IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

ARTÍCULO

La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas

Alicia Chicharro Lázaro

Fecha de presentación: septiembre de 2009
Fecha de aceptación: noviembre de 2009
Fecha de publicación: diciembre de 2009

Resumen

El término *ciberterrorismo* salta a la luz pública en grandes titulares periodísticos a finales del siglo pasado y principios del presente, particularmente, a partir de los atentados del 11-S en Nueva York. Se trata de la forma de terrorismo que emplea las tecnologías de la información y la comunicación para someter a los poderes públicos, a ciertos individuos o grupos de la sociedad o, de manera general, a la opinión pública a un clima de terror, con el fin de lograr sus aspiraciones.

El ciberterrorismo contra o por vía de Internet supone un riesgo significativo hoy en día, cuando los sistemas informáticos son responsables de llevar a cabo muchas funciones esenciales de nuestra sociedad.

Sin embargo, la persecución de la mayoría de estos crímenes es compleja debido a la naturaleza técnica de Internet y a la dimensión internacional del fenómeno del ciberterrorismo, que requiere un tratamiento coordinado entre el máximo número posible de países.

En el seno del Consejo de Europa se han adoptado dos importantes convenciones que, puestas en conjunción, permitirán hacer frente a estos comportamientos delictivos: la Convención sobre Cibercrimen del año 2001 y la Convención para la Prevención del Terrorismo del año 2005. La adaptación de la legislación interna a dichos instrumentos proporcionará a los Estados una cobertura adecuada para perseguir los crímenes asociados al uso de Internet con fines terroristas.

Palabras clave

ciberterrorismo, Consejo de Europa, cibercrimen, terrorismo.

Tema

E-justicia

Legislative Action of the European Council to Combat the Use of the Internet for Terrorist Purposes

Abstract

The term "cyberterrorism" has been highly prominent in major newspaper headlines since the end of the last century and, particularly, after the 9/11 attacks in New York. It is a form of terrorism that uses information and communication technologies to subject public authorities, certain individuals or groups in society and, more generally, public opinion to a climate of terror, to achieve the goals of the cyberterrorists.

Cyberterrorism, either against or over the Internet, supposes a major risk in this age where computer systems are in charge of running many essential functions of society.

However, tackling the major part of these crimes is complex due to the technological nature of the Internet and the international dimension of cyberterrorism, requiring a coordinated response from as many countries as possible.

Within the Council of Europe important conventions have been adopted which, in their entirety, will offer possibilities to face up to this kind of criminal activity: the 2001 Convention on Cybercrime and the 2005 Convention on the Prevention of Terrorism. The adaptation of their internal legislation will provide member states adequate coverage to combat crimes linked to the use of the Internet for purposes of terrorism.

Keywords

cyberterrorism, European Council, cybercrime, terrorism

Subject

e-Justice

1. Introducción

La época actual ha sido calificada como la «era digital». La revolución que han supuesto las nuevas tecnologías de la información y la comunicación (TIC), particularmente a través del desarrollo vertiginoso de Internet, contribuye al fenómeno de la globalización y rompe con las tradicionales fronteras espacio-temporales. Nos situamos en la denominada «sociedad de la información», donde cualquier ordenador conectado a Internet se convierte en un medio de comunicación accesible a prácticamente todo el mundo.[1] Esto incluye a los delincuentes y, particularmente, a los terroristas. La conjunción de tecnología y terrorismo provoca incertidumbre y un alto grado de inseguridad cuando pensamos en el futuro.[2]

El término *ciberterrorismo* salta a la luz pública en grandes titulares periodísticos a finales del siglo pasado y principios del presente, particularmente a partir de los

1. NICANDER, L.; RANSTORP, M. (ed.) (2004). *Terrorism in the information age: new frontiers?*. Estocolmo: National Defense College.
2. Ver LAQUEUR, W. (1999). *The new terrorism: fanatism and the arms of mass destruction*. Oxford: Oxford University, pág. 254. En *The New Yorker* aparecía un artículo en el año 2001, firmado por Specter, que predecía lo siguiente: «The Internet is waiting for its Chernobyl, and I do not think we will be waiting much longer» [artículo en línea].

atentados del 11-S en Estados Unidos,[3] aunque fue un investigador del Instituto para la Seguridad y la Inteligencia de California, Barry Collin, quien acuñó el término en los años ochenta.

Alcanzar una definición precisa de lo que se entiende por ciberterrorismo requiere partir de una serie de premisas que suponen ciertos obstáculos. En primer lugar, el debate en torno a dicho fenómeno se ha llevado a cabo en su gran mayoría a través de medios informales que tratan de dar a entender el concepto más que a establecer una definición operacional y comprensiva del nuevo término. En una época en la que la información deviene conocimiento, es difícil distinguir el ciberterrorismo de su representación mediática. En segundo lugar, la sobreexplotación que ha sufrido dicho vocablo a partir del 11-S lo ha convertido en una palabra-rumor (*buzzword*), que puede tener significados disímiles para distintas personas. En tercer lugar, en el entorno de la informática y particularmente de Internet, es muy habitual la creación de nuevas voces, o bien a partir del prefijo *ciber* o bien añadiendo los adjetivos *informático/a*, *electrónico/a*, *virtual* o *digital*. Por último, el mayor impedimento para asentar el concepto de ciberterrorismo es precisamente la falta de acuerdo sobre la definición de terrorismo.

Todo esto conlleva que no haya una sola definición comúnmente aceptada de ciberterrorismo, lo mismo que no la hay de terrorismo.

Se trata de una composición realizada a partir de la raíz *ciber* y la palabra *terrorismo*.[4] La raíz *ciber* está relacionada con la tecnología.[5] Para la expresión *terrorismo* tenemos que volver a la eterna discusión sobre su concepto que ha hecho correr ríos de tinta sin alcanzar un acuerdo general.[6]

Sí tenemos definiciones en textos normativos internos[7] y en instrumentos internacionales pero de ámbito regional.[8] Incluso podríamos encontrar algún avance hacia una precisión del concepto en los más recientes tratados sectoriales elaborados bajo los auspicios de Naciones Unidas[9] y en los trabajos preparatorios del Tratado General sobre el Terrorismo, cuya adopción

3. *San Francisco Chronicle* en mayo de 1997, *Los Angeles Times* en febrero del 2001, *Boston Herald* en junio, *Washington Post* en septiembre, revista *Time* en noviembre, *Bristol Herald Courrier* en diciembre (todos del mismo año) o *USA Today* en junio de 2002, son algunos de los principales rotativos estadounidenses que han dedicado titulares al «ciberterrorismo» y, en la mayoría de los casos, a la alarmante amenaza que éste supone.
4. Ver DESOUZA, K.; HENSGEN, T. (2003). «Semiotic emergent framework to address the reality of cyberterrorism», *Technological Forecasting and Social Change*, vol. 70, n.º 4, pág. 385-396.
5. *Cibernética* es un término que hemos importado del inglés y que se refiere al estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología. El origen más remoto lo encontramos en la palabra griega , que significa el arte de gobernar una nave.
6. Ver por ejemplo SAUL, B. (2006). *Defining terrorism in international law*, Oxford: Oxford University Press; HUGUES, E. (2002). «La notion de terrorisme en droit international: enquête d'une définition juridique», *Journal du Droit International*, sept., pág. 753-771; ROBERTS, A. (2002). «Can we define terrorism?», *Oxford Today*, n.º 14, pág. 18-24; SKUBISZEWSKI, K. (1989). «Definition of terrorism», *International Yearbook of Human Rights*, vol. 19, pág. 39-53; BARIFFI, F. J. (2008). «Reflexiones en torno al concepto de terrorismo a la luz del Derecho Internacional contemporáneo», *Derechos y Libertades*, vol. 19, pág. 1-6.
7. United Status Code, Title 22, Section 2656f(d): «*The term ' terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience*». En España, si tomamos los artículos 571 a 577 del Código penal, podemos considerar terroristas a «los que, perteneciendo o sin pertenecer a banda armada, organización o grupo terrorista, y con la finalidad de subvertir el orden constitucional o de alterar gravemente la paz pública, o la de contribuir a estos fines atemorizando a los habitantes de una población o a los miembros de un colectivo social político o profesional, cometieren homicidios, lesiones, detenciones ilegales, secuestros, amenazas o coacciones contra las personas, o llevaren a cabo cualesquiera delitos de incendios, estragos, daños o tenencia, fabricación, depósito, tráfico, transporte o suministro de armas, municiones o sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o de sus componentes».
8. Especialmente importantes son las definiciones alcanzadas tanto en el Consejo de Europa, que será objeto de estudio en este trabajo, como en la Unión Europea (Decisión Marco 2002/475/JAI del Consejo, sobre lucha contra el terrorismo, DO L 164, 22.6.2002, pág. 3).
9. Artículo 2 del Convenio Internacional para la represión de la financiación del terrorismo de 1999.

halla en la definición del fenómeno terrorista su mayor traba.

La Asamblea Parlamentaria del Consejo de Europa considera que un acto de terrorismo es cualquier delito cometido por individuos o grupos recurriendo a la violencia o amenazando con utilizarla contra un país, sus instituciones, su población en general o sobre individuos concretos, que, motivado por aspiraciones separatistas, concepciones ideológicas extremistas o fanatismo, o inspirado por móviles irracionales o subjetivos, tiene por objeto someter a los poderes públicos, a ciertos individuos o grupos de la sociedad, o, de manera general, a la opinión pública, a un clima de terror.[10]

Así, *ciberterrorismo* será la forma de terrorismo que emplea las tecnologías de la información y la comunicación para someter a los poderes públicos, a ciertos individuos o grupos de la sociedad, o, de manera general, a la opinión pública, a un clima de terror, con el fin de lograr sus aspiraciones.

Comparada con otras,[11] esta definición permite integrar cualquier tipo de ataque contra los ordenadores, redes o información en ellos contenida, así como cualquier atentado ejecutado a través de la utilización de los mismos, incluso aquel que no produzca daños en el espacio físico sino sólo en el «mundo virtual».[12]

2. La utilización de Internet con fines terroristas

Junto a la amenaza ferozmente real que suponen los ataques terroristas vividos en los últimos años, debemos abordar otro riesgo, esta vez más virtual, que acarrearía el uso de los sistemas informáticos, y sobre todo de Internet, para fines terroristas.[13]

Internet, la Red de Redes, nació de la idea y de la necesidad de establecer múltiples canales de comunicación entre ordenadores.[14]

Con el desarrollo de las tecnologías de la información también se abrió una compuerta para la comisión de delitos a través de las mismas. Históricamente las leyes penales surgen como respuesta a las actividades que producen daño a la sociedad y con la aparición de los ordenadores, comenzaron a emerger nuevos delitos y la preocupación por castigar ciertas conductas, recibiendo el nombre de *delitos informáticos* o *cibercrímenes*.

En sentido estricto, los delitos informáticos son aquellos establecidos por la ley a efectos de protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de las infracciones cometidas contra tales sistemas o cualquiera de sus componentes. En sentido amplio, se enmarcan en esta categoría

10. Recommendation 1426 (1999), European democracies facing up to terrorism (23 September 1999), pág. 5.
11. Por ejemplo Devost, Houghton y Pollard ofrecen una definición de «terrorismo informático» como «el abuso intencionado de un sistema, red o componente de información digital, con el fin de apoyar o facilitar una campaña o una acción terrorista»; DEVOST, M.; HOUGHTON, B.; POLLARD, N. (1997). «Information terrorism: political violence in the information age», *Terrorism and Political Violence*, vol. 9, n.º 1, pág. 75. Los mismos autores lo consideran «the nexos between criminal information system fraud or abuse, and the physical violence of terrorism»; «Information terrorism: Can you trust your toaster?» [artículo en línea]. *The Terrorism Research Center*. [Fecha de consulta: 30 de abril del 2009]. Denning lo define de la siguiente manera: «Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not»; DENNING, D. (2001). «Hacker warriors: rebels, freedom fighters, and terrorists turn to cyberspace» [artículo en línea], *Harvard International Review*. [Fecha de consulta: 30 de abril de 2009]. Ver también IQBAL, M. (2004). «Defining cyberterrorism», *John Marshall Journal of Computer and Information Law*, vol. 22, n. º 2, pág. 397-408.
12. Ver MATES, M. (rep.) (2001). *Technology and terrorism*, Bruselas: OTAN, pág. 3.
13. Ver NEUMANN, P. (2008). *The strategy of terrorism*, Londres-Nueva York: Routledge.
14. En un primer momento, se trataba de garantizar las telecomunicaciones militares con fines de seguridad y defensa en EEUU, pero rápidamente se expandió creando una red pública para uso de las universidades.

todas las conductas delictivas ya tipificadas por la legislación criminal de un país cuando el tipo penal lo permite y se cometen a través del uso del ordenador.[15]

El ciberterrorismo es una conducta ilícita de los denominados *cibercrímenes* o *delitos informáticos*, en los que un elemento esencial es la utilización de ordenadores como instrumentos o como objetivos produciendo un clima de terror, para que se dé el tipo penal.

El ciberterrorismo, cuando tiene por objetivo Internet o se lleva a cabo por dicha vía, representa una amenaza seria, ya que muchos aspectos esenciales de la sociedad actual dependen del correcto funcionamiento de los sistemas informáticos.[16] La informática está presente en la vida cotidiana de una parte importante de los habitantes del planeta. Las administraciones públicas están plenamente integradas en la era digital, controlando sus servicios a través de ordenadores. La empresa privada incorpora las nuevas tecnologías en aras de reducir costes y aumentar beneficios. En cualquier parte del mundo se toma nota, se registra y se archiva utilizando medios telemáticos. Los servidores almacenan cantidades ingentes de datos, algunos de ellos confidenciales o de carácter personal, que deben ser protegidos. La dependencia que la sociedad actual tiene de ellos es innegable, con lo que no podemos ignorar o negar la amenaza que esto conlleva.

La globalización económica acarrea también la mundialización de los peligros y la expansión del terrorismo internacional es uno de ellos. A su vez, una generación de terroristas expertos en informática que utilizan las nuevas tecnologías para sus propósitos pone en riesgo tanto a los propios sistemas informáticos como a las personas físicas y a sus bienes, que pueden ser atacados a través del uso fraudulento de la informática.[17]

Cuando analizamos dicha amenaza y evaluamos las posibles respuestas legales, es necesario distinguir tres fenómenos:[18]

a. ataques por medio de Internet que causen daños no sólo a los sistemas electrónicos de comunicación básicos y a la infraestructura de tecnologías de la información y la comunicación (TIC), sino también a otras infraestructuras, sistemas e intereses jurídicos, incluida la vida humana;[19]

b. propagación de contenido ilegal, incluida la amenaza de ataques terroristas; incitar, anunciar y glorificar el terrorismo; captar fondos y financiar el terrorismo; entrenar a los terroristas; reclutar a personas para el terrorismo; y diseminar material racista o xenófobo;

c. otros usos logísticos de las TIC por los terroristas, como la comunicación interna, la adquisición de información y el análisis de objetivos.

Las nuevas formas de cibercrimen, así como la comisión de delitos tradicionales utilizando en algún momento redes informáticas plantea la necesaria evolución de las normas penales sustantivas, de los métodos de investigación y enjuiciamiento y de las medidas de prevención. Los problemas surgen de la complejidad técnica de los entornos informáticos, la multitud e invisibilidad de los datos electrónicos, de la proliferación de técnicas de encriptación y ocultación de contenidos,[20] la dificultad de identificar a los culpables en Internet, del hecho de que un sistema informático puede ser atacado desde la distancia y de la naturaleza global de Internet, el cual no puede ser controlado con medidas puramente nacionales.[21]

15. Ver SCHELL, B.; MARTIN, C. (2004). *Cybercrime: A reference handbook*, Santa Bárbara: ABC-CLIO.
16. Ver MATUSITZ, J. (2005). «Cyberterrorism», *American Foreign Policy Interests*, vol. 27, n.º 2, pág. 137-147.
17. Ver POST, J.; RUBY, K.; SHAW, E. (2000). «From car bombs to logic bombs: the growing threat from information terrorism», *Terrorism and Political Violence*, vol. 12, n.º 2, pág. 97-122.
18. Informe de los expertos preparado por los profesores Sieber y Brunst del Max Planck Institute for Foreign and International Criminal Law de Freiburg (Alemania): COUNCIL OF EUROPE (2007). *Cyberterrorism - The use of the Internet for terrorist purposes*, Estrasburgo: Council of Europe Publishing.
19. Ver COHEN, F. (2003). «Cyber-risks and critical infrastructures», *Strategic Security*, vol. 27, n.º 2, pág. 1-10.
20. Ver CONWAY, M. (2008). «Code wars: stenography, signals intelligence, and terrorism», *Dublin City University International Studies Working Papers*, vol. 6, 19 pág.
21. Ver COULTHARD, A. (2003). «Cyber terrorism: beyond the hype». En: *Proceeding of the European Conference on Information Warfare and Security 2002*, London: Academic Conferences Ltd., pág. 57-65.

Por todo ello, lo más deseable sería disponer de instrumentos internacionales que regulen el problema y que aboquen a los Estados a armonizar sus leyes penales, así como a cooperar en la investigación, persecución y castigo de los culpables. El gran obstáculo a nivel global tiene dos vertientes: la inexistencia de normativa sobre ciberdelincuencia y la legislación sectorial sobre terrorismo. En el ámbito regional europeo, sin embargo, poseemos instrumentos suficientes tanto en el Consejo de Europa como en la UE.[22] Aquí analizaremos la labor desarrollada por el Consejo de Europa.

3. La lucha contra la cibercriminalidad y el terrorismo en el marco del Consejo de Europa

La persecución de la mayoría de estos crímenes es compleja debido a la naturaleza técnica de Internet y a la dimensión internacional del fenómeno del ciberterrorismo,[23] que requiere un tratamiento coordinado entre el máximo número posible de países.

En el seno del Consejo de Europa[24] se han adoptado dos importantes convenciones, que, puestas en conjunción, permitirán hacer frente a los comportamientos delictivos cometidos a través de vías hasta ahora poco exploradas, pero que abren un sinfín de posibilidades a los terroristas[25]. Estas son la Convención sobre Cibercrimen de 2001 y la Convención para la Prevención del Terrorismo de 2005. Analizaremos si el instrumento específico sobre delitos informáticos es aplicable también al terrorismo y si el texto específico sobre terrorismo se puede aplicar también en el terreno de las nuevas tecnologías[26]. En definitiva, si tomando ambos instrumentos obtenemos una cobertura adecuada para perseguir los crímenes asociados al uso de Internet con fines terroristas.[27]

En cualquier caso, la persecución y procesamiento de los delitos relacionados con el ciberterrorismo nunca significará una merma en la protección de los derechos humanos y las libertades fundamentales, como quedan garantizados en el CEDH de 1950 y sus protocolos adicionales.[28]

3.1. La Convención Europea sobre Cibercrimen

La Convención sobre Cibercrimen de 23 de noviembre del 2001 es el instrumento internacional más completo sobre delitos cometidos contra o a través de ordenadores.[29] Incluye obligaciones acerca de normas penales sustantivas, procedimientos penales y cooperación internacional en este campo.[30] No cabe duda de que este texto puede ser usado en casos de terrorismo, precisamente cuando este delito sea cometido contra o a través de sistemas informáticos.

Los artículos 2 y 3 de la Convención cubren las técnicas utilizadas por *hackers*, que sirven para acceder al ordenador de la víctima e interceptar datos informáticos del

22. Ver FERNÁNDEZ TOMÁS, A. (2004). «Terrorismo, Derecho Internacional Público y Derecho de la Unión Europea». En: *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gazteiz 2004*, Vitoria: Universidad del País Vasco, pág. 191-263.
23. SIEBER, U. (2006). «International cooperation against terrorist use of Internet», *Revue Internationale de Droit Pénal*, vol. 77, pág. 395-449.
24. En la actualidad forman parte de esta organización internacional de ámbito regional europeo 47 Estados.
25. VERTON, D. (2003). *Black ice: the invisible threat of cyberterrorism*, Nueva York: McGraw-Hill.
26. Para el análisis del déficit que presentan las convenciones internacionales sobre terrorismo, ver TOMOUSCHAT, C. (2005). «On the possible 'added value' of a comprehensive Convention on Terrorism», *Human Rights Law Journal*, n.º 26, pág. 287-306.
27. En 2007 se elaboró un informe de expertos sobre ciberterrorismo en el que se advierte de los riesgos y se analizan las respuestas que las normas elaboradas en el seno del Consejo de Europa pueden dar a dicho fenómeno: COUNCIL OF EUROPE (2007). *Cyberterrorism - The use of the Internet for terrorist purposes*, Estrasburgo: Council of Europe Publishing.
28. Ver VON SCHORLEMER, S. (2003). «Human rights: substantive and institutional implications of the war against terrorism», *European Journal of International Law*, vol. 14, n.º 2, pág. 265-282; FERNÁNDEZ DE CASADEVANTE ROMANÍ, C.; JIMÉNEZ GARCÍA, F. (2005). *Terrorismo y derechos humanos*, Madrid: Dykinson; BRIBOSIA, E.; WEYEMBERGH, A. (dir.) (2002). *Lutte contre le terrorisme et droits fundamentaux*, Bruselas: Bruylant.
29. La Convención entró en vigor el 1 de julio del 2004. España de momento no la ha ratificado.
30. Resulta llamativa la lentitud con la que los Estados están accediendo a este instrumento. Sólo tiene 26 ratificaciones. España no es parte por el momento. Ver GERCKE, M. (2006). «The slow wake of a global approach against cybercrime», *Computer Law Review International*, n.º 5, pág. 140-145.

mismo. A su vez, los artículos 4 y 5 de la Convención se refieren a dañar, borrar, alterar o suprimir datos informáticos o interferir en todo el sistema, obligando a las partes a adoptar medidas legislativas o de otro tipo contra todos estos comportamientos.

Estos dos últimos artículos cubren cualquier conducta que tenga por objetivo la interferencia en datos y sistemas informáticos que, como ya hemos visto, es un prerrequisito para los atentados terroristas a través de Internet. El informe explicativo de la Convención afirma que el artículo 5 está formulado de un modo neutral para que todas las clases de funciones puedan encontrarse protegidas por él. Esto significa que cualquier tipo de ataque terrorista contra sistemas informáticos, incluidos los que afecten a bienes y personas, cae en el campo de aplicación de los artículos 4 y 5 de la Convención sobre Cibercrimen.

El artículo 6 trata del abuso de equipos e instrumentos técnicos y prevé que las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos que permitan cometer infracciones, palabras clave, códigos de acceso o datos informáticos similares, o la posesión de alguno de los elementos antes descritos con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5.

Con respecto a la utilización de Internet para fines terroristas, los artículos 2, 3 y 6 otorgan una protección adicional, permitiendo que los posibles autores sean perseguidos de forma diligente.

Las disposiciones de la Convención contemplan la comisión de dichos actos, la tentativa y la complicidad, así como la responsabilidad de las personas jurídicas (artículos 11 y 12). Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en la Convención sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad para las personas físicas.

Antes de esto, los Estados también se comprometen a facilitar las necesarias investigaciones en el entorno cibernético, a través de la implementación de las obligaciones reguladas desde el artículo 14 al 22, que cubren la conservación inmediata de datos informáticos almacenados, la consecutiva congelación y divulgación de datos de tráfico, la orden de comunicación, el registro y decomiso de datos informáticos almacenados, la recolección de los mismos en tiempo real y la interceptación de contenidos. El artículo 19 permite a las autoridades competentes bloquear o remover del sistema informático los contenidos ilegales.[31]

La implementación de las obligaciones incluidas en la Convención sobre Cibercrimen demanda una extensa criminalización de los ataques ciberterroristas cometidos contra ordenadores u otros intereses legales que dependen del correcto funcionamiento de los sistemas informáticos.[32] Los daños causados en bienes o personas no son un prerrequisito para castigar basándose en la Convención sobre Cibercrimen, pero se sigue de la aplicación de normas penales complementarias de los sistemas internos. Así, la Convención sobre Cibercrimen alcanza a la criminalización de ataques a sistemas informáticos por medio del acceso a datos, que no requiere tener en cuenta ni el daño físico ni la intencionalidad (política) del autor.

Durante el proceso de negociación de la Convención sobre Cibercrimen, fue muy difícil llegar a un acuerdo sobre la criminalización de actos de naturaleza racista o xenófoba, por lo que estos actos fueron incluidos en un protocolo adicional. Los Estados que han consentido en obligarse también por este protocolo adaptarán su legislación interna para

31. La prevención en este campo es bastante compleja. En primer lugar, porque Internet y el ciberespacio global que significa es extremadamente difícil de controlar. En segundo lugar, porque alentar a las autoridades nacionales a diseñar mecanismos de control, muy probablemente ineficaces y llamados a fracasar, pone en serio peligro el libre flujo de información y el derecho a la privacidad. De nuevo aquí se manifiesta la dificultad que supone encontrar un equilibrio entre el interés de la seguridad y la protección de los derechos humanos. Ver HOL, A. (2005). *Security and civil liberties: the case of terrorism*, Amberes: Intersentia.
32. Ver LIPSON, H. (2002). «Tracking and tracing cyber-attacks: technical challenges and global policy issues», *CERT Coordination Center Special Report*, noviembre, pág. 37-51.

hacer punible la diseminación de material racista o xenófobo, de amenazas contra personas o grupos de personas que vengan motivadas por razón de su raza, color, ascendencia, origen nacional o étnico o religión, y la publicidad insultante contra esas personas o grupos por los mismos motivos, cuando estos comportamientos se realicen a través de sistemas informáticos.

Si esas previsiones las ponemos en conjunción con el terrorismo, el protocolo resulta relevante respecto a las amenazas e insultos lanzados con la intencionalidad de incitar a la violencia entre grupos con distintos orígenes raciales, nacionales o religiosos. Por tanto, las disposiciones del protocolo cubrirían la utilización de las nuevas tecnologías de la información y la comunicación para estos fines terroristas.

En cuanto a la cooperación internacional, la Convención prevé la extradición para los casos de delitos cometidos a través de la utilización de las tecnologías de la información y la comunicación, pero exige doble incriminación: que el hecho sea punible en el Estado requirente y en el requerido.

Ahora bien, el principal escollo deriva de la inexistencia de una definición generalmente aceptada de lo que se entiende por «delito político». Por este motivo, los Estados que reciben peticiones de extradición son quienes interpretan individualmente si una determinada ofensa debe considerarse o no como tal. Las autoridades concernidas se ven compelidas, respecto a las peticiones de extradición relacionadas con actos terroristas, a tener en cuenta la particular gravedad de las violaciones cometidas. No obstante, nada impide que se pueda denegar la extradición por considerar un determinado acto de terrorismo como delito político, salvo para los países que han ratificado, sin reservas, la Convención del Consejo de Europa sobre Supresión del Terrorismo de 1977, ya que la misma obliga a los Estados parte a no calificar de delitos políticos, las ofensas graves que supongan actos de violencia contra la vida, la integridad física o la libertad de las personas.[33]

Independientemente de lo visto hasta el momento, el informe de expertos sobre Ciberterrorismo del Consejo de Europa advierte que las nuevas tecnologías van abriendo día a día nuevos campos a la investigación criminal y a la transferencia de información entre los cuerpos de seguridad de distintos países.[34]

En consonancia, sus autores sugieren un protocolo adicional para añadir las nuevas técnicas de investigación o la posibilidad de excluir la excepción de cláusula política para algunos de los delitos contemplados en la Convención –especialmente en casos graves de transferencias de datos personales de un sistema a otro.

En contraste, el informe señala que un instrumento adicional que trate sobre los ataques de especial gravedad a las tecnologías de la información y la comunicación o a infraestructuras generales no es esencial. Sería suficiente con que las legislaciones internas de los Estados sobre protección de datos y sistemas informáticos incluyeran sanciones apropiadas para los casos de atentados terroristas contra este tipo de tecnologías. Esas sanciones efectivas, proporcionadas y disuasivas, las requiere la Convención sobre el Cibercrimen, después sólo hay que esperar a alcanzar el resultado de la condena de los ciberterroristas por medio de sentencias de los tribunales internos, en aplicación las leyes internas que hagan punibles los delitos graves contra la protección de datos o los ataques a infraestructuras informáticas.

La puesta al día de la Convención sobre Cibercrimen ha sido largamente debatida,[35] dado el imparable avance de la informática que hace que un texto elaborado y consensuado a finales de la década pasada, hoy resulte obsoleto en varios aspectos. La cooperación internacional y la armonización de legislaciones podrían salir reforzadas de esta revisión, al mismo tiempo que se aproveche para

33. La Convención de 1977 junto a su Protocolo de Enmienda del 2003, abarcan todos los delitos que cubren los convenios sectoriales de Naciones Unidas relativos a actividades terroristas. La Convención asume el principio *aut dedere aut judicare*, que viene a significar que si no se va a extraditar, esos Estados deberían someter los casos a su jurisdicción interna a fin de que sean perseguidos por las autoridades judiciales propias (artículo 4).
34. *Op. cit.*, nota 27, pág. 81-93.

absorber nuevas herramientas y así hacer frente a los actuales riesgos.[36]

Lamentablemente, la Convención sobre el Cibercrimen no tiene el número de ratificaciones que sería deseable.[37] Podríamos decir que los Estados signatarios y todos aquellos otros que quieran acceder –puesto que está abierta a países no miembros del Consejo de Europa–, se lo están tomando con cierta calma, lo que va en detrimento de la prevención de este tipo de delitos que requieren una armonización de las normas nacionales sustantivas, procesales y de cooperación.

3.2. Convención Europea sobre Prevención del Terrorismo

La Convención sobre la Prevención del Terrorismo fue elaborada en 2005 en el seno del Consejo de Europa, aunque está abierta a la participación de todos los países que lo deseen.[38] La Convención propicia una armonización de Derecho penal y con ello facilita la cooperación internacional en materia de prevención y lucha contra el terrorismo.

Según el Preámbulo de la Convención, los actos de terrorismo tienen como propósito por su naturaleza y contexto, intimidar a una población o compeler a un gobierno o a una organización internacional a realizar o a abstenerse de realizar una actividad o a desestabilizar seriamente o destruir la estructura política, constitucional, económica o social de un país o una organización internacional. Y se considerará acto terrorista cualquiera de las infracciones que se prevén en los textos internacionales enumerados en el anexo I de la Convención.

A diferencia de los convenios y tratados internacionales existentes que se dirigen a sancionar el terrorismo una vez que se ha producido el delito, este texto hace especial hincapié en la prevención del terrorismo, impulsando la intervención de las autoridades antes de que los actos terroristas hayan sido cometidos.[39]

Para cumplir con esta obligación, las autoridades nacionales deben mejorar y promover la cooperación en esta materia, intercambiando información, dando protección física a las personas e instalaciones y coordinando los planes de emergencia, entre otras acciones. Igualmente las partes transigen, llegado el caso y en la medida de sus posibilidades, en prestarse mutuamente asistencia y apoyo internacional con el propósito de elevar su capacidad para prevenir la comisión de actos terroristas.

En esta Convención los Estados se comprometen a introducir en su derecho interno como delitos la comisión de cualquier acto o actividad terrorista recogida en los tratados enumerados en su anexo (que son los mencionados en la Resolución 1373 (2001) del Consejo de Seguridad de la ONU), la provocación pública para cometer esos actos, el reclutamiento de personas y su entrenamiento con ese mismo fin, independientemente de que luego se llegue a consumar el acto o actividad terrorista prevista.

Esta es una de las principales novedades de la Convención, ya que, por ejemplo, hasta ese momento pocos países europeos consideraban en sus legislaciones la apología o provocación pública del terrorismo[40]. Además, el artículo 5 fue objeto de profundas reflexiones por parte de un grupo de trabajo dentro del CODEXTER (CODEX-

35. Ver por ejemplo BREYER, P. (2001). «Cyber-crime-Konvention des europarats», *Datenschutz und Datensicherheit*, n.º 25, pág. 592-600 ; DIX, A. (2001). «Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV», *Datenschutz und Datensicherheit,* n.º 25, pág. 588-591.
36. Ver GIACOMELLO, G. (2004). «Bangs for the buck: a cost-benefit análisis of cyberterrorism", *Studies in Conflict & Terrorism*, vol. 27, pág. 387-408.
37. De momento sólo 26 países entre miembros y no miembros del Consejo de Europa han ratificado la Convención sobre Cibercrimen. Como ya hemos señalado, España no es uno de ellos.
38. Hasta la fecha, la han ratificado 19 países, entre ellos España, que depositó su instrumento de ratificación el 27 de febrero de 2009. Para España la Convención es obligatoria desde el pasado 1 de junio de 2009, si bien ya estaba en vigor desde el 1 de junio de 2007 cuando alcanzó la cifra de 6 ratificaciones.
39. Ver NEUMANN, P. (2009). *Old and new terrorism*, Cambridge: Polity Press.
40. La Resolución 1624 (2005) del Consejo de Seguridad de la ONU, de 14 septiembre del 2005, llamaba a todos los Estados a adoptar todas las medidas necesarias y apropiadas y acordes con sus obligaciones de Derecho Internacional para [...] prohibir por ley la incitación para cometer un acto terrorista. La expresión «calls upon States» no denota obligación para los poderes públicos nacionales.

TER-Apología), ya que un problema al que se enfrenta la aplicación de dicha disposición es diferenciar entre apología y libertad de expresión, como derecho fundamental reconocido y amparado por el Convenio Europeo de Derechos Humanos de 1950. Parece claro que sin la intención expresa de incitar a la comisión de actos terroristas y el riesgo de que éstos se cometan, no podrá hablarse de provocación pública. En ambos casos, se trata de elementos muy difíciles de objetivar.[41]

El artículo 6 de la Convención regula el reclutamiento para el terrorismo, calificado este comportamiento como el hecho de enrolar a otra persona para cometer o participar en la comisión de un acto terrorista, o para unirse a una asociación o a un grupo a fin de contribuir a la comisión de una o varias infracciones terroristas. Queda claro que la conducta que se persigue es el acto de reclutamiento en sí mismo, independientemente de si el nuevo afiliado llega a participar efectivamente en actos terroristas.

El entrenamiento terrorista, regulado en el artículo 7 de la Convención, se refiere al hecho de dar instrucciones para la fabricación o utilización de explosivos, de armas de fuego o de otras sustancia nocivas o peligrosas con el objeto de cometer o contribuir a cometer actos terroristas, siempre y cuando el instructor sea consciente de que esa formación tiene por objeto servir para la perpetración de dichos actos.

Nótese que tanto la provocación pública, como el reclutamiento y, hasta cierto punto, el entrenamiento para el terrorismo son conductas que pueden desarrollarse a través de medios informáticos[42]. Es decir, es importante en este punto tener en cuenta que los actos terroristas constituyen un comportamiento que cuando tiene lugar a través de Internet caerá dentro del marco de aplicación tanto de la Convención sobre Cibercrimen del 2001, como de la presente Convención sobre Prevención del Terrorismo del 2005.

En la misma medida, las partes en la Convención se comprometen a establecer penas efectivas, apropiadas y disuasorias para los terroristas, con relación a todos los actos que se consideran terroristas según este instrumento, así como para la tentativa y la complicidad. La tentativa tiene mucho que ver con el reclutamiento y el entrenamiento, ya que es de estas conductas de donde puede deducirse. La complicidad, por su parte, se relaciona más con la organización y contribución a la comisión de los actos terroristas, conceptos que no han quedado concretados ni en la Convención ni en el informe explicativo de la misma. Todas estas actuaciones pueden llevarse a cabo a través de la red y con la ayuda de las nuevas tecnologías.

Por otro lado, el Consejo de Europa se preocupa por armonizar las iniciativas para acabar con el terrorismo internacional con la garantía que lo caracteriza de protección de los derechos humanos.[43] Las partes se ven compelidas a adoptar las medidas necesarias para prevenir las acciones terroristas y sus efectos negativos, siempre desde el respeto del Estado de derecho, los valores democráticos, la protección de los derechos humanos[44] y las demás normas de derecho Internacional, incluyendo las del derecho internacional humanitario.

Sin embargo, hay que tener en cuenta que los efectos de las propias acciones terroristas atentan claramente contra los derechos humanos garantizados en distintos instrumentos internacionales, especialmente contra el derecho a

41. El informe explicativo no aclara nada acerca de la intencionalidad. Sin embargo, respecto al riesgo dice que para evaluarlo, habrá que tener en cuenta quiénes son el autor y el destinatario del mensaje, así como el contexto en el que se produce la incitación de conformidad con la jurisprudencia del TEDH. También deben considerarse la significación y la credibilidad del riesgo, de acuerdo con la legislación interna.
42. Pensemos en los manuales para fabricar bombas, venenos y otras armas con el fin de cometer atentados, que muchas organizaciones terroristas están colgando en la red.
43. Guidelines on human rights and the fight against terrorism, adopted by the Committee of Ministers on 11 July 2002, Directorate General of Human Rights, December 2002.
44. Ver también las referidas Directrices sobre derechos humanos y lucha contra el terrorismo de 11 de Julio de 2002 y la Recomendación (2005) 10 del Comité de Ministros, relativa a las técnicas especiales de investigación en relación con infracciones graves, inclusive los actos de terrorismo, de 10 de abril de 2005.

la vida[45], pero también contra otros relacionados con el empleo de las nuevas tecnologías, como el respeto a la vida privada.[46] Por ello, debemos destacar que se trata del primer convenio que establece una obligación en derecho internacional de proteger a las víctimas del terrorismo.[47]

Entre los Estados parte existe la obligación de ayuda mutua en relación con las investigaciones y procedimientos penales y de extradición abiertos.[48] La finalidad última de esta disposición es la de intercambiar información por todos los mecanismos que los Estados puedan establecer en su derecho interno como forma de cooperación internacional, eso sí, siempre con pleno respeto a las obligaciones relativas a los derechos humanos.[49]

Según el artículo 18, el Estado que no conceda la extradición, se compromete a someter el asunto a las autoridades internas competentes, sin dilación indebida y sin ningún tipo de excepción, para el ejercicio de la acción penal (principio *aut dedere aut judicare*). Además, en la línea de lo dispuesto en el Convenio de 1977 enmendado por el Protocolo del 2003, el artículo 20 incluye la «exclusión de la cláusula de excepción política» para las infracciones reguladas en los artículos 5 a 7 y 9 de la Convención, para las cuales no puede ser denegada la extradición, aunque el párrafo 2 permite la formulación de reservas a este artículo 20.1.

Tanto la ONU como la Organización para la Seguridad y la Cooperación en Europa (OSCE) han saludado la adopción de esta Convención y recomendado su ratificación. A su vez, la Unión Europea ha decidido incluir en su decisión marco sobre lucha contra el terrorismo los tres nuevos delitos tipificados en la Convención.[50] Se trata de un efecto muy positivo de la Convención que ha creado una nueva dinámica y un consenso a nivel al menos regional europeo, si no internacional, sobre la necesidad de aunar esfuerzos en la prevención y no sólo en la lucha contra el terrorismo.

Parece muy precipitado lanzar una llamada a la revisión de este reciente instrumento. Si bien es verdad que algunas de las amenazas actuales en manos de los terroristas no están adecuadamente cubiertas en su catálogo de actos terroristas, una lógica y precisa interpretación de sus disposiciones puestas en conjunción con el resto de textos del Consejo de Europa y de otras organizaciones internacionales, sin duda permitirá cubrir los diversos supuestos que se den en la práctica ciberterrorista.

Conclusión

El ciberterrorismo, contra o por vía de Internet, supone un riesgo significativo desde que los sistemas informáticos hoy en día son responsables de llevar a cabo muchas funciones esenciales de nuestra sociedad. Los cibercriminales pueden atacar todo aquello que es importante para la sociedad moderna y esté conectado a Internet o accesible por otras líneas de comunicación. Luego los terroristas tienen en sus manos la posibilidad de usar las mismas técnicas y adquirir los mismos conocimientos y

45. Precisamente en el marco del Consejo de Europa, el artículo 2 del Convenio Europeo de Derechos Humanos de 1950 dice: «*1. El derecho de toda persona a la vida está protegido por la Ley. Nadie podrá ser privado de su vida intencionadamente, salvo en ejecución de una condena que imponga pena capital dictada por un tribunal al reo de un delito para el que la ley establece esa pena*».
46. El artículo 8.1 del Convenio Europeo de Derechos Humanos garantiza lo siguiente: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia». Obvia señalar la interferencia en la vida privada de una persona que supone cualquier clase de manipulación de sus datos a través de Internet.
47. Esta disposición, según indicó el coordinador antiterrorista del Consejo de Europa, se incluyó a petición de la delegación española durante la negociación del texto, tras superar importantes problemas. Algunas delegaciones se habían mostrado contrarias a que se introdujera dicha disposición en el texto de la Convención, habida cuenta de su carácter eminentemente preventivo. Finalmente, se decidió incluir al menos una disposición de carácter general dado el papel central que deben representar las víctimas en la lucha contra el terrorismo.
48. En el marco del Consejo de Europa, existe una obligación general conforme al Convenio Europeo sobre Extradición de 1957 y sus Protocolos adicionales de 1975 y 1978. Igualmente, no podemos obviar el Convenio Europeo sobre Asistencia Mutua en Materia Penal de 1959 y sus Protocolos de 1978 y 2001.
49. FITZPATRICK, J. (2003). «Speaking law to power: the war against terrorism and human rights», *European Journal of International Law*, vol. 14, n.º 2, pág. 241-264.
50. Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, DO L 330 de 9.12.2008, pág. 21.

herramientas que el resto de los criminales, con el fin de lograr crear un clima de terror que facilite la consecución de sus aspiraciones.

Este tipo de ataques utilizando Internet podrían causar daños en sistemas informáticos, así como en la integridad física de las personas y sus bienes. Además, los terroristas emplean habitualmente la red y las nuevas tecnologías para diseminar contenido ilegal y para la preparación logística de los actos terroristas.

Las convenciones e instrumentos específicos sobre cibercriminalidad, que abocan a la armonización de las normas sustantivas y procedimentales nacionales y a la cooperación internacional en dicho ámbito, son aplicables a la persecución del ciberterrorismo y otros usos de Internet con fines terroristas. Igualmente, las normas sustantivas, procedimentales y de cooperación incluidas en otros instrumentos sobre terrorismo, sobre blanqueo de dinero, sobre financiación de actividades terroristas, sobre mutua asistencia o extradición son también aplicables al ciberterrorismo desde que son formuladas de manera general y así pueden ser utilizadas en el entorno de las nuevas tecnologías.

Con ello, queremos dejar sentado que no existen lagunas trascendentales respecto al ciberterrorismo en las convenciones exclusivas sobre ciberdelincuencia, como tampoco las hay respecto a la utilización de la informática para cometer los ilícitos perseguidos en las convenciones específicas sobre terrorismo. De la combinación de ambas clases de instrumentos internacionales, podemos obtener una regulación casi completa del fenómeno ciberterrorista.

Como bien señala el informe de los expertos, el mayor problema se centra en la falta de ratificaciones de los instrumentos ya existentes. Una participación lo más amplia posible tanto en la Convención sobre Cibercrimen, como en la Convención sobre Supresión del Terrorismo, resulta esencial para combatir el ciberterrorismo y otros usos de Internet con propósitos terroristas. Y este es el campo en el que hay que trabajar, más que estar pensando en sus virtuales reformas. Evidentemente, todos los instrumentos analizados tienen cosas mejorables y a muchos de ellos una puesta al día tampoco les vendría mal.

Cuando nos adentramos en el campo de las nuevas tecnologías, es difícil decidir si todo lo que hemos tratado aquí es fruto de un exagerado «cibertemor» o el ciberterrorismo es una amenaza veraz e inminente. Hay opiniones para todos los gustos: algunos piensan que un ataque de estas características no ha tenido lugar nunca y la amenaza no existe porque las consecuencias serían de muy escaso relieve,[51] mientras otros se muestran mucho más cautos y aseguran que el riesgo es auténtico.[52]

Sin duda, las conductas conocidas como «ciberterrorismo» tienen mucho más que ver con la apología, el reclutamiento y, en menor medida, el entrenamiento terrorista, así como con la adquisición de información, la comunicación interna y el análisis de objetivos utilizando la Red de redes, que con un ataque de «hacker-terroristas» que ponga en peligro el sistema electrónico de comunicaciones a nivel mundial que significa Internet y las diversas infraestructuras que dependen de él.[53]

Sin embargo, no debemos subestimar el potencial de la amenaza ciberterrorista. Tenemos ante nosotros a una nueva generación de jóvenes terroristas que ha crecido en la era digital, familiarizados con los ordenadores. Las capacidades y herramientas necesarias para un atentado cibernético están a su disposición de manera gratuita y fácil de manejar. Tampoco faltan patrocinadores entre ciudadanos «altruistas», empresas, organizaciones e, incluso, gobiernos, que garantizarán la financiación. El

51. Ver GREEN, J. (2002). «The myth of cyberterrorim», *Washington Monthly*, vol. 34, n.º 11, pág. 8-13; SANDWELL, B. (2006). «Monsters in cyberespace, cyberphobia and cultural panic in the information age», *Information, Communication & Society*, vol. 9, n.º 1, pág. 39-61.
52. WEIMANN, G. (2005). «Cyberterrorism: the sum of all fears?», *Studies in Conflict & Terrorism*, vol. 28, pág. 129-149.
53. La mayoría de los expertos coincide en señalar este hecho, poniendo en duda la posibilidad práctica de un ataque de ciberterrorismo con resultados catastróficos, lo que se ha llamado *Electronic Pearl Harbor*. Denning decía en un artículo publicado unas semanas antes del 11-S: «Whereas hacktivism is real and widespread, cyberterrorism exists only in theory. Terrorist groups are using Internet, but they still prefer bombs to bytes as a means of inciting terror»; DENNING, D. (2001). «Hacker warriors: rebels, freedom fighters, and terrorists turn to cyberspace», *Harvard International Review*, verano, pág. 6. Ver también CONWAY, *op. cit.*, pág. 5. Sin embargo, Verton imagina y describe cómo sería un ataque ciberterrorista, a la vez que alerta sobre su peligro en nuestros días; VERTON, D. (2003). *Black ice: the invisible threat of cyberterrorism*, Nueva York: McGraw-Hill, pág. 13-15.

anonimato, la dificultad en la persecución y la innecesaria presencia física en el lugar del atentado siguen siendo ventajas a considerar de manera muy positiva por los terroristas. La posibilidad de ataques a gran escala y con consecuencias que se pueden fácilmente ir alargando en el tiempo, convierte los asaltos digitales en altamente atractivos.[54] La creatividad humana aplicada al lado oscuro del mal, es ilimitada, lo cual se demostró con los retorcidos métodos terroristas utilizados el 11-S y el 11-M, impensables para la mayoría de nosotros.

Bibliografía

ARQUILLA, J.; RONFELDT, D. (1993). «Cyberwar is coming!». *Comparative Strategy*. Vol. 12, n.º 2, pág. 141-165.

BENDRATH, R. (2003). «The American cyber-angst and the real world: Any link?». En: R. LATHAM (ed). *Bombs and bandwidth: the emerging relationship between information technology and security*. Nueva York: The New Press. Pág. 49-73.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES-CSIS (1998). *Cybercrime, cyberterrorism, cyberwarfare: averting an electronic Waterloo*. Washington DC: CSIS Press.

COLLIN, B. (1996). «The future of cyberterrorism». En: *11th Annual International Symposium on Criminal Justice Issues* (Chicago: University of Illinois at Chicago) [ponencia en línea]. [Fecha de consulta: 30 de abril de 2009].
<http://afgen.com/terrorism1.html>

CONWAY, M. (2008). «Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructures». *Working Papers in International Studies Series*. N.º 2008-5. Centre for International Studies, Dublin City University, Irlanda.

COSTIGAN, S. (2007). «Terrorists and the Internet: crashing or cashing in?». En: S. COSTIGAN; D. GOLD. *Terrornomics*. Asdershot/ Burlington: Ashgate. Pág. 113-128.

DAUKANTAS, P. (2001). «Professors hash out emergency response, cyberterrorism strategies». *Government Computer News* [artículo en línea]. [Fecha de consulta: 30 de abril de 2009].
<http://gcn.com/articles/2001/12/14/professors-hash-out-emergency-response-cyberterrorism-strategies.aspx?sc_lang=en>

DENNING, D. (2003). «Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy» [en línea]. En: John Arquilla, David Ronfeldt (ed.) (2003). *Networks and Netwars. The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand Corporation. [Fecha de consulta: 30 de abril de 2009].
<http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf>

EMBAR-SEDDON, A. (2002). «Cyberterrorism: Are we under siege?». *American Behavioral Scientist*. Vol. 45, n.º 6, pág. 1033-1043.

ERIKSSON, J.; NOREEN, E. (2002). «Setting the agenda of threats: An explanatory model». *Uppsala Peace Research Papers*. Vol. 6, 26 pág.

GORDON, S. ; FORD, R. (2003). «Cyberterrorism?». *Symantec Security Response White Paper*. Marzo 2003. 16 pág.

INGLES-LE NOBLE, J. (1999). «Cyberterrorism hype». *Jane's Intelligence Review*. Vol. 1, 10 pág.

54. Ver GERCKE, M. (2007). «Cyberterrorismus –Aktivitäten terroristischer organisationen im Internet», *Computer und Recht*, vol. 23, n.º1, pág. 62-68.

JANCZEWSKI, I.; COLARIK, A. (2008). *Cyber warfare and cyber terrorism*. Hershey: Information Science Reference.

MATUSITZ, J. (2008). «Cyberterrorism: postmodern state of chaos». *Information Security Journal*. Vol. 17, n.º 4, pág. 179-187.

SCHWARTAU, W. (ed.) (1994). *Information warfare. Cyberterrorism: protecting your personal security in the electronic age*. New York: Thunder's Mouth Press.

VATIS, M. A. (2001). «Cyber attacks during the war on terrorism: a predictive analysis». *Institute for Security Technology Studies at Dartmouth College Reports*. Vol. 22, 29 pág.

WILSON, C. (2005). «Computer attacks and cyberterrorism: vulnerabilities and policy issues for congress». *Congressional Research Service Report for Congress (RL32114)*. 1 Abril 2005. 46 pág.

Cita recomendada

CHICHARRO, Alicia (2009). «La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa]

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_chicharro/n9_chicharro_esp>

ISSN 1699-8154

Sobre la autora

Dra. Alicia Chicharro Lázaro
alicia.chicharro@unavarra.es

Doctora en Derecho por la Universidad Pública de Navarra. De 1995 a 1999, beca FPI (MEC). Del 2001 al 2003, fue colaboradora externa de la editorial Aranzadi como analista de sentencias del TJCE, y entre el 2002 y el 2009, profesora ayudante en la UPNA. Actualmente es profesora asociada en el Departamento de Derecho público de esta Universidad y juez sustituta en los Juzgados de Navarra. Ha participado en estancias de investigación en centros extranjeros, como la Universidad de Oxford, el Max-Planck-Institut o la Comisión Europea. Autora de algunas publicaciones, como «La lucha contra el terrorismo internacional: regulación internacional y europea» (2007), en *Temas Actuales de Derecho*, Pamplona: UPNA, y *El principio de subsidiariedad en la Unión Europea* (2001), Pamplona: Aranzadi.

Departamento de Derecho público
Universidad Pública de Navarra
Campus de Arrosadía
31006 Pamplona, España

UOC
Universitat Oberta de Catalunya
www.uoc.edu