Revista Española de Derecho Internacional
Sección ESTUDIOS
Vol. 69/2, julio-diciembre 2017, Madrid, pp. 195-221
http://dx.doi.org/10.17103/redi.69.2.2017.1.08

ISSN: 0034-9380; E-ISSN: 2387-1253

LA CIBERSEGURIDAD Y EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) POR EL TERRORISMO

Sagrario Morán Blanco *

1. CONSIDERACIONES INTRODUCTORIAS

1. Por los progresos tecnológicos y científicos descubiertos y aplicados en la realidad cotidiana internacional, asistimos, desde finales del pasado siglo, a una revalorización de nuevas dimensiones de la seguridad que permiten que se hable, en la actualidad, de su carácter multidimensional[1]. Una

* El presente trabajo se realizó en el marco del Proyecto de Investigación I+D DER 2014-55848-P, titulado «Actores Económicos Internacionales y Derechos Humanos», así como dentro del proyecto de Investigación Red de excelencia Nuevos Desafíos del Derechos Internacional (DER 2015-69273-REDT). Sagrario Morán Blanco es Profesora Titular de Derecho Internacional Público y Relaciones Internacionales de la Universidad Rey Juan Carlos de Madrid. Correo electrónico: *mariasagrario.moran@urjc.es*. Todas las páginas *web* han sido consultadas por última vez el 13 de junio de 2017.

[1] Entre otros, Buzan, B., «New Pattern of Global Security in the Twenty-First Century», *International Affairs*, vol. 67, 1991, núm. 3, p. 433; Grebosz Andrejhazz, M., «Mutidimensional Character of Globalization», *Zeszyty Naukowe Politechniki Ldzkiej, Organizacja I Zarzadzanie*, vol. 59, 2015, núm. 1.196, p. 14; Zietek, A. W., «Cultural Security: How to analyze it?», Paper to be presented at the 8th Pan-European Conference on International Relations: *One International Relations or Many? Multiple Worlds, Multiple Crisis*, University of Warsaw, 2013.

de las últimas dimensiones de la seguridad es la conocida como «ciberseguridad», es decir, la seguridad del ciberespacio, el «nuevo» espacio surgido a partir de la aparición de esas herramientas que se han convertido en indispensables para el funcionamiento de las sociedades actuales, además de factores estratégicos de primer orden: las Tecnologías de la Información y las Comunicaciones (TIC). Hoy todos los sectores sociales y económicos dependen de la infraestructura de la información y de las telecomunicaciones[2].

2. Las amenazas presentes desde tiempos «inmemoriales» en la sociedad internacional también han penetrado en el ciberespacio, consiguiendo poner en peligro los sistemas informáticos de las empresas e instituciones públicas y, por extensión, a los propios Estados. Las TIC se han convertido, así, en uno de los grandes desafíos de la seguridad por el uso que el terrorismo o la delincuencia hacen de estas para el logro de sus objetivos. El ciberespacio es el «nuevo» terreno donde se desarrollan las «guerras» financieras, energéticas, empresariales, mediáticas, porque esta dimensión espacial se ha convertido en una parte esencial de nuestras sociedades, además de ser un factor determinante en la evolución de las culturas e, incluso, de su convergencia futura[3]. En pocas palabras, se ha fomentado, en la actualidad, la aparición de un nuevo espacio relacional generador de oportunidades y riesgos[4].

3. El objetivo de este trabajo es, precisamente, analizar los beneficios y las ventajas de las TIC en la sociedad internacional y, sobre todo, el uso que los diferentes grupos terroristas hacen de ellas, con el fin de promover y favorecer sus objetivos, generando, a su vez, la aparición de nuevos riesgos, retos y amenazas como el «ciberterrorismo». Por esto, se examinan los marcos e instrumentos político-jurídicos y la práctica de los Estados, también la adoptada en el seno de los organismos internacionales; para hacer frente a este reto de carácter transnacional.

2. EL ESPACIO CONFIGURADOR DE LA CIBERSEGURIDAD: EL CIBERESPACIO

4. El espacio donde se desenvuelve esta nueva dimensión de la seguridad, que es la ciberseguridad, se denomina, como ya hemos dicho, ciberespacio, «nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información —incluida Internet—, las

[2] Suárez-Mira, C., «Internet y derecho penal: viejos y nuevos delitos», en Fernández, J. y Sansó-Rubert, D. (eds.), *Internet: un nuevo horizonte para la seguridad y la defensa*, Santiago de Compostela, Universidad de Santiago de Compostela-CESEDEN, 2010, pp. 103-124.

[3] Véanse Aznar, F., *Entender la guerra en el siglo xxi*, Madrid, Editorial Complutense, 2011; y Beck, U., *Sobre el terrorismo y la guerra*, Madrid, Paidós, 2003.

[4] Véase Joyanes Aguilar, L. (coord.), «Ciberseguridad, Retos y amenazas a la Seguridad Nacional en el Ciberespacio», *Cuadernos de Estrategia*, 2010, núm. 149, *passim*; y «Conectividad, Convergencia, Seguridad e Integración: Un marco para la evolución de las TIC», *Cuadernos OPTI*, 2005, p. 56.

redes y los sistemas de información y de telecomunicaciones»[5]. El ciberespacio, que no entiende de fronteras, difumina las que existen en los espacios terrestre, marítimo o aéreo, permitiendo a sus usuarios participar en una globalización total que comporta numerosos beneficios pero, también, relevantes amenazas y riesgos.

5. El ciberespacio se puede definir como una realidad espacio-virtual, que no tiene una localización física y que abarca los sistemas de información y comunicación contenidos en la Red. De esta nueva dimensión del espacio dependen, también, nuestros servicios básicos, infraestructuras críticas, economía y progreso como sociedad. Por tanto, «la tecnología es el elemento físico básico, configurador del ciberespacio»[6] o, dicho de otra forma, las TIC se configuran como el elemento físico que hace posible el ciberespacio y, desde finales de los años ochenta, este nuevo espacio ha demostrado ser un medio de comunicación dinámico y con capacidad para llegar a todos los rincones del planeta[7]. Ahora bien, el ciberespacio tiene una serie de características y, entre ellas, están la ausencia del espacio físico y del tiempo, «la deslocalización, la transnacionalidad, la neutralidad y la descentralización»[8].

6. Aunque los beneficios de las TIC son numerosos, sin embargo, rápidamente hemos sido conscientes de que la misma tecnología que facilita la comunicación puede explotarse con fines terroristas y delincuenciales. En efecto, las TIC se han convertido en un instrumento del que se sirven los radicales para conseguir sus objetivos. Este nuevo escenario, que facilita el intercambio de información y de la comunicación entre ciudadanos, empresas e instituciones públicas, y que alberga información valiosa y sustenta servicios estratégicos; conlleva, al mismo tiempo, serios riesgos y amenazas que pueden afectar a la seguridad nacional e internacional. Esto nos revela que hay vulnerabilidades a la privacidad y seguridad de las personas. Por ello, hay que unir todos los esfuerzos posibles para desmantelar el riesgo que se puede dar si los «ciberterroristas» y «ciberdelincuentes» hacen realidad sus planes y objetivos.

7. En esta línea, se ha dicho que el ciberespacio «capacita a muchos sujetos —y no solo a los Estados— para acceder a un arma cibernética con capacidad de realizar acciones susceptibles de ser calificadas como ataques,

---

[5] El término se usó por primera vez por William Gibson en 1984 en *Neuromante*. Véase el documento «Estrategia de Ciberseguridad Nacional, 2013», Capítulo I, p. 9, en *http://www.lamoncloa.gob.es/documents/20131332estrategiaciberseguridadx.pdf*.

[6] *El uso de Internet con fines terroristas*, Nueva York, Oficina de las Naciones Unidas contra la Droga y el Delito, Naciones Unidas, 2013, p. 3.

[7] Molina Mateos, J. M., «Globalización, Ciberespacio y estrategia. Especial consideración a la estrategia de la información», *Documento Opinión,* núm. 100/2014, de 12 de septiembre, p. 20. Véase Couldry, N. y Curran, J., *Contesting Media Power. Alternative Media in a Networked World*, Nueva York, Rowman Littlefield Publishers, 2003.

[8] Blasco, A. J., *¿Qué es Internet? En principios de derecho de Internet*, Valencia, Tirant lo Blanch, 2002, pp. 30-98. En Ramos Alonso, I., «Terrorismo Yihadista y Nuevas Tecnologías», *Documento del Centro Criminal para el estudio y prevención de la delincuencia de la Universidad Miguel Hernández*, 2016, p. 3.

agresiones o usos de la fuerza armada en el contexto internacional»[9]. Mas, en particular, como señala Ángel Gómez de Ágreda, el ciberespacio «vive en un estado permanente de agresión en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección»[10]. Por todo, queda claro que el reto que tenemos por delante es conformar un ciberespacio seguro, libre y pacífico.

8. Ahora bien, definir el ciberespacio obliga, también, a catalogar otros conceptos como es el de «ciberarma», puesto que en esta nueva dimensión del espacio se producen ataques. Margarita Robles Carrillo señala, a estos efectos, que el «Consejo de Seguridad de Naciones Unidas, que es el máximo responsable en materia de mantenimiento de la paz y la seguridad internacional, no ha querido o no ha tenido ocasión de pronunciarse calificando una acción cibernética como un uso de la fuerza, una amenaza a la paz, un quebrantamiento de la paz o un acto de agresión»[11]. De tal forma que procede afirmar que las obligaciones adquiridas por los Estados en el marco de Naciones Unidas (Capítulo VII) se extienden al ciberespacio[12].

9. Nuestra asignatura aún pendiente es definir el concepto de «arma cibernética», esto es, cómo se califica jurídicamente una acción cibernética capaz de constituir un uso de la fuerza prohibido por las normas del Derecho internacional (DI)[13]. En este sentido, es fundamental tener en cuenta que en el entorno virtual todo es más ambiguo, porque una misma acción puede cumplir diferentes funciones. Una acción en Internet puede ser un acto de guerra o un acto de espionaje, indistintamente. Aunque «su calificación dependerá de la intención del autor», no debemos perder de vista que, «los efectos de la acción cibernética se manifiestan también como un elemento clave para determinar su naturaleza como acción armada»[14].

10. En resumen, el examen de la práctica internacional nos revela que «no hay un concepto de ciberarma definida jurídicamente, aceptado institucionalmente o compartido doctrinalmente». Una acción cibernética puede ser calificada como cibercriminalidad, ciberespionaje, ciberterrorismo, etc. Con ello, se aprecia que no es fácil definir y catalogar todo aquello que sucede en el ciberespacio y que, en consecuencia, esto permanece como tarea pendiente si se quieren combatir, con eficacia, los actos terroristas que se producen en ese espacio.

---

[9] Robles Carrillo, M., «El concepto de arma cibernética en el marco internacional: una aproximación funcional», *Documento de Opinión 101/2016 del Instituto Español de Estudios Estratégicos*, 2016, p. 13.

[10] Gómez de Ágreda, A., «El ciberespacio como escenario de conflictos. Identificación de las amenazas», en *El ciberespacio. Nuevo escenario de confrontación*, Madrid, Monografías del CESEDEN, 2012, p. 180.

[11] Robles Carrillo, M., *op. cit.*, nota 9, pp. 6-7.

[12] En la Cumbre del G-7 celebrada en Ise-Shima, Japón, en mayo de 2016, se adoptaba una declaración conjunta sobre los principios y acciones en el ciberespacio. En *ibid.,* p. 7.

[13] *Ibid.*, pp. 9-12. Véase también Silver, D. N., «Computer Network Attack as a use of Force under Article 2(4) of the United Nations Charter», *International Law Studies*, vol. 76, 2002, p. 74.

[14] Robles Carrillo, M., *op. cit.*, nota 9, p. 17.

2.1. Las oportunidades y beneficios de las TIC en la Sociedad Internacional a la luz de eventuales actos terroristas

11. desarrollo de las TIC ha generado un nuevo espacio de relación que brinda evidentes beneficios y ventajas, también en el plano internacional. Entre ellas se pueden destacar, al menos, las siguientes:

12. Primera, la rapidez y facilidad de los intercambios de información y comunicaciones. Las noticias de un atentado las podemos tener actualizadas al segundo en las páginas de cualquier periódico o canal de televisión o radio y, del mismo modo, los terroristas pueden comprobar, en tiempo real y casi al instante, las reacciones que provocan sus acciones en la comunidad internacional.

13. Segunda, la ubicuidad y el bajo coste es otro de los principales factores de las ventajas de las TIC. La tecnología de Internet hace que resulte fácil para una persona comunicarse con relativo anonimato. Precisamente por ello, los terroristas y delincuentes no dudan en trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que este ofrece. Hay que destacar, también, que muchas de las herramientas utilizadas por los terroristas y delincuentes pueden obtenerse de forma gratuita o a un coste muy reducido. Políticos y responsables policiales reconocen «que usando fuentes abiertas y sin actuar ilegalmente es posible obtener hasta el 80% de la información necesaria sobre el enemigo» [15]. El uso de tecnologías de cifrado de datos (encriptado), por parte de los terroristas, para ocultar sus comunicaciones en Internet dificulta, asimismo, su identificación y detención. Todo parece indicar que la aplicación de mensajería gratuita, *Telegram,* habría sido una de las herramientas utilizadas por los terroristas que planificaron el atentado contra la revista satírica *Charlie Hebdo* (París), en enero de 2015 [16]. Pero, también, en el atentado de Londres, en marzo de 2017, se comprobó como el terrorista que lo llevó a cabo utilizó *WhatsApp*, justo antes del ataque.

14. Por último, la efectividad y el impacto son notas características de las TIC. Los terroristas y delincuentes han comprobado que sus acciones criminales consiguen un gran impacto en la comunidad internacional gracias a su difusión a través de las TIC. El principal objetivo del terrorismo, que no es otro que aterrorizar a la población a través de sus atentados, es más «sencillo» que nunca gracias al efecto multiplicador del miedo que los atentados tienen gracias a las TIC. Recordemos el sentimiento de terror que generó la visualización, a través de las redes sociales, del degollamiento del periodista norteamericano, James Foley, en agosto de 2014, por un terrorista del *Estado Islámico de Iraq y el Levante* (ISIS).

---

[15] Gutiérrez, A., «¿Cómo el terrorismo islamista usa Internet?», en *file://Dialnet-Como ElTerrorismoIslamistaUsaInternet-4111887.pdf*.

[16] Para las consecuencias de este atentado, en perspectiva jurídica: Díaz Galán, E. C., «Bombardeos en Siria e Iraq: la aparición de nuevos componentes normativos para la licitud o ilicitud del uso de la fuerza en el orden internacional», *REDI*, vol. 68, 2016, núm. 1, pp. 231-235.

2.2. Protección de las infraestructuras críticas y las dificultades del terrorismo para realizar ciberataques

15. El objetivo dirigido a atacar, desde el ciberespacio, los lugares más sensibles de un Estado, es decir, todo aquello que compromete a sus sectores estratégicos, no parece posible para los terroristas y delincuentes, a día de hoy. En concreto, las actividades realizadas por este medio resultan más fáciles de detectar por las agencias de Seguridad o de la Policía, mediante el rastreo de las tarjetas de crédito, cuentas bancarias, teléfonos móviles, etc. En realidad, la posibilidad del uso del ciberespacio por organizaciones terroristas para llevar a cabo ataques contra sistemas informáticos, cuya hipótesis más peligrosa sería un ataque contra alguna infraestructura crítica, parece difícil. De hecho, podemos constatar que, hasta la fecha, no se ha materializado[17].

16. No olvidemos, a estos efectos, que los grupos terroristas no gozan de personal altamente cualificado en las nuevas tecnologías. A ello se suma el factor, quizá más notable, que consiste en que «la mayoría de los sistemas informáticos sensibles, como por ejemplo los del Ministerio de Defensa de Estados Unidos o de los servicios de inteligencia, no están conectados a Internet. Son lo que se denomina *air-gapped systems*, por lo que no pueden sufrir un ataque dirigido desde la Red»[18]. Estos sistemas manejan lo que se conoce como infraestructuras críticas (servicios de emergencia, financieros, de materiales peligrosos, etc.). En suma, no se aprecia peligro real tanto por la formación y preparación de los terroristas como por la protección de la que gozan los sistemas sensibles.

17. No obstante, estas observaciones no eliminan por completo la amenaza porque el ciberterrorismo no descarta la posibilidad de utilizar el ciberespacio como un objetivo en sí mismo para la perpetración de ataques contra servicios esenciales o infraestructuras críticas. Está claro que el fin de los Estados es hacer un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques, por lo que es necesario que los Sistemas TIC de las Administraciones públicas y de las empresas e infraestructuras críticas posean el adecuado nivel de ciberseguridad.

---

[17] El Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) 2007 las define como: «Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas». Este Plan fue revisado a través de la Instrucción 01/2016, de 10 de febrero. Actualmente el PNPIC aprobado el año pasado es fruto del Sistema de Protección de Infraestructuras Críticas «emanado de la Ley 8/2011, PIC».

Para conocer qué es una infraestructura crítica europea (ICE) véase la Directiva europea 2008/114/CE, de 8 de diciembre, sobre «Identificación y designación de infraestructuras críticas europeas y evaluación de la necesidad de mejorar su protección», *https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.*

[18] Sansó-Rubert, D., «Yihadismo e internet, un nuevo espacio para la acción terrorista», en Fernández, J. y Sansó-Rubert, D. (eds.), *op. cit.*, nota 2, p. 72. Véase Walden, I., *Computer Crimes and Digital Investigations*, Oxford, Oxford University Press, 2007.

18. Una de las principales amenazas a la seguridad de las TIC son los ciberataques, entendidos como «cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados de fuentes anónimas que también roban, alteran o destruyen un blanco específico mediante *hackeo* de un sistema vulnerable»[19]. En otros términos, un ciberataque se refiere a la explotación deliberada de redes informáticas como medio de lanzar un ataque a un objetivo determinado, con capacidad para poner en riesgo la seguridad nacional de los Estados. Estos ataques suelen buscar el crear disfunciones en los sistemas de ordenadores, mediante el uso de técnicas de piratería informática, virus informáticos, etcétera.

19. Los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. Unos ataques que, en ocasiones, son realizados por los propios Estados, por ser estos quienes disponen de capacidades y conocimientos de inteligencia para realizarlos. Pero, asimismo, los Estados pueden ser objetivo de ciberataques que pueden complicar el funcionamiento de sus sociedades. La práctica nos revela que, en los últimos años, se han detectado ciberataques contra las infraestructuras críticas de Estados o contra objetivos muy concretos, pero igualmente estratégicos. Los delitos informáticos y los ciberatacantes han experimentado, sin duda, una tendencia creciente y han evolucionado en sus objetivos, organización, sofisticación, complejidad y coordinación[20]. Un caso especialmente conocido, que cabe recordar, fue el ataque a parte del ciberespacio de Estonia, en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico. Pero, la mayor parte de los incidentes de seguridad han tenido y tienen como consecuencia el robo de datos de usuarios, a pesar de las medidas de protección adoptadas por los sistemas.

20. Todo ello ha generado un incremento en la regulación civil y penal sobre los delitos en la Red, además de que se establezcan estándares y normativas de seguridad. Más allá, la guerra puede desarrollarse también hoy en parte en esta nueva dimensión espacial que es el ciberespacio. Hablaríamos entonces de la ciberguerra, un aspecto de la guerra que implica, entre otras cosas, «el sabotaje y bloqueo de sistemas, el robo de propiedad intelectual y las actividades de inteligencia sobre personas y proyectos»[21]. En la práctica, estaríamos ante un tipo de guerra con características nuevas y muy diferentes a la convencional, al desarrollarse también en lo que se considera el quinto terreno (el cibernético, junto a los ya tradicionales tierra, mar, aire y espacio)[22].

---

[19] Véase *http://tvpacifico.mx/portal/noticias_display/168117/estas-companias-fueron-afectadas-por-el-ciberataque*.

[20] *Estudio sobre la Cibercriminalidad en España*, Madrid, Ministerio del Interior, 2015, p. 42.

[21] «Cyber War: Definitions, Deterrence, and Foreign Policy», *Hearing Before The Committee On Foreign Affairs House of Representatives. First Session, September 30*, 2015, p. 12.

[22] Alejandro Suárez Sánchez-Ocaña llama al ciberespacio «el quinto elemento». En Suárez Sánchez-ocaña, A., *El quinto elemento: Espionaje, ciberguerra y terrorismo. Una amenaza real e inminente*,

Incluso, en ocasiones, podemos ver cómo una agresión militar convencional podría venir acompañada —en el antes o el después— de un ciberataque. En esta línea, el *Informe sobre Cibercriminalidad* de 2015 afirma que, durante ese año y 2014, el sector energético fue el más atacado por los ciberdelincuentes[23].

3. USO DE LAS TIC POR LOS ACTORES NO ESTATALES VIOLENTOS: CIBERTERRORISMO

21. Las TIC constituyen un medio, un fin o una combinación de ambos, utilizadas tanto por las organizaciones terroristas como por las delictivas para lograr sus objetivos. Las características de deslocalización, transnacionalidad, neutralidad y descentralización del ciberespacio favorecen al terrorismo que se adapta a dicha estructura, complicando la labor policial para combatirlo. De hecho, tanto los grupos terroristas como delincuenciales han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses y, en los últimos años, se han incrementado los delitos informáticos ejecutados por ambos grupos[24].

3.1. Ciberterrorismo y la complejidad de su definición

22. Está claro que las organizaciones terroristas son actores de carácter no estatal que aprovechan y se benefician de las vulnerabilidades tecnológicas, convirtiendo al ciberespacio en un nuevo campo de acción[25]. Eso explica que se acuñaran, coincidiendo con la aparición de Internet en los años ochenta, los términos de «ciberterrorismo» y «ciberdelincuencia». Ambas realidades son, hoy, verdaderas amenazas que conllevan la utilización de las TIC como herramientas clave para la realización de actividades de propaganda, comunicaciones internas, formación y adoctrinamiento, financiación, radicalización, reclutamiento y obtención de información, principalmente, por parte de los grupos terroristas delincuenciales.

Barcelona, Planeta, 2015. MOLINA, L., «Conflictos bélicos e internet», en FERNÁNDEZ, J. y SANSÓ-RUBERT, D. (eds.), *op. cit.*, nota 2, pp. 27-42; COLE, R. *et al.,* «Social engineering: the human element in information warfare CS4235a», *Information Warfare Group*; y HARTWING, R. P., *Cyber Risks. The Growing Threat*, Insurance Information Institute, 2013.

[23] *Estudio sobre la Cibercriminalidad...*, *op. cit.*, nota 20, p. 66. Mención especial merece el conocido como «Manual de Tallín», elaborado por un grupo de expertos independientes en el 2013, donde explican cómo aplicar las normas del Derecho internacional a las ya entonces llamadas guerras cibernéticas, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, 2.ª ed., Cambridge, Cambridge University Press, 2017. Otro estudio de gran relevancia es BOOTHBY, S. H., «Methods and Means of Cyber Warfare», *International Law Studies*, núm. 89.

En *https://www.usnwc.edu/getattachment/e14a7a47-a925-445c-8015-9a4ce67cce34/methods-and-means-of-cyber-warfare.aspx*.

[24] Se aprecia un «proceso progresivo de cambio de la ciberdelincuencia individual a la estructurada y organizada por grupos criminales»: véase *Estudio sobre la Cibercriminalidad..., op. cit.*, nota 20.

[25] Véase por su interés con el tema que se aborda TORRES SORIANO, M. R., «Cómo contener a un Califato virtual», *Cuadernos de Estrategia*, 2016, núm. 180, pp. 167-194.

23. No existe, sin embargo, una definición universalmente aceptada del «ciberterrorismo» ni, tan siquiera, una aproximación conceptual que haya conseguido el suficiente consenso en la comunidad internacional, aunque desde los años ochenta se han formulado varias definiciones doctrinales e institucionales de esta realidad. En particular, tras los atentados terroristas del 11-S, la Unión Europea (UE) definió el ciberterrorismo como «el empleo de las TIC, por parte de grupos terroristas, para la consecución de sus objetivos; utilizando Internet como instrumento de comisión del delito o como acción del delito»[26]. Esto implica el uso de las TIC como instrumento de apoyo a los objetivos terroristas, así como herramienta de ataque directo a infraestructuras críticas. En verdad, las TIC no se presentan como un método de ataque sino, en concreto, como un arma para magnificar los atentados terroristas, difundir el terror entre la comunidad internacional, reclutar e incluso formar y financiar[27].

24. Desde la perspectiva doctrinal, merece la pena reseñar que, algunos autores han señalado que el ciberterrorismo es «la convergencia entre el terrorismo y el ciberespacio: una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logra intimidar o presionar a un Estado y sus ciudadanos»[28]. En otras palabras, el ciberterrorismo es una actividad terrorista que se ejecuta en el mundo virtual, en el ciberespacio. Pero, aunque no se haya alcanzado una definición aceptada en la práctica internacional, sí podemos determinar el contenido de lo que se entiende por ciberterrorismo en el orden internacional. Así, podemos comprobar cómo, en los últimos tiempos, se procede a la detención de presuntos miembros de ISIS por realizar labores íntegramente en el ciberespacio, alentando el reclutamiento de nuevos miembros entre sus contactos y seguidores, así como incitando a la comisión de actos terroristas de cualquier índole en nombre de ISIS[29].

25. Conscientes de esta realidad, los terroristas prestan cada vez más atención a la seguridad y utilizan medios más complejos. El dominio informático es clave para estos grupos, ya que pueden actuar desde cualquier punto del planeta y establecer una red terrorista «virtual»[30]. En ocasiones, su

---

[26] Propuesta de Decisión Marco del Consejo, relativa a los ataques de los que son objeto los sistemas de información, de 19 de abril de 2002 [COM (2002) 173 final].

[27] Véase Dogrul, M., Aslan, A. y Celik, E., «Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism», en *3rd International Conference on Cyber Conflict*, 2011, p. 32.

[28] Dennis, D. E., *Information Warfare and Security*, Addison Wesley, 1998; y Cavaller, V., Cano, J. y Sabillon, R., «Cibercrimen y ciberterrorismo: dos amenazas emergentes en un contexto global», en Velasco, F., Navarro, D. y Arcos, R. (eds.), *La Inteligencia como disciplina científica*, Madrid, Plaza y Valdés, 2010, p. 505.

[29] En 2015, el Gobierno español elevó a cuatro el nivel de alerta antiterrorista. El Ministerio del Interior puso en marcha la iniciativa *Stop Radicalismos*, a través de la cual los ciudadanos pueden proporcionar de forma confidencial y segura información sobre casos de radicalización en su entorno. En *http://politica.elpais.com/politica/2017/02/07/actualidad/1486454847_476862.html*.

[30] Heisbourg, F., *Hiperterrorismo, la nueva guerra*, Colombia, Espasa, 2003, p. 135. Véase por su interés científico el artículo del Prof. Jiménez García, F., titulado «Combatientes terroristas extranjeros

preocupación por la seguridad queda patente por el uso de numerosas líneas telefónicas utilizando identidades falsas. No obstante, el uso de los servicios de indización, como los buscadores de Internet, también hace que sea más fácil descubrir y obtener contenido relacionado con el terrorismo [31]. Por tanto, para los diferentes grupos terroristas que actúan en la sociedad internacional, Internet y en definitiva las TIC, se han convertido en un «arma» esencial para el desarrollo de su estrategia terrorista.

26. Con ello, el terrorista dirige su mirada, en la actualidad, al ciberespacio al que ha convertido en un nuevo campo de acción. Sabedor de los daños enormes que puede causar, utiliza las TIC, no tanto para perpetrar delitos graves, como ya hemos dicho, sino para llevar a cabo actividades de apoyo como, por ejemplo, expandir su mensaje, multiplicar el terror psicológico, captar a jóvenes interesados en adherirse a su causa y formar a individuos que se encuentran en diferentes lugares para que se conviertan en combatientes de la *yihad global*. El ciberterrorismo persigue crear terror en el ciberespacio para luego plasmar sus objetivos en el mundo real.

27. El uso del ciberespacio brinda numerosos beneficios a las organizaciones terroristas [32], aunque también recibe muchas críticas. Así, Daniel Sansó-Rubert considera como «manifestaciones exageradas» las amenazas sobre el ciberterrorismo y afirma que expandir el miedo sobre el ciberterrorismo «es una forma de ganar apoyo político para la sanción de leyes, que otorguen mayor discrecionalidad a los organismos de seguridad al amparo de la lucha antiterrorista» [33]. Queda claro, entonces, que detrás de esto hay intereses de sectores tanto públicos como privados. A pesar de todo, no se puede obviar que el ciberterrorismo es una amenaza y que no todo es producto de estrategias e intereses.

3.2. Los fines de las TIC por parte de los Grupos Terroristas Yihadistas

28. El examen del uso específico que las diferentes organizaciones terroristas hacen de las TIC, nos permite perfilar los fines que estas organizaciones persiguen con el empleo de las TIC. Sobre esta base podemos subrayar lo siguiente.

29. En primer lugar, uno de los principales usos de las TIC por las organizaciones terroristas es la difusión de propaganda. Esta puede incluir contenidos como comunicaciones de audio e imágenes de vídeo de actos de violencia, presentaciones en las que los terroristas imparten instrucción ideo-

---

y conflictos armados: utilitarismo inmediato ante fenómenos no resueltos y normas no consensuadas», *REDI*, vol. 68, 2016, núm. 2, pp. 277-301.

[31] «IOCTA 2015, Internet Organized Crime Threat Assessment», European Police Office, 2015.

[32] Heisbourg, F., *op. cit.*, nota 30, p. 134.

[33] Sansó-Rubert, D., *op. cit.*, nota 18, pp. 73-74.

lógica, explican, justifican, muestran su estilo de vida, proyectando siempre una imagen idealizada y atractiva; y alientan al usuario a unirse a su causa. Como señala Javier Jordán, «la propaganda que se distribuye a través de esas comunidades virtuales transmite elementos racionales, emocionales y cognitivo-normativos y dicha comunicación pública refuerza los valores y convicciones del imaginario yihadista y justifica las conductas transgresoras, permitiendo que los procesos de radicalización sean en algunos casos de carácter autodidacta» [34].

30. Todos los contenidos expuestos y reflejados pueden distribuirse usando una «amplia gama de herramientas, tales como sitios *web* protegidos por contraseña, salas de charlas y foros de acceso restringido, revistas en línea» [35]. En particular, *Twitter* se presenta como la gran protagonista y un canal privilegiado [36]. Como menciona Carlos Suárez-Mira Rodríguez, el terrorismo ha encontrado en la Red «un prodigioso instrumento de propagación y ejecución» [37]. Más aún, de tal modo es así que se ha podido decir que hasta el 60 por 100 de los terroristas detenidos en 2004 y 2010 manifestaron haber utilizado Internet y las redes sociales en su proceso de radicalización. Es probable que esta cifra haya aumentado desde entonces.

31. Por ello, conviene distinguir entre la mera propaganda y el material destinado a incitar a otros a cometer actos de terrorismo. En los Estados occidentales se considera que el uso de propaganda con el fin de incitar a otros a cometer actos de terrorismo es punible y perseguible [38]. Más allá, los contraargumentos y otras comunicaciones estratégicas pueden ser un medio eficaz de desbaratar el proceso de radicalización e inculcación de ideales extremistas, que a su vez pueden manifestarse en actos de terrorismo. Por ello, desde distintos ámbitos se aboga por el uso de estrategias que contrarresten la propaganda terrorista vía *online* a través de programas dirigidos a prevenir la radicalización. En esta dirección, podemos mencionar, en la práctica española, el *Plan Estratégico Nacional de Lucha contra la Radicalización Violenta*, elaborado por el Ministerio del Interior Español.

32. En segundo lugar, el terrorismo yihadista utiliza el ciberespacio como su campo de acción o plataforma para el reclutamiento. A través de la

---

[34] Jordán, J., «Proceso de radicalización yihadista en España. Análisis sociopolítico en tres niveles», *Revista de Psicología Social*, vol. 24, 2009, núm. 2, pp. 197-216.

[35] Weimann, G., *Terror on the Internet: The new challenges*, Washington D. C., Instituto de la Paz de los Estados Unidos, 2006, pp. 37-38; y Barranco, D., «Los *Community* manager del terror. La propaganda *online* de ISIS y su ofensiva sobre Iraq», *Instituto de Estudios Estratégicos*, 2014.

[36] Berger, J. M., «The ISIS Twitter census defining and describing the population of ISIS supporters on Twitter», Brookings, 2015.

[37] Suárez-Mira Rodríguez, C., «Internet y el Derecho Penal: Viejos y nuevos delitos», en Fernández Rodríguez, J. J. (dir.), *Internet, un nuevo horizonte para la Seguridad y la Defensa*, Santiago de Compostela, Servicio de Publicaciones de Intercambio Científico de la Universidad de Santiago de Compostela, 2010, p. 122.

[38] Según un estudio realizado por Oliver Roy, «la mayor parte de los sitios *webs* de contenido proselitista vinculado a organizaciones terroristas yihadistas no provienen del mundo musulmán, sino que están alojados en países anglosajones»: véase Sansó-Rubert, D., *op. cit.*, nota 18, p. 63.

Red los terroristas pueden reclutar y entrenar a nuevos miembros, comunicarse entre ellos, transmitir información sobre planes de actos terroristas, investigar o reconocer blancos potenciales. Todo ello a un coste mínimo, y valiéndose de las características propias que ofrece Internet: inmediatez, accesibilidad global y anonimato[39]. Las redes sociales son fundamentales para grupos como ISIS y, en concreto, los ciberforos de acceso restringido ofrecen a los potenciales reclutas «un lugar para enterarse de la existencia de organizaciones terroristas y prestarles apoyo, así como para participar en acciones directas en pos de objetivos terroristas»[40]. Así lo ha expresado Naciones Unidas en diferentes informes y resoluciones, desde principios del siglo XXI, en los que señala expresamente la importancia de la lucha contra el uso terrorista de Internet como elemento clave de una amplia estrategia contra el terrorismo[41]. En esta línea, algunas resoluciones del Consejo de Seguridad (CS), inciden en esta cuestión, entre las que destaca la Resolución 1963 (2010)[42].

33. En tercer lugar, las organizaciones terroristas como *Al Qaeda* o *ISIS* utilizan, cada vez más, a las TIC como campamentos de entrenamiento virtuales y adiestramiento. Se ha dicho, con razón, que «hay una gama cada vez mayor de medios de comunicación que proporcionan plataformas para la difusión de guías prácticas en forma de manuales en línea, ficheros de audio y vídeo, materiales de información y asesoramiento»[43]. Estas páginas *webs* ofrecen, también, conocimientos e instrucciones sobre temas como la forma de «fabricar explosivos, cómo realizar secuestros, utilizar armas de fuego, métodos para no ser detenidos, cómo planear y ejecutar ataques terroristas». Recordemos que *Inspire*, como ejemplo destacado, fue una revista en línea supuestamente publicada por *Al-Qaeda en la Península Arábiga,* con el objetivo declarado de permitir a los musulmanes entrenarse para la *yihad* en su casa[44].

34. Por último, según Naciones Unidas, otra de las funciones que cumple la Red para los grupos terroristas y las nuevas tecnologías es la relativa a la financiación. Por ejemplo, ISIS utiliza Internet para financiar actos de te-

---

[39] Véase GERWEHR, S. y DALY, S., «Al Qaida: terrorist selection and recruitment», en KAMIEN, D. (ed.), *The McGraw-Hill Homeland Security Handbook*, Nueva York, McGraw Hill, 2006, p. 83; Grupo de Expertos en materia de radicalización violenta de la Comisión Europea, «Radicalization processes leading to acts of terrorism», 2008; y en *www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf*.

[40] KOHLMAN, E. F., «The real online terrorist threat», *Foreing Affairs*, vol. 85, 2006; KOHLMAN, E. F., «Al Qaida's My Space Terrorist recruitmenon the Internet», *CTC Sentinel*, vol. 1, 2008, pp. 8-9; y GOHEL, S. M., «The Internet and its role in terrorist recruitment and operational planning», *CTC Sentinel*, vol. 2, 2009, pp. 12-15.

[41] Resolución 60/825 de la Asamblea General, «Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo», Informe del Secretario General, de 27 de abril de 2006, párr. 38.

[42] S/RES/1963 (2010).

[43] *The use of the Internet for terrorist purposes*, Nueva York, Publicaciones de las Naciones Unidas, 2012, p. 8.

[44] *Ibid.*, p. 8. Véase CONWAY, M., «Terrorist "use" of the Internet and fighting back», *Information & Security*, vol. 19, 2006, pp. 12-14.

rrorismo. La recaudación de fondos y recursos «puede clasificarse en cuatro categorías: la recaudación directa, el comercio electrónico, el empleo de los servicios de pago en línea y las contribuciones a organizaciones benéficas»[45]. La recaudación directa se lleva a cabo utilizando métodos como el «*crowfunding*» y a través de salas de charla, páginas *web* y redes sociales o mensajes dirigidos a simpatizantes solicitando donaciones. El comprador puede realizar el pago a través de transferencia bancaria electrónica, una vía que permiten algunas plataformas de comunicación y páginas *web*, o a través de tarjeta de crédito u otro tipo de procedimientos de pago ofrecidos por *Skype* o *Pay Pal*[46].

35. En suma, la práctica internacional nos revela la trascendencia de las TIC como vehículo, al menos, de proselitismo, información, reclutamiento y financiación por parte de los terroristas. Para contrarrestarlo se precisa de la acción coordinada y conjunta de toda la comunidad internacional, respetando, eso sí, los derechos humanos, y siempre en consonancia con las obligaciones contraídas en virtud del DI[47]. Pero, los grupos terroristas saben que el ciberespacio les puede pasar factura ya que sus mensajes, publicados a través de las TIC, pueden ser rastreados por los servicios de inteligencia y de la policía, y facilitar su detención[48].

4. RESPUESTA POLÍTICO-JURÍDICA AL DESAFÍO DEL CIBERTERRORISMO

36. Los Estados están obligados a articular un sistema nacional de «ciberseguridad» que gestione, con eficacia, los riesgos que amenazan el ciberespacio. El fortalecimiento de la «ciberseguridad» proporciona a las Administraciones públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general, una mayor confianza en el uso de las TIC. Por ello, los organismos públicos responsables reconocen la importancia que tiene trabajar en coordinación con el sector privado y con los propios ciudadanos, para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información. Ahora bien, el logro de un ciberespacio más seguro y fiable solamente es posible mediante el refuerzo de la colaboración y la cooperación internacionales, creando relaciones de confianza, sobre todo entre los Estados, para el intercambio de información y de los datos esenciales en materia de «ciberseguridad».

---

[45] *The use of the Internet...*, *op. cit.*, nota 43, p. 7.

[46] Véase Informe del Secretario General sobre «la amenaza que plantea ISIS para la paz y la seguridad internacionales y las actividades que realizan las Naciones Unidas en apoyo de los Estados para combatir la amenaza», S/2016/92.

[47] Martín Martínez, M., «Terrorismo y Derechos Humanos en la UE y en el Consejo de Europa: ¿Marco de Referencia Mundial?», en *Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz*, Bilbao, Publicaciones de la Universidad del País Vasco, 2009, *passim*.

[48] «Investigations Involving the Internet and Computer Network», Instituto Nacional de Justicia, p. 10.

37. Por ello, se han adoptado instrumentos de carácter internacional en la lucha contra el terrorismo en los que, en algunos casos, se contienen mecanismos amplios para la cooperación internacional en los procesos penales relacionados con el terrorismo. Estos instrumentos prevén figuras como la extradición, la asistencia judicial recíproca, la ejecución recíproca de sentencias, la remisión de actuaciones penales y el traslado de las personas condenadas o el intercambio de información entre los organismos encargados de hacer cumplir la ley[49]. Pero junto a estos avances, en el ámbito normativo, Naciones Unidas desempeña un papel fundamental impulsando el intercambio de información y las buenas prácticas entre los Estados e intentando, al mismo tiempo, tejer un consenso sobre enfoques comunes para combatir el uso de las TIC por el terrorismo[50]. Con este objetivo, precisamente, se elaboró la *Estrategia Global de las Naciones Unidas contra el terrorismo*, adoptada por la Asamblea General en su Resolución 60/288, en 2006[51].

4.1. Principales instrumentos y políticas contra el ciberterrorismo

38. En la lucha contra el ciberterrorismo los Estados aplican políticas antiterroristas de «infiltración y monitorización», dirigidas por los centros de inteligencia y agencias policiales, con el fin de prevenir posibles atentados terroristas y obtener pruebas que ayuden en la instrucción judicial; y, también, llevan a cabo las políticas contraterroristas dirigidas a la creación de cuerpos e instituciones especializadas. En este sentido, en España destaca el *Mando Conjunto de Ciberdefensa* (MCCD) o la *Oficina de Coordinación Cibernética* (OCC), creada en 2014, que es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad. Podemos recordar, también, que en los Estados Unidos se han creado varios centros como el *US Cyber Threat Intelligence Integration Center* (CTIIC).

39. En el marco de la UE se puso en marcha, el 11 de enero de 2013, el *Centro Europeo sobre la Cibercriminalidad (EC3)*. Este Centro representa a la comunidad policial de la UE en áreas de interés común: requerimientos, gobernanza de Internet y desarrollos legislativos; y está ubicado en las dependencias de Europol. En particular, el EC3 orienta su trabajo contra la criminalidad cometida por grupos organizados, en especial aquellos que generan importantes beneficios procedentes de actividades ilícitas, como el fraude *online*[52]. Además,

---

[49] *International Cooperation in criminal matters: Counter-terrorism*, United Nations Office on Drugs and Crime, 2013, *passim*.

[50] En *http://www.unodc.org/documents/terrorism/Publications/FAQ/Spanish.pdf*.

[51] A/RES/60/288. El Quinto Examen de la Estrategia Global de las Naciones Unidas contra el terrorismo se realizó el 1 de julio de 2016.

[52] Ya en 2004, la UE creo la Agencia Europea de Seguridad de las Redes y de la Información (ENISA): véase *DO* L núm. 77, de 13 de marzo de 2004. En 2013 se aprobó el Reglamento (UE) núm. 526/2013, del Parlamento Europeo y del Consejo, de 21 de mayo, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) núm. 460/2004 (*DO* L núm. 165, de 18 de junio de 2013).

se ha aprobado la *Agenda Europea de Seguridad (2015-2020*), un instrumento que establece las bases para la cooperación y acción conjunta de la Unión Europea en relación con la seguridad[53]. Esta Agenda establece prioridades como la lucha contra el terrorismo y prevenir la radicalización. En clara relación con estos objetivos, se enmarcan el *Programa Europeo de protección de Infraestructuras Críticas y el Programa de protección de Infraestructuras TIC*[54]. El examen de estos programas nos revela que se contemplan acciones que están básicamente destinadas hacia la prevención de la amenaza. Entre estas acciones, destacan «los ciber ejercicios de adiestramiento que realiza la UE, tanto a nivel continental como con EEUU»[55].

40. Además de estos instrumentos, políticas e iniciativas, debemos destacar cómo algunos Estados, entre ellos Francia, Reino Unido, Alemania, España, los Estados Unidos, Israel, Corea del Sur; y organismos internacionales como la OTAN, ONU y la UE, han aprobado sus propias estrategias nacionales o específicas de ciberseguridad, es decir, han adoptado «marcos normativos, planes y estrategias concretas para la defensa del ciberespacio». El objetivo central de estos instrumentos no es otro que dar respuesta al reto de preservar el ciberespacio y, con ello, expresar de forma objetiva la voluntad política de los Gobiernos y de los organismos internacionales más comprometidos con la ciberseguridad.

41. En España se aprobó *la Estrategia de Ciberseguridad Nacional* de 2013[56], cuyo objetivo es lograr que se haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las «capacidades de prevención, detección, reacción, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques»[57] porque, precisamente, a este fin debe servir la Política de Ciberseguridad Nacional. Además, el documento nos ofrece un marco normativo que regula el ciberespacio y su seguridad.

42. También la UE elaboró la *Estrategia de Ciberseguridad,* en 2008, donde se establecen los activos que hay que proteger, haciendo hincapié en la protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad. Desde la óptica de la UE en la lucha contra el terrorismo, el respeto por los derechos humanos y el Estado de Derecho son parte integrante, puesto que el Estado de Derecho debe protegernos pero, también, debe estar sometido a controles para evitar abusos de poder. En este sentido, el desarrollo y la aplicación de leyes que penalizan la incitación a cometer actos de terrorismo, sin dejar por ello de proteger derechos humanos como

---

[53] *Estudio sobre la Cibercriminalidad...*, *op. cit.*, nota 20, p. 22.

[54] Véase en *http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al33260.*

[55] Olvera Gorts, M., «Ciberterrorismo: la respuesta de la Unión Europea en el ámbito de las infraestructuras críticas», *Red SAFE WORLD*, 2011, en *http://www.belt.es/imagenes/ciberterrorismo-monica-olvera.pdf*.

[56] En *http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.* Caro Bejarano, M. J., «Estrategia de Ciberseguridad Nacional», *Documento de Análisis del Instituto Español de Estudios Estratégicos*, 2013, núm. 65.

[57] De Salvador Carrasco, L., «Los problemas estructurales en el planteamiento de la Ciberseguridad», *Documento Marco del Instituto Español de Estudios Estratégicos*, 2014, núm. 9, p. 7.

es la libertad de expresión, entre otros, presentan un reto constante para los encargados de formular políticas, los juristas, y en general los responsables de hacer cumplir la ley[58].

43. En relación con la UE, conviene destacar, asimismo, la aprobación de varias Comunicaciones presentadas a principios del segundo decenio del siglo XXI. Entre ellas, la Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 22 de noviembre de 2010, en la que se proponen cinco objetivos estratégicos a lograr entre 2011 y 2014, con sus correspondientes líneas de acción, siendo los más destacables: prevenir el terrorismo y abordar su captación. También, recordemos la Comunicación de la Comisión al Parlamento Europeo, de 30 de marzo de 2009, sobre protección de infraestructuras críticas de información, titulada: «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia». Y, por último, la Comunicación, de 31 de marzo de 2011, sobre la protección de infraestructuras críticas de información, titulada: «Logros y próximas etapas: hacia la ciberseguridad global», en la que se nos ofrece y facilita una clasificación de la amenaza cibernética así como los logros conseguidos en este campo[59]. Por tanto, la UE ha hecho notables esfuerzos en la lucha contra el terrorismo y la delincuencia informática que se traducen, en esencia, en la definición de una terminología común al respecto, creando un marco de referencia compartido que facilita la defensa ante el ciberterrorismo y la persecución de los delitos de ciberdelincuencia. Sin embargo, no existe una estrategia integral europea específica en materia de «ciberseguridad».

44. En relación con la OTAN, esta organización lleva organizando congresos de ciberseguridad desde comienzos del siglo XXI y en la Cumbre de Praga, en 2002, decidió aplicar un programa global de coordinación de la ciberdefensa y diseñar un sistema de protección defensivo contra ataques informáticos. No obstante, la OTAN se enfrentó con el problema de manera evidente en la Cumbre de Bucarest de 2008 en la que declara que: «Se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciberataques». Ese mismo año el Consejo del Atlántico Norte firma la «Política de Ciberdefensa de la OTAN», con el objetivo de mejorar su sistema defensivo contra ciberataques. Por entonces, ya había tenido lugar el ataque informático contra Estonia, verdadero hecho impulsor en la decisión de la OTAN de definir un nuevo concepto estratégico de política de ciberdefensa. El último impulso en este ámbito se producía en la Cumbre de Varsovia de diciembre de 2016, en la que la Alianza reconocía al ciberespacio como el quinto dominio de las operaciones militares[60].

---

[58] En la *Estrategia global de las Naciones Unidas contra el terrorismo*, A/RES/60/288, se afirma que las «medidas eficaces contra el terrorismo y la protección de los derechos humanos no son objetivos contrapuestos, sino que se complementan y refuerzan mutuamente».

[59] OLVERA GORTS, M., *op. cit.*, nota 55. Véase «Código de Derecho de la Ciberseguridad», Instituto Nacional de Seguridad, 2016, *passim*.

[60] Véase al respecto, *http://www.nato.int/cps/en/natohq/official_texts_133169.htm*. GANUZA ARTILES, N., «La situación de la ciberseguridad en el ámbito internacional y en la OTAN», en *Ciberseguridad:*

4.2. La incompleta acción judicial de carácter estatal contra el ciberterrorismo

45. En el ciberespacio resulta clave detectar, investigar y perseguir las actividades terroristas y delictivas que tienen lugar, sobre la base de un marco jurídico y operativo eficaz. El uso de las TIC por estos grupos criminales es un problema transnacional que requiere una respuesta integrada a través de las fronteras y, por ello, exige una plena cooperación entre los distintos sistemas nacionales de justicia penal. Ahora bien, la particularidad del medio donde llevan a cabo sus actividades los ciberterroristas, «rompe los esquemas de investigación y enjuiciamiento conocidos, ya que el cibercrimen no tiene fronteras, por lo que el principio de territorialidad del Derecho pierde parte de su significado» [61]. Desde el punto de vista jurídico, las TIC han dado lugar a la aparición de nuevas formas de comisión delictiva.

46. Naciones Unidas ha dejado claro, en los instrumentos político-jurídicos que ha adoptado, que una respuesta eficaz de la justicia penal a las amenazas que plantea el uso de las tecnologías de la información y de la comunicación por los diferentes grupos terroristas precisa que los Estados establezcan políticas y leyes nacionales objetivas dirigidas, fundamentalmente, al logro de los siguientes objetivos: «*a)* la penalización de los actos ilícitos cometidos por terroristas a través de Internet o servicios conexos; *b)* el otorgamiento de facultades especiales de investigación a los organismos de seguridad encargados de las investigaciones relacionadas con el terrorismo; *c)* la regulación de los servicios relacionados con Internet [...] y el control del contenido; *d)* la facilitación de la cooperación internacional; *e)* el desarrollo de procedimientos especializados judiciales o probatorios, y *f)* la observancia de las normas internacionales de derechos humanos» [62]. Sin embargo, hasta principios del siglo XXI, no existía una legislación específica sobre esta cuestión y las normas que se habían adoptado por ciertos países, sobre todo europeos, se caracterizaban por su fragmentación y dispersión, por su amplitud a la hora de interpretarlas y siempre con el objetivo expreso de no perjudicar otros derechos fundamentales como la libertad de expresión. No obstante, los Estados se han visto en la obligación de adoptar normas específicas sobre esta materia.

47. En relación con la elaboración de legislación antiterrorista específicamente destinada a combatir el uso de Internet por los terroristas, tan solo un número limitado de Estados se han ocupado de esta cuestión, y, además, no existe ningún instrumento de alcance universal contra el terrorismo que imponga a los Estados la obligación de promulgar leyes dirigidas contra la

---

Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, *Cuadernos de Estrategia*, 2010, núm. 149, pp. 167-214; y MOLINER GONZÁLEZ, J., «La Cumbre de la OTAN en Varsovia», *Documento de Opinión del Instituto Español de Estudios Estratégicos*, 2016, núm. 79 bis.

[61] A/RES/69/28.

[62] *Ibid.*, p. 29.

utilización de Internet por parte de los terroristas[63]. Por ello, es conveniente que los Estados elaboren una legislación, lo más completa posible, que ofrezca a las autoridades la base jurídica suficiente para hacer efectiva la cooperación internacional con otros Estados, sobre todo en las investigaciones relacionadas con el terrorismo transnacional, y que se adopten normas internas con las figuras delictivas necesarias para satisfacer los requisitos de la doble incriminación.

48. Son algunos Estados europeos los que han sufrido directamente la lacra terrorista y, por tanto, los que más se han preocupado por adoptar normas de este tipo. Así, por ejemplo, el Reino Unido aprobó, en el último decenio, diversas normas destinadas a combatir el uso de Internet con fines terroristas. En concreto, después de los atentados de 2005 en Londres, el Gobierno británico aprobó la *Ley de Terrorismo* de 2006, que contiene disposiciones que tratan específicamente de la actividad basada en Internet que puede alentar o facilitar la comisión de actos de terrorismo. Esta ley complementa la *Ley de uso indebido de computadoras* de 1990 que trata, en particular, de delitos cometidos a través de la Red y de la «ciberdelincuencia» en general. Cabe destacar, también, que el art. 59 de la *Ley de Terrorismo* de 2000 tipifica «el acto de incitar a otra persona a cometer un acto de terrorismo, en todo o en parte, fuera del Reino Unido»[64], lo que nos remite a situaciones que quedan cubiertas en los supuestos de delitos cometidos en el ciberespacio.

49. Por lo que se refiere a España destacan, sin duda, las Leyes Orgánicas 1/2015 y 2/2015, que regulan nuevos tipos penales en el ámbito de la cibercriminalidad, como son, en particular, los delitos de descubrimiento y revelación de secretos, de daños informáticos, de pornografía infantil, los delitos contra la propiedad intelectual, de terrorismo y los delitos de odio. Este avance legislativo, con el objeto de dar respuesta a la nueva fenomenología criminal, viene dado, entre otras cosas, por la adopción de la Directiva Europea 2013/40/UE, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información, y por la que se sustituyó la Decisión Marco 2005/222/JAI del Consejo. Por tanto, la legislación española, con base en parte, también, en la normativa de la UE, nos aporta un marco, aunque quizá insuficiente, para combatir la cibercriminalidad[65]. En resumen, no es fácil encontrar, en la práctica de los Estados, un marco jurídico completo que permita una acción judicial eficaz.

---

[63] Véase Conway, M., «Terrorism and Internet governance: core issues», *Disarmament Forum*, vol. 3, 2007, p. 27.

[64] Renieris, E. M., «Combating incitement to terrorism on the Internet», *op. cit.*, pp. 682-683.

[65] Ahora bien, junto a estas modificaciones del Código Penal sobre la cibercriminalidad, hay que señalar, también, que nuestro país ha ratificado el Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, adoptado en Estrasburgo en 2003, y que entró en vigor en España el abril de 2015: véase *Estudio sobre la Cibercriminalidad en España...*, *op. cit.*, nota 20, p. 4.

4.3. Regulación de los cibercafés y otros lugares: carencias y obstáculos

50. Los terroristas se han servido de cibercafés, en algunos casos, para llevar a cabo actos relacionados con el terrorismo. No hay datos precisos sobre la proporción de este tipo de actividad en relación con las actividades realizadas legítimamente y las que no lo son a través de estos servicios de Internet. Precisamente por ello, «la investigación de los casos de terrorismo con uso de Internet u otros servicios conexos por presuntos terroristas suele exigir la realización de actividades intrusivas o coercitivas de registro, vigilancia o monitorización por los servicios de inteligencia o los organismos encargados de hacer cumplir la ley» [66].

51. No obstante, para que las autoridades emprendan ese tipo de actividades necesitan de la cooperación de los proveedores de servicios públicos de telecomunicaciones o servicios conexos. Por ello, los Estados deben ofrecer una base jurídica que incida de forma evidente sobre las obligaciones de las partes del sector privado [67], en la que se indique cuál es el plazo aplicable, si lo hubiere, durante el cual los proveedores deben retener los datos en su poder. Además, sería conveniente que las autoridades se pusieran en contacto con sus homólogos del país en el que se encuentran los datos y adoptasen las medidas (tanto oficiales como oficiosas) necesarias para garantizar la conservación de los datos para su posible entrega [68].

52. El problema, en la actualidad, tiene que ver con que muchos Estados no han legislado sobre esta cuestión, con lo que no existen normas ni se han establecido obligaciones aceptadas universalmente para los proveedores de servicios de Internet y para otros proveedores de comunicaciones, en relación con la retención de datos de Internet, claves en las investigaciones penales. La infraestructura de las redes de servicios de Internet suele ser propiedad, en su totalidad o en parte, de entidades privadas, y, asimismo, son empresas privadas generalmente los propietarios de las plataformas de medios sociales, quienes facilitan la difusión de contenidos generados por los usuarios a un público más amplio, así como los «populares» buscadores de Internet que seleccionan el contenido en función de los criterios proporcionados por el usuario [69].

53. En el plano internacional existen distintos enfoques. En algunos Estados, como Egipto, India, Jordania y Pakistán, los Gobiernos aplican medi-

---

[66] *The use of the Internet...*, *op. cit.*, nota 43, p. 44.

[67] A nivel internacional, y en clara relación con lo mencionado, destaca la iniciativa contra el ciberterrorismo denominada *Alianza Internacional Multilateral contra el Ciberterrorismo* (IMPACT por sus siglas en inglés *http://www.impact-alliance.org/*), integrada por empresas y Gobiernos de varias regiones del planeta y cuyo objetivo no solo es combatir el ciberterrorismo sino también los delitos y amenazas que se dan en el ciberespacio.

[68] Véase *http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52007DC0649*.

[69] Los tres métodos principales para limitar el impacto de tales comunicaciones consisten en controlar el acceso a la infraestructura de la red, censurar el contenido de Internet o una combinación de ambos. Conway, M., *op. cit.,* nota 63, p. 26.

das legislativas o reglamentarias concretas que obligan a los operadores de cibercafés a obtener, retener y, previa solicitud, entregar una identificación de los clientes a los organismos encargados de hacer cumplir la ley[70]. Por tanto, algunos Gobiernos han impuesto obligaciones específicas a los operadores de los cibercafés, obligando a los proveedores de servicios de Internet a retener, por ley, ciertos tipos de datos relacionados con comunicaciones durante un plazo determinado; con el fin de poder obtener, conservar y, previa solicitud, presentar a la Policía identificación fotográfica, domicilio y datos de uso, y conexión de los clientes. La utilidad de esas medidas es cuestionable y no suele ser tan eficaz por diversas razones. Entre ellas, por el largo tiempo que precisan los procedimientos tradicionales de asistencia judicial recíproca en casos transnacionales y, sobre todo, porque hay otros servicios de Internet a disposición del público, por ejemplo, los ordenadores de las bibliotecas públicas o locales públicos con conexión inalámbrica a Internet (WiFi), que ofrecen oportunidades similares para el uso anónimo de Internet por terroristas.

54. Podemos recordar, que, en 2007, los Emiratos Árabes Unidos aprobaron leyes cibernéticas federales que, además de penalizar la piratería y otras actividades relacionadas con Internet, penalizaron, también, la creación de sitios *web* o la publicación de información para grupos terroristas con nombres falsos con la intención de facilitar la comunicación entre ellos y sus dirigentes, difundir sus ideologías, financiar sus actividades o informar sobre cómo fabricar explosivos. Tan solo un año después, el Gobierno de Arabia Saudí, en la misma línea, promulgó una ley que tipifica como delito poseer un sitio *web* que promueva o apoye el terrorismo[71].

55. En el ámbito de la UE, sí ha habido intentos por parte de algunos Estados de adoptar una legislación precisa por la que se exija a los proveedores de servicios de telecomunicaciones que capturen y archiven de forma automática los datos de las comunicaciones de sus usuarios. Así, el Gobierno de Italia impuso, en 2005, obligaciones reglamentarias a los operadores de los cibercafés respecto de la identificación de los clientes; sin embargo, esta reglamentación fue derogada a finales de 2010, en parte, para evitar críticas de los usuarios. También, en 2006, Francia adoptó varias normas contra el terrorismo que facilitan, a los efectos de las investigaciones, el control de las comunicaciones y el acceso de las fuerzas policiales a los datos de comunicaciones de los cibercafés, proveedores de servicios en Red y compañías telefónicas[72].

56. Pero resulta de mayor interés anotar que, ese mismo año, impulsada en parte por los ataques terroristas que se habían producido en Madrid y en

---

[70] MANTEL, B., «Terrorism and the Internet: should web sites that promote terrorism be shut down?», *CQ Global Researcher*, vol. 3, 2009, núm. 11; y THEOHARY, C. A. y ROLLINS, J., «Terrorist use of the Internet: information operations in cyberspace», *Congressional Research Service report*, 2011, p. 8.

[71] El delito puede ser castigado con multa y hasta diez años de prisión: véase WESTLEY, D., «Saudi tightens grip on Internet use», *Arabian Business*, 2008.

[72] FERNÁNDEZ PINÓS, J. E., «Cuestiones procesales relativas a la investigación y persecución de conductas delictivas en Internet», en *http://www.uoc.edu/in3/dt/20063/index.html*.

Londres[73], la UE adoptó una Directiva sobre la retención obligatoria de los datos de tráfico de las comunicaciones. En particular, se trataba de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de la Unión Europea, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[74]. Esta Directiva obligaba a los Estados miembros a adoptar una legislación que exija a los proveedores de telecomunicaciones retener determinados datos de tráfico, relativos a las comunicaciones electrónicas durante un periodo de entre seis meses y dos años, debiéndose poner estos datos «a disposición policial»[75].

57. Por tanto, la Directiva 2006/24/CE tenía por objeto principal armonizar las obligaciones mínimas de retención de datos. Sin embargo, esta Directiva, que reconocía explícitamente las dificultades que producen las diferencias legales y técnicas entre las disposiciones nacionales relativas a los tipos de datos que deben retenerse, así como en cuanto a las condiciones y los periodos de retención de los datos, quedó anulada por la Sentencia dictada por la Gran Sala del Tribunal de Justicia de la Unión Europea (TJUE), el 8 de abril de 2014[76]. Como señala Francisco Jiménez García, esta sentencia «reitera que la normativa sobre conservación de datos debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal»[77]. En la actualidad existen diferencias, en el ámbito europeo, en cuanto al tiempo durante el cual, los proveedores de servicios de Internet que operan en el espacio europeo, retienen los datos.

58. Conviene añadir dos reflexiones más: por un lado, en el plano internacional, los logros son menores y, de hecho, no existe ningún acuerdo internacional sobre el tipo de datos que deben retener los proveedores de servicios de Internet ni sobre el plazo de retención; y por otro lado, en relación con la regulación de los contenidos relacionados con el terrorismo, los enfoques varían de unos Estados a otros. En suma, la comunidad internacional carece de una normativa específica y completa que regule una de las cuestiones que presentan un mayor interés en la lucha contra el terrorismo en el ciberespa-

---

[73] Comisión Europea, «Informe de la Comisión al Consejo y al Parlamento Europeo: Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), COM (2011) 225, de 18 de abril de 2011, sección 3.2».

[74] *DO* L núm. 105, de 13 de abril de 2006.

[75] *Ibid.*

[76] El TJUE declaró nula la Directiva en base a lo establecido en el art. 7 de la *Carta de los Derechos Fundamentales del 2000* que dice textualmente «toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de sus comunicaciones», y en el art. 8, que indica «toda persona tiene el derecho a la protección de datos personales que le conciernan»: veáse Sentencia *Digital Rights Ireland Ltd*, C-293/12, ECLI:EU:C:2014:238, apartados 38-54.

[77] Jiménez García, F., *La prevención y lucha contra el blanqueo de capitales y la corrupción*, Granada, Comares, 2015, pp. 217-218.

cio, con independencia de que se hayan llevado a cabo regulaciones parciales y sectoriales en esta materia.

4.4. Regulación del delito de incitación a cometer actos de terrorismo a través de las TIC

59. La comunidad internacional ha avanzado significativamente en la regulación del delito de incitación a la comisión de actos de terrorismo[78]. En 2005, como respuesta a la creciente amenaza terrorista, se adoptó en Varsovia el *Convenio núm. 196 para la Prevención del Terrorismo*, en el marco del Consejo de Europa, que impone, con rotundidad, a los Estados miembros la obligación de tipificar «la incitación pública a cometer un delito de terrorismo», así como el reclutamiento y adiestramiento de terroristas. Ahora bien, la aplicación de este Convenio, que se basa en parte en el art. 3 del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de las TIC, busca un equilibrio dentro de ese conflicto permanente entre la aplicación de la ley y la protección de las libertades y los derechos humanos[79].

60. También, el CS de Naciones Unidas ha adoptado la Resolución 1624 (2005) en la que exhorta a los Estados a que lleven a cabo medidas a fin de prohibir por ley la incitación a cometer actos terroristas y prevenir las conductas de esa índole[80], sin descuidar sus obligaciones internacionales en virtud de la normativa sobre derechos humanos. El informe del Secretario General titulado «Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo» interpreta y califica esta Resolución como «la base para tipificar la inducción a la comisión de atentados y a la captación de terroristas, incluso a través de Internet». Tomando en consideración esta Resolución, el Consejo de la UE modificó, en 2008, la Decisión Marco 2002/475/JAI69[81] con la finalidad de incluir específicamente

---

[78] En España, los arts. 18 y 579 del Código Penal español hacen de la incitación pública a cometer un delito de terrorismo un acto preparatorio del delito de provocación. El art. 57 castiga el delito de enaltecimiento del terrorismo, delito que se incorporó en el Código Penal por la Ley Orgánica 7/2000, de 22 de diciembre.

[79] Aparicio Díaz, L., «Una primera aproximación a la Decisión Marco 2008/919/JAI, de 28 de noviembre, que modifica la Decisión Marco del Consejo 2002/475/JAI, de 13 de junio, sobre la lucha contra el terrorismo», *Athena Intelligence Journal*, vol. 4, 2009, núm. 1, pp. 88-117.

[80] Dicha Resolución dice expresamente: «Condenando también en los términos más enérgicos la incitación a la comisión de actos de terrorismo [...] de justificación o glorificación (apología) de actos de terrorismo que puedan incitar a la comisión de nuevos actos de terrorismo», «Profundamente preocupado por el hecho de que la incitación a la comisión de actos de terrorismo por motivos de extremismo e intolerancia constituye un peligro grave y creciente para el goce de los derechos humanos y una amenaza para el desarrollo social y económico de todos los Estados, socava la estabilidad y prosperidad mundiales, y debe ser afrontada por las Naciones Unidas y todos los Estados con urgencia y de manera activa, y subrayando la necesidad de adoptar todas las medidas necesarias y apropiadas de conformidad con el Derecho internacional, en los planos nacional e internacional, para proteger el derecho a la vida». S/RES/1624 (2005), en *http://www.un.org/en/sc/ctc/docs/2015/N1514132_ES.pdf*.

[81] «El Consejo de la Unión Europea adoptó la Decisión marco 2002/475/JAI, de 13 de junio, sobre la lucha contra el terrorismo, que armoniza la definición de los delitos de terrorismo en todos los Esta-

las disposiciones sobre incitación pública a cometer un delito de terrorismo, el reclutamiento y el adiestramiento de terroristas.

61. En esta línea, la Decisión Marco 2008/919/JAI proporciona, también, una base para perseguir la difusión de propaganda terrorista y la transmisión de conocimientos para la fabricación de bombas a través de Internet, en la medida en que dicha difusión se haga intencionalmente y cumpla los requisitos de los delitos mencionados[82]. Con ello, se incorporan nuevos delitos referentes a la conducta que puede llevar a cometer actos de terrorismo, independientemente de los medios o instrumentos tecnológicos mediante los cuales se cometan esos delitos. En otros términos, las disposiciones de esta Decisión Marco no se refieren específicamente a Internet, si bien cubren las actividades llevadas a cabo por este medio.

62. Desde esta perspectiva, tanto el art. 3 de la Decisión Marco de 2008 como el art. 5 del Convenio Europeo para la Prevención del Terrorismo, del Consejo de Europa, obligan a los Estados parte a penalizar los actos o las declaraciones que constituyen incitación a cometer actos de terrorismo. Todo ello ha provocado que, en Europa, comiencen a someterse a los tribunales con éxito actos de incitación al terrorismo. Podemos recordar, como supuesto significativo, que, en Alemania, en 2008, Ibrahim Rashid, inmigrante kurdo iraquí, fue declarado culpable de incitación. Tras ser acusado de librar una «yihad virtual» en Internet, los fiscales alegaron que, al publicar propaganda de *Al Qaeda* en las salas de charla de Internet, «Rashid estaba tratando de conseguir reclutas para unirse al grupo terrorista y participar en la yihad»[83], lo que nos revela los avances que se vienen produciendo en esta materia.

4.5. La insuficiencia de instrumentos jurídicos de carácter internacional y regional para combatir el uso de las TIC por el terrorismo

63. La comunidad internacional no ha afrontado con intensidad la adopción de normas destinadas a combatir el uso de las TIC por el terrorismo. No obstante, debemos subrayar, al menos, algunos de los tímidos avances que se han producido.

64. Primero, no existe ningún instrumento de alcance universal que se refiera a este aspecto de la actividad terrorista: combatir el uso de Internet por los terroristas. No contamos con un Convenio universal que trate específicamente la prevención y represión del uso de Internet por terroristas. En cualquier caso, conviene preguntarse si es precisa o no la elaboración de normas

---

dos miembros de la Unión Europea, mediante la introducción de una definición específica y común del concepto de "terrorismo", establece normas de competencia para garantizar que los delitos terroristas sean perseguidos de manera eficaz, y esboza medidas concretas con respecto a las víctimas de los delitos de terrorismo», en Olvera Gorts, M., *op. cit.*, nota 55.

[82] *DO* L núm. 330, de 10 de diciembre de 2013.

[83] *The Use of Internet...*, *op. cit.*, nota 48, p. 42.

específicas destinadas a combatir el terrorismo en el ciberespacio o, si por el contrario, serían suficientes las normas que se han adoptado en la lucha contra el terrorismo en general. En realidad, se revela la necesidad de contar con normas que se ocupen, específicamente, de los componentes que definen estas manifestaciones del terrorismo a través de las «nuevas» tecnologías.

65. Segundo, se han producido algunos avances en el ámbito de una organización regional, como el Consejo de Europa, y dentro del contexto internacional que se generó tras los atentados del 11-S (2001). En este caso, se adoptó, en Budapest, el 23 de noviembre de 2001, el Convenio sobre la Ciberdelincuencia que se constituye en el único instrumento multilateral de carácter vinculante que trata de la actividad delictiva realizada en Internet. Este Convenio tiene por objeto principal armonizar las legislaciones nacionales relativas al delito cibernético, mejorar los procedimientos internos para detectar, investigar y perseguir esos delitos, y proporcionar arreglos de cooperación internacional rápida y fiable sobre estas cuestiones[84]. En él se establece una norma mínima común respecto de los delitos internos cometidos con ordenadores y, asimismo, se prevé la penalización de nueve delitos, incluidos los delitos relacionados con el acceso no autorizado a sistemas, programas o datos informáticos, y la manipulación ilícita de estos; el fraude y la falsificación informáticos; y la tentativa de cometer tales actos o complicidad en su comisión[85]. Nos interesa resaltar que se obliga a los Estados parte a elaborar y adoptar normas que exijan a los proveedores de servicios de Internet conservar los datos especificados almacenados en sus servidores durante un plazo máximo de noventa días (renovable), si así lo requieren los servicios policiales en el curso de una investigación o procedimiento penal, hasta que se puedan adoptar las medidas jurídicas apropiadas para exigir la divulgación de esos datos[86]. En todo caso, los resultados alcanzados, en el ámbito regional europeo, a la hora de combatir el uso de la TIC por el terrorismo, resultan insuficientes desde una óptica completa de la lucha contra el ciberterrorismo.

66. Por último, algunos instrumentos regionales y subregionales[87] contienen normas de fondo y de procedimiento para penalizar los actos de te-

---

[84] Consejo de Europa, *European Treaty Series*, núm. 185.

[85] Informe explicativo del Convenio sobre el delito cibernético del Consejo de Europa, párr. 33: véase *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ ETS%20185%20Explanatory%20report_Spanish.pdf*.

[86] Es precisa la lectura de los arts. 1 y 19, en particular. Documento Cibercriminalidad, Secretaría de Estado de Seguridad del Ministerio del Interior, en *http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815*. También, conviene mencionar que el Consejo de Europa ha elaborado un *Protocolo adicional al Convenio sobre el delito cibernético relativo a la penalización de actos de índole racista y xenófoba* que puede facilitar el enjuiciamiento de los actos de terrorismo cometidos por Internet con la intención de incitar a la violencia por motivos de raza, color, ascendencia u origen nacional o étnico, o religión, *BOE* núm. 26, de 30 de enero de 2015, Sec. I, pp. 7215-7224.

[87] Junto a los instrumentos jurídicos vinculantes hay otros que pueden contener disposiciones relativas a la lucha contra el uso de Internet con fines terroristas. Entre ellos el Convenio de la Asociación de Naciones de Asia Sudoriental contra el terrorismo (2007). Directiva sobre la lucha contra la ciberdelincuencia (2009), de la Comunidad Económica de los Estados de África Occidental, etcétera.

rrorismo que pueden cometerse por medio de las TIC. En este sentido, cabe resaltar que la UE ha puesto en marcha distintas acciones como consecuencia de los ataques realizados por organizaciones delincuenciales contra los sistemas de información y por la amenaza, cada vez mayor, de que se produzcan ataques terroristas contra sistemas de información que forman parte de infraestructuras vitales de los Estados miembros. Entre estas medidas destaca la adopción de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información. Esta Decisión Marco dispone que cada Estado miembro debe adoptar «las medidas necesarias para que el acceso intencionado y sin autorización al conjunto o a una parte de un sistema de información, la intromisión no autorizada e intencionada en los sistemas de información interrumpiendo de forma significativa su funcionamiento y el acto intencionado y no autorizado de intromisión ilegal en los datos de un sistema informático, sean considerados infracciones penales» [88]. Pero, también, como se dice, «se alcanza consenso en las sanciones relativas a estas infracciones» [89].

67. En definitiva, la comunidad internacional no ha elaborado relevantes instrumentos que, de manera específica, estén destinados a atajar la comisión de actos terroristas en el ciberespacio y, desde el plano internacional, se ha dedicado muy poca atención normativa a la comisión de delitos de este tipo que se realizan a través de Internet. La carencia de legislación internacional en esta materia puede encontrar su explicación en que los Estados consideran suficientes los diversos instrumentos adoptados en la lucha contra el terrorismo. Sin embargo, la singularidad y peculiaridades de la comisión de actos terroristas en el ciberespacio aconsejan, a mi juicio, una labor normativa más intensa por parte de la comunidad internacional.

5. CONCLUSIONES

68. Es difícil la lucha contra el terrorismo que se ejerce en el ciberespacio y se revela, además, la necesidad de que se adopten medidas político-jurídicas que combatan esta manifestación del terrorismo. Desde principios del siglo XXI se viene admitiendo la existencia de una amenaza visible, como es el ciberterrorismo, que entraña numerosos riesgos para la seguridad nacional e internacional, y que es fruto del uso de las TIC por los grupos terroristas para favorecer el logro de sus intereses. El empleo de las TIC, como instrumento de apoyo a los objetivos terroristas, es una realidad, si bien también parece evidente que no lo es como herramienta de ataque directo a infraestructuras críticas de los Estados u organismos e instituciones. En esencia, las TIC son una vía que sirve al terrorismo para alcanzar su fin: aterrorizar a la pobla-

[88] Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información (*DO* L núm. 69, de 16 de marzo de 2005). OLVERA GORTS, M., *op. cit.*, nota 55.

[89] En dicho documento se definen los conceptos de «sistema informático», «datos informáticos», «persona jurídica» y «sin autorización». *Ibid.*

ción, cuanta más mejor, además de reclutar miembros; difundir propaganda e incluso «instruir sobre cómo cometer atentados», pero que no sirve, a día de hoy, como método de ataque[90].

69. El uso de las TIC con fines terroristas y delincuenciales es un fenómeno que se ha extendido con especial rapidez desde principios del siglo XXI y que explica la expansión y emergencia de nuevos grupos criminales. Esto obliga a los Estados a actuar de una forma coordinada; sin embargo, la comunidad internacional no ha sido capaz de adoptar una definición consensuada sobre qué se entiende por terrorismo, ni tampoco del ciberterrorismo. Por extensión, no ha sido capaz de adoptar un instrumento jurídico, de alcance universal, que trate específicamente las materias cibernéticas y la cooperación internacional en asuntos penales (incluido terrorismo) relacionados con cuestiones cibernéticas.

70. La carencia de una legislación clara sobre ciberseguridad complica sobremanera y es un obstáculo para una cooperación internacional eficaz en la investigación y persecución de los casos de terrorismo relacionados con el uso de las TIC. Una respuesta eficaz de la sociedad internacional a las amenazas que plantea dicho uso por los terroristas precisa, sin duda, que los organismos internacionales de carácter universal y regional adopten convenios o normas específicas, atendiendo a la singularidad del ciberespacio. En razón de la ausencia de legislación común en materia de ciberseguridad sería fundamental, por lo menos, promover la aproximación y armonización legislativa y la cooperación judicial y policial internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo. Además, en el plano estatal, son pocos los Estados que han elaborado normas destinadas específicamente contra los actos cometidos por terroristas a través de las TIC. La mayoría de los países invocan las leyes penales generales, sobre ciberdelincuencia o contra el terrorismo, o todas ellas, para penalizar este tipo de delitos y enjuiciar a los autores. El nivel de regulación gubernamental de Internet varía mucho entre los Estados, y a falta de una autoridad mundial y centralizada responsable de la regulación de Internet, los interesados privados, tales como los proveedores de servicios, los sitios *web* con contenido generado por los usuarios y los buscadores de Internet, siguen desempeñando un importante papel en la regulación de la disponibilidad de contenidos relacionados con el terrorismo difundidos por Internet.

71. No obstante, desde finales del primer decenio del siglo XXI, prácticamente todos los Estados y los principales organismos internacionales han identificado la seguridad de su ciberespacio como un objetivo estratégico de Seguridad Nacional. De hecho, se ha producido un incremento en la regulación civil y penal sobre delitos en la Red, además de establecerse estándares y normativas de seguridad. La impunidad en la Red está reduciéndose porque se ha ampliado la tipificación de delitos. Pese a todo, en nombre de la seguridad no se deben restringir las libertades o violar los derechos fundamenta-

[90] DOGRUL, M., ASLAN, A. y CELIK, E., *op. cit.*, nota 27, p. 32.

les. El respeto por los derechos humanos y el Estado de Derecho son parte integrante e imprescindible de la lucha contra el terrorismo, también en el ciberespacio.

RESUMEN

LA CIBERSEGURIDAD Y EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) POR EL TERRORISMO

El objetivo de este estudio es analizar los beneficios y virtudes de las TIC en la sociedad internacional y, sobre todo, el uso que los diferentes grupos terroristas hacen de ellas, con el fin de promover y favorecer sus fines, generando la aparición de nuevos riesgos, retos y amenazas como el ciberterrorismo. Además, se estudian los instrumentos de carácter político así como los marcos jurídicos y la práctica de los Estados, también la adoptada en el seno de los organismos internacionales, para hacer frente a este reto de carácter transnacional. En definitiva, determinar qué elementos, en los planos internacional y nacional, representan obstáculos para la cooperación, así como las carencias que aún quedan por cubrir para aproximarnos al reto de un ciberespacio pacífico, seguro y libre.

Palabras clave: ciberterrorismo, ciberespacio, transnacional, Internet, Tecnologías de la Información y de la Comunicación, políticas y marcos jurídicos.

ABSTRACT

THE CYBERSECURITY AND THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) FOR TERRORISM

This study analyzes the benefits and virtues of ICTs in the international society and, above all, the use that different terrorist groups make of them, in order to promote and favour their objectives, generating new risks, challenges and threats such as cyberterrorism. In addition, the instruments of a political nature as well as regulations and State practice, including that adopted within international organizations, are studied in order to meet this transnational challenge. In short, this study examines what elements, at international and national level, represent obstacles to cooperation, as well as the gaps that remain to be filled in order to approach the challenge of a peaceful, safe and free cyberspace.

Keywords: cyberterrorism, cyberspace, transnational, Internet, Information and Communication Technologies, policies and legal frameworks.