públicas o privadas, ni

[169] DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 263.

[170] Tanto un ataque DoS como un ataque DDoS tratan de inhabilitar una máquina, un sistema, una aplicación, una web o un servidor con innumerables peticiones o conexiones de usuarios de forma simultánea, en apariencia lícitas, pero que realmente provienen de equipos infectados con un *malware* que los convierte en *bots* cuya única finalidad es inutilizar alguno de los anteriores elementos. Un DoS genera esas peticiones masivas desde un mismo ordenador o dirección IP y un DDoS lo hace desde múltiples.

[171] El «secuestro de datos» consiste en un ataque que restringe el acceso mediante técnicas de cifrado solicitando a cambio un «rescate» para recuperar el acceso al equipo y la información contenida en él.

[172] Se conoce así a la técnica utilizada para obtener fraudulentamente información personal como contraseñas o información bancaria.

[173] Así se denomina al ataque a una página web para «deformarla», es decir, cambiar su apariencia con imágenes o mensajes determinados, como si de un grafiti virtual se tratase.

tampoco expandir el miedo entre la población o sectores concretos de esta[174].

Los ataques propios del hacktivismo buscan generar —y en numerosas ocasiones lo consiguen— perturbaciones, molestias, daños económicos y de reputación, e incluso cierta conmoción o ansiedad en algunos individuos o grupos, pero es bastante cuestionable que estos ataques por sí mismos provoquen un terror más o menos generalizado para con la vida o la integridad de las personas, o que sean capaces de afectar realmente a infraestructuras críticas o sistemas financieros[175]. En breves palabras, puede decirse que el hacktivismo pretende «protestar y perturbar; pero no matar, mutilar o aterrorizar»[176].

¿Entonces por qué la confusión? Una explicación podría ser que la falta de definiciones compartidas globalmente facilita que se asiente el argumentario de quienes, según sus convicciones o de lo afectados que se sientan por sus actuaciones, entienden que son terroristas —concepto sin duda simbólico y poderoso— colectivos como el extinto *LulzSec* o el famoso *Anonymous*[177], involucrados hasta la fecha en actividades eminentemente hacktivistas. Otro motivo quizá sea que, tal y como se ha definido aquí el ciberterrorismo —medio y objetivo «ciber», recuérdese—, este necesita técnicas de hackeo, y que haya quien por este hecho caiga en el error de ver un comportamiento terrorista en cualquier actividad de un hacker. Por último, debe admitirse que los contornos a veces se difuminan porque en ocasiones diversos grupos terroristas se han servido del hacktivismo, por ejemplo, a través de bombardeos de correos

[174] WEIMANN, G., "Cyberterrorism: The (…)", *op. cit.*, p. 131.

[175] KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, pp. 117-121; DENNING, D. E., "Stuxnet: What Has Changed?", *Future Internet*, vol. 4, nº 3, pp. 679-680.

[176] WEIMANN, G., "Cyberterrorism: The (…)", *op. cit.*, p. 136.

[177] Probablemente los más conocidos en la actualidad, pero no los primeros, *vid.* DENNING, D. E., "The Rise of Hacktivism", *Georgetown Journal of International Affairs*, 8 de septiembre de 2015 [en línea].

electrónicos[178] o con ataques como el de 2015 a la televisión francesa *TV5Monde*[179].

En definitiva, la idea que debe retenerse es que el hacktivismo busca comunicar e interactuar con la sociedad mediante disrupciones en internet, pero no a través del terror, como sí lo hace el ciberterrorismo[180]. Y aun cuando los grupos terroristas puedan recurrir al hacktivismo como una actividad más de su agenda[181], esto no debe llevar *per se* a hablar de ciberterrorismo, dado que las técnicas de hackeo, a pesar de que son utilizadas por estos grupos, no alcanzan tal categoría sino cuando causan un daño grave a la vida de las personas o a los bienes, instalaciones o propiedades públicas o privadas[182].

IV. ¿UNA AMENAZA REAL?

Para evaluar esta amenaza puede partirse de una afirmación difícilmente contestable hoy por hoy: «aunque todos los grupos terroristas se encuentran presentes en la Red, un ciberterrorismo auténtico es hasta ahora una posibilidad, más que una realidad cotidiana»[183]. Lo que es tanto como decir que estamos ante un escenario en cierta medida lejano; afirmación que puede reconducirse a dos sencillas

---

[178] En 1998 una filial de los Tigres para la liberación del Eelam Tamil, conocida como *Internet Black Tigers*, realizó un ataque tipo DDoS enviando unos 800 correos electrónicos al día durante dos semanas a las embajadas de Sri Lanka. Se ha apuntado que esta actuación sí pudo haber causado miedo entre el personal de las embajadas, *vid.* DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 269. Sin embargo, parece más adecuado considerar que no fue un caso de ciberterrorismo, sino de hacktivismo realizado por un grupo terrorista ya que no causó daño a las personas ni tampoco a ninguna propiedad. También lo entienden así SAUL, B. y HEATH, K., "Cyber (…)", *op. cit.*, p. 157.

[179] Este ataque, cuya autoría no termina de estar clara, pues se duda si lo realizaron hackers rusos o miembros del *Daesh* (*vid.* <http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html>), «secuestró» durante unas 18 horas las emisiones de televisión, la web y los perfiles en redes sociales de dicha cadena. Pese a que algún miembro del gobierno francés se animó a calificarlo de «acto terrorista» (*vid.* <https://twitter.com/fleurpellerin/status/586046264887930881>), lo cierto es que tal calificación no es la adecuada, como también señalan BROADHURST, R. *et al.*, *Cyber Terrorism (…)*, *op. cit.*, p. 56.

[180] KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, p. 121.

[181] De hecho, esto abre un interesante debate acerca de si no sería más conveniente incluir el hacktivismo como otro uso más del internet con fines terroristas —al menos cuando aquel es utilizado por los terroristas— para reducir categorías en este ámbito en lugar de aumentarlas y crear más confusión.

[182] Tal idea es compartida por SAUL, B. y HEATH, K., "Cyber (…)", *op. cit.*, p. 157.

[183] SEGURA SERRANO, A., "Ciberseguridad y Derecho Internacional", *Revista Española de Derecho Internacional*, vol. 69, nº 2, 2017, p. 294.

razones: (i) porque estos sujetos no pueden recurrir al ciberterrorismo; o (ii) porque estos sujetos no quieren servirse de él.

La primera de ellas considera que, aunque los terroristas estuvieran interesados en adentrarse en el ciberterrorismo, no podrían hacerlo ya que carecen de la capacidad, de las habilidades y de la técnica suficiente[184] para perpetrar ataques avanzados que vayan más allá del simple hackeo. En parte, esto es lo que se extrae del informe más reciente de Europol según el cual, frente a la creciente sofisticación en el uso de internet con fines terroristas, las capacidades de los grupos terroristas para involucrarse en el ciberterrorismo son todavía limitadas y sus técnicas rudimentarias[185]. De aceptar estas razones, no quedaría sino considerar que un ciberterrorismo capaz de afectar al orden mundial —una suerte de «Pearl Harbor digital»[186] o un ataque capaz de generar un contexto similar al post 11-S— es altamente improbable en este momento[187].

¿Y en un futuro? No sería raro agarrarse a aquello de que es «cuestión de tiempo» que al final suceda[188]. Sin embargo, se ha replicado que no existe razón alguna que justifique que el paso del tiempo por sí solo, como si fuese a traer caído del cielo un maná de sabiduría cibernética para los terroristas, juegue a favor de ellos y que, de persistir su incapacidad para dominar estos instrumentos tan complejos, «lejos de encontrarse en un proceso de sofisticación

---

[184] CONWAY, M., "Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur", *Communications of the ACM*, vol. 54, nº 2, 2011, p. 27. Una vía para salvar esto podría ser recurrir a los servicios de quienes sí tienen esa capacidad, lo que se conoce como «*crime as a service*». TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 31 considera que esto no sucederá, pero lo cierto es que, por ejemplo, el IRA Provisional en su momento ya recurrió a hackers, *vid.* DENNING, D. E., "Cyberterrorism: The (…)", *op. cit.*, p. 34.

[185] EUROPOL, "European Union (…)", *op. cit.,* pp. 9 y 20.

[186] Concepto surgido a comienzos de los años 90 y que ha tenido cierto calado, más político que académico, *vid.* STOHL, M., "Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War", en CHEN, T. M., JARVIS, L. y MACDONALD, S. (Eds.), *Cybertorrism: Understanding, Assessment, and Response*, Springer, New York, 2014, pp. 89-90.

[187] CHICHARRO LÁZARO, A., "Respuesta internacional (…)", *op. cit.*, p. 22.

[188] En el seno de la ONU el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de junio de 2013 (A/68/98) apuntaba que «los grupos terroristas utilizan las tecnologías de la información y las comunicaciones para comunicarse, recopilar información, reclutar adeptos, organizar, planificar y coordinar ataques, promover sus ideas y actividades, y recabar financiación. Si esos grupos consiguiesen instrumentos para llevar a cabo ataques, podrían emplear las tecnologías de la información y las comunicaciones para realizar actividades desestabilizadoras».

progresiva, *los terroristas* pueden quedarse estancados de manera indefinida en las capas más superficiales del uso bélico del ciberespacio»[189].

Claro, que de lo que se acaba de decir a señalar que es apodíctico que nunca van a ser capaces de conseguirlo, hay un trecho. Podríamos estar —¿por qué no?— ante una de esas situaciones en las que querer es poder, en cuyo caso precisamente ese paso del tiempo, aunque no traiga por sí mismo esa capacidad, sí permitiría lograr una especialización durante su transcurso. Para ello sería imprescindible que el terrorismo mostrase un verdadero propósito de dominar la dimensión virtual, algo que no sería de extrañar viendo la maestría alcanzada en lo que al uso de internet con fines terroristas se refiere; e incluso podría considerarse una consecuencia lógica de la evolución del fenómeno terrorista[190].

Pero más allá de la falta de capacidad —sin desmerecer la postura ni perderla de vista— ¿y si lo que sucede es que no quieren? También podría ocurrir que carezcan momentáneamente de interés en el ciberterrorismo[191]. Para explicar por qué este sería un razonamiento plausible recuperamos unas palabras de RAMÓN CHORNET: «el terrorismo se presenta siempre con un contenido simbólico: su propósito, su razón de ser es la provocación, la creación de un estado de miedo y ansiedad»[192]; y uno de los pilares de esa parafernalia simbólica es indudablemente la espectacularidad de sus acciones[193]. En lo que atañe a dicha espectacularidad, no es descabellado considerar más impactante, emocional y, en fin, rentable para sus propósitos mediáticos y psicológicos la explosión de una bomba o un atropello masivo que un ciberataque[194]; máxime cuando este último es más difícil de controlar que otros métodos cinéticos —precisamente por las habilidades y capacidades que se requieren— para lograr el nivel de daño deseado[195].

Este camino termina en una última pregunta: ¿y el día que puedan y quieran? Puede que tal fecha suponga un punto de inflexión en dos sentidos. El primero es que quizá entonces la sociedad in-

---

189 TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 31. La cursiva es añadidura nuestra.

190 GAZAPO LAPAYESE, M. J., *Daesh: terrorismo (…)*, *op. cit.*, p. 85, se cuestiona si «puede estar empezando a surgir una nueva oleada terrorista que tiene al ciberespacio como elemento principal sobre el que pivotar».

191 FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 478.

192 RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, p. 72.

193 TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 20.

194 NYE JR., J. S., *Cyber (…)*, *op. cit.*, p. 11.

195 DENNING, D. E., "Activism, Hacktivism, (…)", *op. cit.*, p. 263.

ternacional, al contar ya con un precedente sin ambigüedades, adquiera conciencia de lo que sí es el ciberterrorismo y de lo que no lo es[196]. El segundo es que, dado que los instrumentos internacionales contra el terrorismo se han adoptado siguiendo una especie de patrón «acción-reacción»[197], podría ser ese el preciso momento a partir del cual los Estados se animen a desarrollar el derecho internacional en lo que al ciberterrorismo se refiere[198].

Entretanto, la mejor receta es la precaución. Por una parte, no alimentando desde este lado su motivación e interés con discursos catastrofistas, pues todo ello podría terminar desembocando en una «profecía auto-cumplida»[199]. Por la otra, siendo conscientes de que lo que aún no ha sucedido no significa que nunca vaya a suceder y, por lo tanto, no cometiendo el error soberbio de ignorar o menospreciar la amenaza potencial —y puede que no tan lejana— que supone el ciberterrorismo[200].

V. CONCLUSIONES

Estas páginas han servido para presentar una definición de ciberterrorismo surgida de una profundización en el análisis del vínculo existente entre el terrorismo e internet. La principal virtud de tal definición es que permite distinguir esta ciberamenaza de otras categorías y actuaciones igualmente resultantes de dicho vínculo pero que, como se ha tenido ocasión de exponer, no son ciberterrorismo. No obstante, debe advertirse que, atendiendo a la distinción entre definiciones nominales y definiciones esenciales realizada en este campo de estudio[201], la ofrecida pertenece a las primeras. No se trata de una definición taxativa que presuma de haber hallado el concepto esencial del ciberterrorismo, sino de una definición funcional destinada a ofrecer las pautas necesarias para identificar cuándo una determinada actuación puede subsumirse en un supuesto de ciberterrorismo.

---

[196] Hipotéticos casos catalogados como ciberterrorismo se ofrecen en KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, p. 122 y DENNING, D. E., "Stuxnet: What (…)", *op. cit.*, p. 678.

[197] FIDLER, D. P., "Cyberspace, Terrorism (…)", *op. cit.*, p. 478; SAUL, B. y HEATH, K., "Cyber (…)", *op. cit.*, p. 150.

[198] Es cierto que la Convención sobre la Lucha contra el Terrorismo de 2007 de la Asociación de Naciones del Sudeste Asiático (ASEAN) sí nombra el ciberterrorismo (art. VI), pero sin definirlo.

[199] TORRES SORIANO, M. R., "¿Es el (…)", *op. cit.*, p. 32.

[200] KENNEY, M., "Cyber-Terrorism (…)", *op. cit.*, p. 121; KLEIN, J. J., "Deterring and (…)", *op. cit.*, p. 38.

[201] RAMÓN CHORNET, C., *Terrorismo y (…)*, *op. cit.*, pp. 58-59.

Es de justicia preguntarse si el esfuerzo definitorio realizado presenta o no algún interés para el derecho internacional, puesto que la definición del proyecto de Convenio general sobre terrorismo internacional es lo suficientemente amplia para cubrir —en caso de convertirse en *lex lata* algún día— el ciberterrorismo según se ha definido aquí. Sin esperar al daño para intentar sanarlo, podría responderse en adelanto que la constante innovación tecnológica es una realidad que, si bien es imparable, no puede permitirse que devenga incomprensible. Por consiguiente, es de suma importancia que la ciencia jurídica realice esfuerzos de concreción y distinción de las diversas conductas que tienen lugar en el ciberespacio. Además, no solo debe resaltarse la importancia que albergaría alcanzar tal definición, sino también la singular necesidad de que la misma se consagre en el ámbito universal, ya que universales son el ciberespacio y los riesgos que entraña.

Al fin y al cabo, este proceder no es sino una extensión del seguido en los distintos ordenamientos jurídicos cuando nuestros legisladores diferencian entre los delitos de terrorismo y aquellos otros delitos vinculados a actividades terroristas. En suma, trasladar asimismo esta distinción al mundo «ciber» se antoja pertinente, pues que el ciberterrorismo y otras actuaciones, como el hacktivismo o el uso de internet con fines terroristas, puedan llegar a compartir las mismas consecuencias jurídicas en el ámbito internacional es, más que cuestionable, preocupante.

Por último, apuntar dos breves reflexiones finales. La primera es recordar unas certeras palabras del otrora ministro belga GOL: «el terrorismo sin publicidad no existe»[202]. Por extensión, su vástago, el ciberterrorismo, por más que la tecnología sí lo permitiera, tampoco. Pese a todo, tras tantas décadas afrontando esta lacra y sus consecuencias, y después de haber alcanzado —en teoría— una mejor comprensión de lo que este fenómeno supone, no hemos aprendido tan valiosa lección. De hecho, con la universalización de la comunicación que ha propiciado internet, y más particularmente las redes sociales, parece que se ha retrocedido un paso en este sentido. Ahora la inmediatez, la espectacularidad y la necesidad de aprobación inundan la web cuando se aborda cualquier tema, incluido el terrorismo —y eso que el terrorismo es cualquier cosa menos un tema cualquiera—. Parece que no entendemos, o no queremos entender, que actuando así lo que hacemos es darles publicidad gratuitamente a los terroristas, retroalimentarlos y hacerles el juego. Por

[202] GOL, J., "Coordination (…)", *op. cit.*, p. 5.

ello, aunque cueste asumirlo porque exista la percepción generalizada de que el terrorismo se combate en esferas superiores, lo cierto es que corrigiendo determinados comportamientos individuales también nosotros podemos aportar nuestro granito de arena en esta guerra mediática y psicológica que el terrorismo nos ha declarado.

La segunda es reconocer que el estudio de cualquiera de las manifestaciones del terrorismo provoca la latencia de una incómoda sensación: parece que mientras que nosotros tenemos los relojes, ellos tienen el tiempo. Tiempo para adaptarse a las nuevas realidades; tiempo para aprender los conocimientos y adquirir las habilidades requeridas; tiempo para evaluar si les interesa o no recurrir a lo «ciber» como mecanismo de destrucción; y tiempo para, llegado el caso, elegir un objetivo que haga tambalear los cimientos de nuestra sociedad. Porque si algo está claro es que el tiempo es la principal arma del terrorismo y que su mejor táctica es limitarse a esperar a que otros construyan para luego ellos destruir.

Justo por eso conviene terminar recordando que nosotros somos los que fabricamos y reparamos los relojes en los que ellos miran el paso del tiempo. Sin duda, esto lo que nos diferencia y lo que, mientras siga así, hará que no puedan vencer. No lo olvidemos nunca.