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

http://idp.uoc.edu

ARTICLE

La tasca legislativa del Consell d'Europa davant la utilització d'Internet amb finalitats terroristes

Alicia Chicharro Lázaro

Data de presentació: setembre de 2009
Data d'acceptació: novembre de 2009
Data de publicació: desembre de 2009

Resum
El terme *ciberterrorisme* salta a la llum pública en grans titulars periodístics a finals del segle passat i principis del present, particularment, a partir dels atemptats de l'11-S a Nova York. Es tracta de la forma de terrorisme que empra les tecnologies de la informació i la comunicació per a sotmetre els poders públics, certs individus o grups de la societat o, de manera general, l'opinió pública a un clima de terror, a fi d'aconseguir les seves aspiracions.
El ciberterrorisme contra Internet o per via d'Internet representa un risc significatiu avui en dia, quan els sistemes informàtics són responsables de dur a terme moltes funcions essencials de la nostra societat.

Tanmateix, la persecució de la majoria d'aquests crims és complexa a causa de la naturalesa tècnica d'Internet i a la dimensió internacional del fenomen del ciberterrorisme, que requereix un tractament coordinat entre el màxim nombre possible de països.

En el si del Consell d'Europa s'han adoptat dues importants convencions que, posades en conjunció, permetran fer front a aquests comportaments delictius: la Convenció sobre Cibercrim de l'any 2001 i la Convenció per a la Prevenció del Terrorisme de l'any 2005. L'adaptació de la legislació interna a aquests instruments proporcionarà als estats una cobertura adequada per a perseguir els crims associats a l'ús d'Internet amb fins terroristes.

Paraules clau
ciberterrorisme, Consell d'Europa, cibercrimen, terrorisme

Tema
E-justícia

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. Introducció

L'època actual ha estat qualificada com l'«era digital». La revolució que han suposat les noves tecnologies de la informació i la comunicació (TIC), particularment a través del desenvolupament vertiginós d'Internet, contribueix al fenomen de la globalització i trenca amb les tradicionals fronteres espaciotemporals. Ens situem en la denominada *societat de la informació,* on qualsevol ordinador connectat a Internet es converteix en un mitjà de comunicació accessible a pràcticament tothom.[1] Això inclou també els delinqüents i, particularment, els terroristes. La conjunció de tecnologia i terrorisme provoca incertesa i un alt grau d'inseguretat quan pensem en el futur.[2]

El terme *ciberterrorisme* salta a la llum pública en grans titulars periodístics a finals del segle passat i principis del present, particularment a partir dels atemptats de l'11-S als Estats Units,[3] encara que va ser un investigador de

1. NICANDER, L.; RANSTORP, M. (ed.) (2004). *Terrorism in the information age: new frontiers?*. Estocolm: National Defense College.
2. Vegeu LAQUEUR, W. (1999). *The new terrorism: fanatism and the arms of mass destruction*. Oxford: Oxford University, pág. 254. A *The New Yorker* apareixia un article el 2001, signat per Specter, que predeia el següent: «The Internet is waiting for its Chernobyl, and I do not think we will be waiting much longer» [article en línia].
3. *San Francisco Chronicle* el maig de 1997, Los Angeles Times el febrer de 2001, el Boston Herald al juny, el Washington Post al setembre, la revista *Time* al novembre, el *Bristol Herald Courrier* al desembre (tots del mateix any) o el USA Today el juny de 2002, són alguns dels principals rotatius nord-americans que han dedicat titulars al «ciberterrorisme» i, en la majoria dels casos, a l'alarmant amenaça que aquest representa.

l'Institut per a la Seguretat i la Intel·ligència de Califòrnia, Barry Collin, qui va encunyar el terme als anys vuitanta.

Aconseguir una definició precisa del que s'entén per *ciberterrorisme* requereix partir d'una sèrie de premisses que suposen certs obstacles. En primer lloc, el debat entorn de aquest fenomen s'ha dut a terme majoritàriament a través de mitjans informals que tracten de donar a entendre el concepte més que a establir una definició operacional i comprensiva del nou terme. En una època en la qual la informació esdevé coneixement, és difícil distingir el ciberterrorisme de la seva representació mediàtica. En segon lloc, la sobreexplotació que ha patit aquest vocable a partir de l'11-S, l'ha convertit en una paraula rumor (*buzzword*) que pot tenir significats dissímils per a diferents persones. En tercer lloc, en l'entorn de la informàtica i particularment d'Internet, és molt habitual la creació de noves veus o bé a partir del prefix *ciber,* o bé afegint-hi els adjectius *informàtic/a*, *electrònic/a*, *virtual o digital*. Finalment, el màxim impediment per a establir el concepte de ciberterrorisme és precisament la falta d'acord sobre la definició de terrorisme.

Tot això comporta que no hi hagi una sola definició comunament acceptada de *ciberterrorisme*, de la mateixa manera que no n'hi ha de *terrorisme*.

Es tracta d'una composició realitzada a partir de l'arrel *ciber* i la paraula *terrorisme*.[4] L'arrel *ciber* està relacionada amb la tecnologia.[5] Per a l'expressió *terrorisme* hem de tornar a l'eterna discussió sobre el seu concepte, que ha fet córrer rius de tinta sense que s'hagi arribat a un acord general.[6]

Sí que en tenim definicions en textos normatius interns[7] i en instruments internacionals però d'àmbit regional.[8] Fins i tot podríem trobar algun avenç cap a una precisió del concepte en els tractats sectorials més recents elaborats sota els auspicis de les Nacions Unides[9] i en els treballs preparatoris del Tractat general sobre el terrorisme, l'adopció del qual troba en la definició del fenomen terrorista la trava més important.

L'Assemblea Parlamentària del Consell d'Europa considera que un acte de terrorisme és qualsevol delicte comès per individus o grups recorrent a la violència o amenaçant d'utilitzar-la contra un país, les seves institucions, la seva població en general o sobre individus concrets, que, motivat per aspiracions separatistes, concepcions ideològiques extremistes o fanatisme, o inspirat per mòbils irracionals o subjectius, té per objecte sotmetre els poders públics, certs individus o grups de la societat o, de manera general, l'opinió pública, a un clima de terror.[10]

4. Vegeu DESOUZA, K.; HENSGEN, T. (2003). «Semiotic emergent framework to address the reality of cyberterrorism», *Technological Forecasting and Social Change*, vol. 70, núm. 4, pàg. 385-396.
5. *Cibernètica* és un terme que hem importat de l'anglès i que es refereix a l'estudi de les analogies entre els sistemes de control i comunicació dels éssers vius i els de les màquines; i, en particular el de les aplicacions dels mecanismes de regulació biològica a la tecnologia. L'origen més remot el trobem en la paraula grega , que significa l''art de governar una nau'.
6. Vegeu, per exemple, 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*, set., pàg. 753-771; ROBERTS, A. (2002). «Can we define terrorism?», *Oxford Today*, núm. 14, pàg. 18-24; SKUBISZEWSKI, K. (1989). «Definition of terrorism», *International Yearbook of Human Rights*, vol. 19, pàg. 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, pàg. 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*». A Espanya, si prenem els articles 571 a 577 del Codi penal podem considerar terroristes «els qui, tant si pertanyen com si no a banda armada, organització o grup terrorista, i amb la finalitat de subvertir l'ordre constitucional o d'alterar greument la pau pública, o la de contribuir a aquestes finalitats atemorint els habitants d'una població o els membres d'un col·lectiu social polític o professional, cometin homicidis, lesions, detencions il·legals, segrestos, amenaces o coaccions contra les persones, o duguin a terme qualssevol delictes d'incendis, estralls, danys o tinença, fabricació, dipòsit, tràfic, transport o subministrament d'armes, municions o substàncies o aparells explosius, inflamables, incendiaris o asfixiants, o dels seus components».
8. Especialment importants són les definicions a què s'ha arribat tant en el Consell d'Europa, que serà objecte d'estudi en aquest treball, com en la Unió Europea (Decisió marc 2002/475/JAI del Consell, sobre lluita contra el terrorisme, DG. L 164, 22.6.2002, pàg. 3).
9. Article 2 del Conveni internacional per a la repressió del finançament del terrorisme de 1999.
10. Recommendation 1426 (1999), European democracies facing up to terrorism (23 September 1999), pàg. 5.

Així, *ciberterrorisme* serà la forma de terrorisme que empra les tecnologies de la informació i la comunicació per a sotmetre els poders públics, certs individus o grups de la societat o, de manera general, l'opinió pública, a un clima de terror, a fi d'aconseguir les seves aspiracions.

Comparada amb d'altres,[11] aquesta definició permet integrar qualsevol tipus d'atac contra els ordinadors, xarxes o la informació que hi continguin, així com qualsevol atemptat executat utilitzant-los, fins i tot aquell que no produeixi danys en l'espai físic sinó només en el «món virtual».[12]

2. La utilització d'Internet amb finalitats terroristes

Junt amb l'amenaça ferotgement real que suposen els atacs terroristes viscuts els últims anys, hem d'abordar un altre risc aquesta vegada més virtual que comportaria l'ús dels sistemes informàtics i, sobretot, d'Internet per a finalitats terroristes.[13]

Internet, la Xarxa de xarxes, va néixer de la idea i de la necessitat d'establir múltiples canals de comunicació entre ordinadors.[14]

Amb el desenvolupament de les tecnologies de la informació també es va obrir una comporta per a cometre de delictes per mitjà d'aquestes. Històricament, les lleis penals sorgeixen com a resposta a les activitats que produeixen dany a la societat i amb l'aparició dels ordinadors, van començar a emergir nous delictes i la preocupació per castigar certes conductes que van rebre el nom de *delictes informàtics o cibercrimens*.

En sentit estricte, els delictes informàtics són aquells establerts per la llei als efectes de protegir de manera integral els sistemes que utilitzin tecnologies d'informació, així com de prevenir i sancionar les infraccions comeses contra tals sistemes o qualsevol dels seus components. En sentit ampli, s'emmarquen en aquesta categoria totes les conductes delictives ja tipificades per la legislació criminal d'un país quan el tipus penal ho permet i es cometen a través de l'ús de l'ordinador.[15]

El ciberterrorisme és una conducta il·lícita de les denominades *cibercrims* o *delictes informàtics*, en les quals un element essencial és la utilització d'ordinadors com a instruments o com a objectius que produeixen un clima de terror, perquè es doni el tipus penal.

El ciberterrorisme, quan té per objectiu Internet o es du a terme per aquesta via, representa una amenaça seriosa, ja que molts aspectes essencials de la societat actual depenen del funcionament correcte dels sistemes informàtics.[16] La informàtica està present en la vida quotidiana d'una part important dels habitants del planeta. Les administracions públiques estan plenament integrades en l'era

11. Per exemple Devost, Houghton i Pollard ofereixen una definició de *terrorisme informàtic* com «l'abús intencionat d'un sistema, xarxa o component d'informació digital, a fi de donar suport a una campanya o una acció terrorista o facilitar-la»; DEVOST, M.; HOUGHTON, B.; POLLARD, N. (1997). «Information terrorism: political violence in the information age», *Terrorism and Political Violence*, vol. 9, núm. 1, pàg. 75. Els mateixos autors el consideren «the nexos between criminal information system fraud or abuse, and the physical violence of terrorism»; «Information terrorism: Can you trust your toaster?» [article en línia]. *The Terrorism Research Center*. [Data de consulta: 30 d'abril de 2009]. Denning el defineix de la següent 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*. [Data de consulta: 30 d'abril de 2009]. Vegeu també IQBAL, M. (2004). «Defining cyberterrorism», *John Marshall Journal of Computer and Information Law*, vol. 22, núm. 2, pàg. 397-408.
12. Vegeu MATES, M. (rep.) (2001). *Technology and terrorism*, Bruselas: OTAN, pàg. 3.
13. Vegeu NEUMANN, P. (2008). *The strategy of terrorism*, Londres-Nova York: Routledge.
14. En un primer moment, es tractava de garantir les telecomunicacions militars amb finalitats de seguretat i defensa als EUA, però ràpidament es va expandir creant una xarxa pública per a l'ús de les universitats.
15. Vegeu SCHELL, B.; MARTIN, C. (2004). *Cybercrime: A reference handbook,* Santa Bárbara: ABC-CLIO.
16. Vegeu MATUSITZ, J. (2005). «Cyberterrorism», *American Foreign Policy Interests*, vol. 27, núm. 2, pàg. 137-147.

digital, controlant-ne els serveis a través d'ordinadors. L'empresa privada incorpora les noves tecnologies per reduir costos i augmentar beneficis. A qualsevol part del món es pren nota, es registra i s'arxiva utilitzant mitjans telemàtics. Els servidors emmagatzemen quantitats ingents de dades, algunes confidencials o de caràcter personal, que han de ser protegides. La dependència que la societat actual en té és innegable, amb la qual cosa no podem ignorar o negar l'amenaça que això comporta.

La globalització econòmica comporta també la mundialització dels perills i l'expansió del terrorisme internacional n'és un. Al seu torn, una generació de terroristes experts en informàtica que utilitzen les noves tecnologies per als seus propòsits posa en risc tant els propis sistemes informàtics com les persones físiques i els seus béns que poden ser atacats mitjançant l'ús fraudulent de la informàtica.[17]

Quan analitzem aquesta amenaça i avaluem les possibles respostes legals, és necessari distingir tres fenòmens:[18]

a. atacs per mitjà d'Internet que causin danys no solament als sistemes electrònics de comunicació bàsics i a la infraestructura de tecnologies de la informació i la comunicació (TIC), sinó també a altres infraestructures, sistemes i interessos jurídics, inclosa la vida humana;[19]

b. propagació de contingut il·legal, inclosa l'amenaça d'atacs terroristes; incitar al terrorisme, anunciar-lo i glorificar-lo; captar fons i finançar el terrorisme; entrenar els terroristes; reclutar persones per al terrorisme; i disseminar material racista o xenòfob;

c. altres usos logístics de les TIC pels terroristes, com la comunicació interna, l'adquisició d'informació i l'anàlisi d'objectius.

Les noves formes de cibercrim, així com la comissió de delictes tradicionals utilitzant en algun moment xarxes informàtiques, planteja la necessària evolució de les normes penals substantives, dels mètodes de recerca i enjudiciament i de les mesures de prevenció. Els problemes sorgeixen de la complexitat tècnica dels entorns informàtics, la multitud i invisibilitat de les dades electròniques, de la proliferació de tècniques d'encriptació i ocultació de continguts,[20] la dificultat d'identificar els culpables a Internet, del fet que un sistema informàtic pot ser atacat des de la distància i de la naturalesa global d'Internet, la qual no pot ser controlada amb mesures purament nacionals.[21]

Per tot això, el més desitjable seria disposar d'instruments internacionals que regulin el problema i que aboquin els estats a harmonitzar les seves lleis penals, així com a cooperar en la recerca, persecució i càstig dels culpables. El gran obstacle global té dos vessants: la inexistència de normativa sobre cibercriminalitat i la legislació sectorial sobre terrorisme. En l'àmbit regional europeu, tanmateix, tenim prou instruments tant en el Consell d'Europa com en la UE.[22] Aquí analitzarem la tasca desenvolupada pel Consell d'Europa.

17. Vegeu 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, núm. 2, pàg. 97-122.
18. Informe dels experts preparat pels professors Sieber i Brunst del Max Planck Institute for Foreign and International Criminal Law de Freiburg (Alemanya): COUNCIL OF EUROPE (2007). *Cyberterrorism - The use of the Internet for terrorist purposes*, Estrasburg: Council of Europe Publishing.
19. Vegeu COHEN, F. (2003). «Cyber-risks and critical infrastructures», *Strategic Security*, vol. 27, núm. 2, pàg. 1-10.
20. Vegeu CONWAY, M. (2008). «Code wars: stenography, signals intelligence, and terrorism», *Dublin City University International Studies Working Papers*, vol. 6, 19 pàg.
21. Vegeu COULTHARD, A. (2003). «Cyber terrorism: beyond the hype». A: *Proceeding of the European Conference on Information Warfare and Security 2002*, Londres: Academic Conferences Ltd., pàg. 57-65.
22. Vegeu 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*, Vitòria: Universidad del País Vasco, pàg. 191-263.

3. La lluita contra la cibercriminalitat i el terrorisme en el marc del Consell d'Europa

La persecució de la majoria d'aquests crims és complexa a causa de la naturalesa tècnica d'Internet i a la dimensió internacional del fenomen del ciberterrorismo,[23] que requereix un tractament coordinat entre el màxim nombre possible de països.

En el si del Consell d'Europa[24] s'han adoptat dues importants convencions que, posades en conjunció, permetran fer front als comportaments delictius comesos a través de vies fins ara poc explorades, però que obren moltes possibilitats als terroristes[25]. Aquestes són la Convenció sobre Cibercrim de 2001 i la Convenció per a la Prevenció del Terrorisme de 2005. Analitzarem si l'instrument específic sobre delictes informàtics és aplicable també al terrorisme i si el text específic sobre terrorisme es pot aplicar també al terreny de les noves tecnologies[26]. En definitiva, si prenent ambdós instruments obtenim una cobertura adequada per a perseguir els crims associats a l'ús d'Internet amb finalitats terroristes.[27]

En qualsevol cas, la persecució i el processament dels delictes relacionats amb el ciberterrorisme mai no significarà una disminució en la protecció dels drets humans i les llibertats fonamentals, com queden garantits en el CEDH de 1950 i els seus protocols addicionals.[28]

3.1. La Convenció Europea sobre Cibercrim

La Convenció Europea sobre Cibercrim de 23 de novembre de 2001 és l'instrument internacional més complet sobre delictes comesos contra ordinadors o a través d'ordinadors.[29] Inclou obligacions sobre normes penals substantives, procediments penals i cooperació internacional en aquest camp.[30] Sens dubte, aquest text pot ser usat en casos de terrorisme, precisament quan aquest delicte sigui comès contra sistemes informàtics o a través de sistemes informàtics.

Els articles 2 i 3 de la Convenció cobreixen les tècniques utilitzades per *hackers* i que serveixen per a accedir a l'ordinador de la víctima i interceptar-ne dades informàtiques. Al seu torn, els articles 4 i 5 de la Convenció es refereixen a danyar, esborrar, alterar o suprimir dades informàtiques o interferir en tot el sistema, obligant les parts a adoptar mesures legislatives o d'un altre tipus contra tots aquests comportaments.

Aquests dos últims articles cobreixen qualsevol conducta que tingui per objectiu la interferència en dades i sistemes informàtics que, com ja hem vist, és un prerequisit per als atemptats terroristes a través d'Internet. L'informe explicatiu de la Convenció afirma que l'article 5 està formulat d'una manera neutral perquè pugui protegir totes les classes de funcions. Això significa que qualsevol tipus d'atac terrorista contra sistemes informàtics, inclosos els que afectin béns i persones, cau en el camp d'aplicació dels articles 4 i 5 de la Convenció sobre Cibercrim.

23. SIEBER, U. (2006). «International cooperation against terrorist use of Internet», *Revue Internationale de Droit Pén*al, vol. 77, pàg. 395-449.
24. En l'actualitat formen part d'aquesta organització internacional d'àmbit regional europeu 47 estats.
25. VERTON, D. (2003). *Black ice: the invisible threat of cyberterrorism*, Nova York: McGraw-Hill.
26. Per a l'anàlisi del dèficit que presenten les convencions internacionals sobre terrorisme, vegeu TOMOUSCHAT, C. (2005). «On the possible 'added value' of a comprehensive Convention on Terrorism», *Human Rights Law Journal*, núm. 26, pàg. 287-306.
27. El 2007 es va elaborar un informe d'experts sobre ciberterrorisme en què s'adverteix dels riscos i s'analitzen les respostes que les normes elaborades en el si del Consell d'Europa poden donar a aquest fenomen: COUNCIL OF EUROPE (2007). *Cyberterrorism - The use of the Internet for terrorist purposes*, Estrasburg: Council of Europe Publishing.
28. Vegeu VON SCHORLEMER, S. (2003). «Human rights: substantive and institutional implications of the war against terrorism», *European Journal of International Law*, vol. 14, núm. 2, pàg. 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*, Brussel·ls: Bruylant.
29. La Convenció va entrar en vigor l'1 de juliol de 2004. Espanya de moment no l'ha ratificat.
30. Crida l'atenció la lentitud amb què els estats estan accedint a aquest instrument. Només té 26 ratificacions. Espanya no n'és part de moment. Vegeu GERCKE, M. (2006). «The slow wake of a global approach against cybercrime», *Computer Law Review Internationa*l, núm. 5, pàg. 140-145.

L'article 6 tracta de l'abús d'equips i instruments tècnics i preveu que les parts adoptaran les mesures legislatives o d'un altre tipus que s'estimin necessàries per a preveure com a infracció penal, d'acord amb el seu dret intern, la producció, venda, obtenció per a la seva utilització, importació, difusió o altres formes de posada a disposició de dispositius que permetin cometre infraccions, paraules clau, codis d'accés o dades informàtics similars, o la possessió d'algun dels elements abans descrits amb la intenció d'utilitzar-los com a mitjà per a cometre alguna de les infraccions previstes en els articles 2 a 5.

Respecte a la utilització d'Internet per a finalitats terroristes, els articles 2, 3 i 6 atorguen una protecció addicional, permetent que els possibles autors siguin perseguits de forma diligent.

Les disposicions de la Convenció preveuen la comissió d'aquests actes, la temptativa i la complicitat, així com la responsabilitat de les persones jurídiques (articles 11 i 12). Les parts adoptaran les mesures legislatives o d'un altre tipus que s'estimin necessàries per a permetre que les infraccions penals establertes en la Convenció siguin castigades amb sancions efectives, proporcionades i dissuasives, incloses penes privatives de llibertat per a les persones físiques.

Abans d'això, els estats també es comprometen a facilitar les recerques necessàries en l'entorn cibernètic, a través de la implementació de les obligacions regulades des de l'article 14 al 22, que cobreixen la conservació immediata de dades informàtiques emmagatzemades, la consecutiva congelació i divulgació de dades de tràfic, l'ordre de comunicació, l'escorcoll i decomís de dades informàtiques emmagatzemades, la recollida d'aquestes en temps real i la intercepció de continguts. L'article 19 permet a les autoritats competents bloquejar o treure del sistema informàtic els continguts il·legals.[31]

La implementació de les obligacions incloses en la Convenció sobre Cibercrim demana una extensa criminalització dels atacs ciberterroristes comesos contra ordinadors o altres interessos legals que depenen del funcionament correcte dels sistemes informàtics.[32] Els danys causats en béns o persones no és un prerequisit per a castigar partint de la Convenció sobre Cibercrim, però se segueix de l'aplicació de normes penals complementàries dels sistemes interns. Així, la Convenció sobre Cibercrim aconsegueix la criminalització d'atacs a sistemes informàtics per mitjà de l'accés a dades, que no requereix tenir en compte ni el dany físic ni la intencionalitat (política) de l'autor.

Durant el procés de negociació de la Convenció sobre Cibercrim va ser molt difícil arribar a un acord sobre la criminalització d'actes de naturalesa racista o xenòfoba, per la qual cosa aquests actes van ser inclosos en un Protocol addicional. Els estats que han consentit a obligar-se també per aquest protocol adaptaran la seva legislació interna per fer punible la disseminació de material racista o xenòfob, d'amenaces contra persones o grups de persones que vinguin motivades per raó de la seva raça, color, ascendència, origen nacional o ètnic o religió, i la publicitat insultant contra aquestes persones o grups pels mateixos motius, quan aquests comportaments es realitzin a través de sistemes informàtics.

Si aquestes previsions les posem en conjunció amb el terrorisme, el Protocol resulta rellevant respecte a les amenaces i insults llançats amb la intencionalitat d'incitar a la violència entre grups amb diferents orígens racials, nacionals o religiosos. Per tant, les disposicions del Protocol cobririen la utilització de les noves tecnologies de la informació i la comunicació per a aquestes finalitats terroristes.

Quant a la cooperació internacional, la Convenció preveu l'extradició per als casos de delictes comesos a través de la utilització de les tecnologies de la informació i la comu-

31. La prevenció en aquest camp és bastant complexa. En primer lloc, perquè Internet i el ciberespai global que significa és extremadament difícil de controlar. En segon lloc, perquè encoratjar les autoritats nacionals a dissenyar mecanismes de control, molt probablement ineficaços i cridats a fracassar, posa seriosament en perill el lliure flux d'informació i el dret a la privacitat. De nou aquí es manifesta la dificultat que suposa trobar un equilibri entre l'interès de la seguretat i la protecció dels drets humans. Vegeu HOL, A. (2005). *Security and civil liberties: the case of terrorism*, Anvers: Intersentia.

32. Vegeu LIPSON, H. (2002). «Tracking and tracing cyber-attacks: technical challenges and global policy issues», *CERT Coordination Center Special Report*, novembre, pàg. 37-51.

nicació, però exigeix doble incriminació: que el fet sigui punible en l'estat requeridor i en el requerit.

Ara bé, el principal escull deriva de la inexistència d'una definició generalment acceptada del que s'entén per *delicte polític*. Per aquest motiu, els estats que reben peticions d'extradició són els que interpreten individualment si una determinada ofensa s'ha de considerar o no com a tal. Les autoritats concernides es veuen compel·lides, respecte a les peticions d'extradició relacionades amb actes terroristes, a tenir en compte la particular gravetat de les violacions comeses. No obstant això, res no impedeix que es pugui denegar l'extradició perquè es consideri un determinat acte de terrorisme com a delicte polític, excepte per als països que han ratificat, sense reserves, la Convenció del Consell d'Europa sobre Supressió del Terrorisme de 1977, ja que obliga els estats part a no qualificar de delictes polítics, les ofenses greus que suposin actes de violència contra la vida, la integritat física o la llibertat de les persones.[33]

Independentment del que hem vist fins al moment, l'informe d'experts sobre ciberterrorisme del Consell d'Europa adverteix que les noves tecnologies van obrint dia a dia nous camps a la recerca criminal i a la transferència d'informació entre els cossos de seguretat de diferents països.[34]

En consonància, els seus autors suggereixen un protocol addicional per afegir les noves tècniques de recerca o la possibilitat d'excloure l'excepció de clàusula política per a alguns dels delictes previstos en la Convenció –especialment en casos greus de transferències de dades personals d'un sistema a l'altre.

En contrast, l'informe assenyala que un instrument addicional que tracti sobre els atacs d'especial gravetat a les tecnologies de la informació i la comunicació o a infraestructures generals no és essencial. N'hi hauria prou que les legislacions internes dels estats sobre protecció de dades i sistemes informàtics incloguessin sancions apropiades per als casos d'atemptats terroristes contra aquest tipus de tecnologies. Aquestes sancions efectives, proporcionades i dissuasives les requereix la Convenció sobre Cibercrim, després només cal esperar a assolir el resultat de la condemna dels ciberterroristes per mitjà de sentències dels tribunals interns, en aplicació les lleis internes que facin punibles els delictes greus contra la protecció de dades o els atacs a infraestructures informàtiques.

La posada al dia de la Convenció sobre Cibercrim ha estat debatuda llargament,[35] atès l'imparable avenç de la informàtica que fa que un text elaborat i consensuat a finals de la dècada passada avui resulti obsolet en diversos aspectes. La cooperació internacional i l'harmonització de legislacions podrien sortir reforçades d'aquesta revisió, al mateix temps que s'aprofiti per a absorbir noves eines i així fer front als actuals riscos.[36]

Lamentablement, la Convenció sobre Cibercrim no té el nombre de ratificacions que seria desitjable.[37] Podríem dir que els estats signataris i tots aquells altres que hi vulguin accedir –ja que està oberta a països no membres del Consell d'Europa–, s'ho estan prenent amb certa calma, la qual cosa va en detriment de la prevenció d'aquest tipus de delictes que requereixen una harmonització de les normes nacionals substantives, processals i de cooperació.

33. La Convenció de 1977, junt amb el seu Protocol d'esmena de 2003, inclouen tots els delictes que cobreixen els convenis sectorials de les Nacions Unides relatius a activitats terroristes. La Convenció assumeix el principi *aut dedere aut judicare*, que significa que si no s'extradeix, aquests estats haurien de sotmetre els casos a la seva jurisdicció interna a fi que siguin perseguits per les autoritats judicials pròpies (article 4).
34. *Op. cit.*, nota 27, pàg. 81-93.
35. Vegeu, per exemple, BREYER, P. (2001). «Cyber-crime-Konvention des europarats», *Datenschutz und Datensicherheit*, núm. 25, pàg. 592-600 ; DIX, A. (2001). «Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV», *Datenschutz und Datensicherheit*, núm. 25, pàg. 588-591.
36. Vegeu GIACOMELLO, G. (2004). «Bangs for the buck: a cost-benefit análisis of cyberterrorism», *Studies in Conflict & Terrorism*, vol. 27, pàg. 387-408.
37. De moment només 26 països entre membres i no membres del Consell d'Europa han ratificat la Convenció sobre el Cibercrim. Com ja hem assenyalat, Espanya no és un d'ells.

3.2. Convenció Europea sobre la Prevenció del Terrorisme

La Convenció Europea sobre la Prevenció del Terrorisme va ser elaborada el 2005 en el si del Consell d'Europa, encara que està oberta a la participació de tots els països que ho desitgin.[38] La Convenció propicia una harmonització del dret penal i amb això facilita la cooperació internacional en matèria de prevenció i lluita contra el terrorisme.

Segons el preàmbul de la Convenció, els actes de terrorisme tenen com a propòsit, per la seva naturalesa i context, intimidar una població o compel·lir un govern o una organització internacional a realitzar o a abstenir-se de realitzar una activitat o a desestabilitzar seriosament o destruir l'estructura política, constitucional, econòmica o social d'un país o una organització internacional. I es considerarà acte terrorista qualsevol de les infraccions que es preveuen en els textos internacionals enumerats en l'annex I de la Convenció.

A diferència dels convenis i tractats internacionals existents que es dirigeixen a sancionar el terrorisme una vegada que s'ha produït el delicte, aquest text subratlla de manera especial la prevenció del terrorisme, impulsant la intervenció de les autoritats abans que els actes terroristes hagin estat comesos.[39]

Per complir amb aquesta obligació, les autoritats nacionals han de millorar i promoure la cooperació en aquesta matèria, intercanviant informació, donant protecció física a les persones i a les instal·lacions i coordinant els plans d'emergència, entre altres accions. Igualment les parts transigeixen, arribat el cas i en la mesura de les seves possibilitats, a prestar-se mútuament assistència i suport internacional per a elevar la seva capacitat per a prevenir la comissió d'actes terroristes.

En aquesta convenció els estats es comprometen a introduir al seu dret intern com a delictes la comissió de qualsevol acte o activitat terrorista recollida en els tractats enumerats en l'annex (que són els esmentats en la Resolució 1373 (2001) del Consell de Seguretat de l'ONU), la provocació pública per a cometre aquests actes, el reclutament de persones i el seu entrenament amb aquesta mateixa finalitat, independentment que després s'arribi a consumar l'acte o activitat terrorista prevista.

Aquesta és una de les principals novetats de la Convenció ja que, per exemple, fins a aquell moment pocs països europeus consideraven en les seves legislacions l'apologia o provocació pública del terrorisme.[40] A més, l'article 5 va ser objecte de profundes reflexions per part d'un grup de treball dins del CODEXTER (CODEXTER-Apologia), ja que un problema a què s'enfronta l'aplicació d'aquesta disposició és diferenciar entre apologia i llibertat d'expressió, com a dret fonamental reconegut i emparat pel Conveni europeu dels drets humans de 1950. Sembla clar que sense la intenció expressa d'incitar a la comissió d'actes terroristes i el risc que aquests es cometin, no es podrà parlar de provocació pública. En ambdós casos, es tracta d'elements molt difícils d'objectivar.[41]

L'article 6 de la Convenció regula el reclutament per al terrorisme, i qualifica aquest comportament com el fet d'enrolar una altra persona per a cometre o participar en la comissió d'un acte terrorista, o per a unir-se a una associació o a un grup a fi de contribuir a la comissió d'una o diverses infraccions terroristes. Queda clar que la conducta que es persegueix és l'acte de reclutament en si mateix, independentment de si el nou afiliat arriba a participar efectivament en actes terroristes.

L'entrenament terrorista, regulat en l'article 7 de la Convenció, es refereix al fet de donar instruccions per a la fabricació

38. Fins i tot la data, l'han ratificat 19 països, entre ells Espanya, que va dipositar el seu instrument de ratificació el 27 de febrer de 2009. Per a Espanya la Convenció és obligatòria des del passat 1 de juny de 2009, si bé ja vigia des de l'1 de juny de 2007 quan va assolir la xifra de 6 ratificacions.
39. Veure NEUMANN, P. (2009). *Old and new terrorism*, Cambridge: Polity Press.
40. La Resolució 1624 (2005) del Consell de Seguretat de l'ONU, de 14 setembre 2005, cridava a tots els Estats adoptar totes les mesures necessàries i apropiades i acords amb les seves obligacions de Dret Internacional per a [...] prohibir per llei la incitació per cometre un acte terrorista. L'expressió «calls upon States» no denota obligació per als poders públics nacionals.
41. L'informe explicatiu no aclareix res sobre la intencionalitat. Tanmateix, respecte al risc diu que per a avaluar-lo, caldrà tenir en compte qui és l'autor i el destinatari del missatge, així com el context en el qual es produeix la incitació de conformitat amb la jurisprudència del TEDH. També s'han de considerar la significació i la credibilitat del risc, d'acord amb la legislació interna.

o utilització d'explosius, d'armes de foc o de d'altres substàncies nocives o perilloses per a cometre o contribuir a cometre actes terroristes, sempre que l'instructor sigui conscient que aquella formació té com a objectiu servir per a la perpetració d'aquests actes.

Noteu que tant la provocació pública, com el reclutament i, fins a cert punt, l'entrenament per al terrorisme són conductes que poden desenvolupar-se a través de mitjans informàtics[42].. És a dir, és important en aquest punt tenir en compte que els actes terroristes constitueixen un comportament que quan té lloc a través d'Internet caurà dins del marc d'aplicació tant de la Convenció sobre el Cibercrim de 2001, com de la present Convenció sobre la Prevenció del Terrorisme de 2005.

De la mateixa manera, les parts en la Convenció es comprometen a establir penes efectives, apropiades i dissuasives per als terroristes en relació amb tots els actes que es consideren terroristes segons aquest instrument, així com per a la temptativa i la complicitat. La temptativa té molt que veure amb el reclutament i l'entrenament, ja que és d'aquestes conductes d'on pot deduir-se'n. La complicitat, per la seva banda, es relaciona més amb l'organització i contribució a la comissió dels actes terroristes, conceptes que no han quedat concretats ni en la Convenció ni en el seu informe explicatiu. Totes aquestes actuacions poden dur-se a terme a través de la Xarxa i amb l'ajuda de les noves tecnologies.

D'altra banda, el Consell d'Europa es preocupa per harmonitzar les iniciatives per a posar fi al terrorisme internacional amb la garantia que el caracteritza de protecció dels drets humans.[43] Les parts es veuen compel·lides a adoptar les mesures necessàries per a prevenir les accions terroristes i els seus efectes negatius, sempre des del respecte de l'estat de dret, els valors democràtics, la protecció dels drets humans[44] i les altres normes de dret internacional, incloent-hi les del dret internacional humanitari.

Tanmateix, cal tenir en compte que els efectes de les pròpies accions terroristes atempten clarament contra els drets humans garantits en diferents instruments internacionals, especialment contra el dret a la vida,[45] però també contra altres de relacionats amb l'ús de les noves tecnologies com el respecte a la vida privada.[46] Per això, hem de destacar que es tracta del primer conveni que estableix una obligació en dret internacional de protegir les víctimes del terrorisme.[47]

Entre els estats part hi ha l'obligació d'ajuda mútua en relació amb les recerques i procediments penals i d'extradició oberts.[48] La finalitat última d'aquesta disposició és la d'intercanviar informació per tots els mecanismes que els estats puguin establir en el seu dret intern com a forma de cooperació internacional, això sí, sempre amb ple respecte a les obligacions relatives als drets humans.[49]

42. Pensem en els manuals per a fabricar bombes, verins i altres armes a fi de cometre atemptats que moltes organitzacions terroristes estan penjant a la Xarxa.
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. Vegeu també les directrius referides sobre drets humans i lluita contra el terrorisme d'11 de juliol de 2002 i la Recomanació (2005) 10 del Comitè de Ministres, relativa a les tècniques especials de recerca en relació amb infraccions greus, inclusivament els actes de terrorisme, de 10 d'abril de 2005.
45. Precisament en el marc del Consell d'Europa, l'article 2 del Conveni europeu de drets humans de 1950 diu: «1. El dret de tota persona a la vida està protegit per la Llei. Ningú no pot ser privat de la seva vida intencionadament, excepte en execució d'una condemna que imposi pena capital dictada per un tribunal al reu d'un delicte per a qui la llei estableix aquesta pena».
46. L'article 8.1 del Conveni europeu de drets humans garanteix el següent: «Tota persona té dret al respecte de la seva vida privada i familiar, del seu domicili i de la seva correspondència.» Obvia assenyalar la interferència en la vida privada d'una persona que suposa qualsevol classe de manipulació de les seves dades a través d'Internet.
47. Aquesta disposició, segons va indicar el coordinador antiterrorista del Consell d'Europa, es va incloure a petició de la delegació espanyola durant la negociació del text, després de superar importants problemes. Algunes delegacions s'havien mostrat contràries que s'introduís aquesta disposició en el text de la Convenció, tenint en compte el seu caràcter eminentment preventiu. Finalment, es va decidir incloure-hi almenys una disposició de caràcter general atès el paper central que han de representar les víctimes en la lluita contra el terrorisme.
48. En el marc del Consell d'Europa, hi ha una obligació general d'acord amb el Conveni Europeu sobre Extradició de 1957 i els seus protocols addicionals de 1975 i 1978. Igualment, no podem obviar el Conveni Europeu sobre Assistència Mútua en Matèria Penal de 1959 i els seus protocols de 1978 i 2001.
49. FITZPATRICK, J. (2003). «Speaking law to power: the war against terrorism and human rights», *European Journal of International Law*, vol. 14, núm. 2, pàg. 241-264.

Segons l'article 18, l'Estat que no concedeixi l'extradició es compromet a sotmetre l'assumpte a les autoritats internes competents, sense dilació indeguda i sense cap tipus d'excepció, per a l'exercici de l'acció penal (principi *aut dedere aut judicare*). A més, en la línia del que es disposa en el Conveni de 1977 esmenat pel Protocol de 2003, l'article 20 inclou l'«exclusió de la clàusula d'excepció política» per a les infraccions regulades en els articles 5 a 7 i 9 de la Convenció, per a les quals no pot ser denegada l'extradició, encara que el paràgraf 2 permet la formulació de reserves a aquest article 20.1.

Tant l'ONU com l'Organització per a la Seguretat i la Cooperació a Europa (OSCE) han saludat l'adopció d'aquesta convenció i n'han recomanat la ratificació. Al seu torn, la Unió Europea ha decidit incloure en la seva decisió marc sobre lluita contra el terrorisme els tres nous delictes tipificats en la Convenció.[50] Es tracta d'un efecte molt positiu de la Convenció que ha creat una nova dinàmica i un consens a escala almenys regional europeu, si no internacional, sobre la necessitat d'unir esforços en la prevenció i no solament en la lluita contra el terrorisme.

Sembla molt precipitat llançar una crida a la revisió d'aquest recent instrument. Si bé és veritat que algunes de les amenaces actuals a les mans dels terroristes no estan adequadament cobertes en el seu catàleg d'actes terroristes, una lògica i precisa interpretació de les seves disposicions posades en conjunció amb la resta de textos del Consell d'Europa i d'altres organitzacions internacionals, sens dubte permetrà cobrir els diversos supòsits que es donin en la pràctica ciberterrorista.

Conclusió

El ciberterrorisme contra Internet o per via d'Internet representa un risc significatiu des que els sistemes informàtics avui en dia són responsables de dur a terme moltes funcions essencials de la nostra societat. Els cibercriminals poden atacar tot allò que és important per a la societat moderna i estigui connectat a Internet o accessible via altres línies de comunicació. Després els terroristes tenen a les seves mans la possibilitat d'usar les mateixes tècniques i adquirir els mateixos coneixements i eines que la resta dels criminals, a fi d'aconseguir crear un clima de terror que faciliti la consecució de les seves aspiracions.

Aquest tipus d'atacs utilitzant Internet podrien causar danys en sistemes informàtics, així com en la integritat física de les persones i els seus béns. A més, els terroristes empren habitualment la Xarxa i les noves tecnologies per a disseminar contingut il·legal i per a la preparació logística dels actes terroristes.

Les convencions i instruments específics sobre cibercriminalitat, que acosten a l'harmonització de les normes substantives i procedimentals nacionals i a la cooperació internacional en aquest àmbit, són aplicables a la persecució del ciberterrorisme i altres usos d'Internet amb finalitats terroristes. Igualment, les normes substantives, procedimentals i de cooperació incloses en altres instruments sobre terrorisme, sobre blanqueig de diner, sobre finançament d'activitats terroristes, sobre mútua assistència o extradició, són també aplicables al ciberterrorisme des que són formulades de manera general i així poden ser utilitzades en l'entorn de les noves tecnologies.

Amb això, volem deixar establert que no hi ha llacunes transcendentals respecte al ciberterrorisme en les convencions exclusives sobre ciberdelinqüència, com tampoc no n'hi ha respecte a la utilització de la informàtica per a cometre els il·lícits perseguits en les convencions específiques sobre terrorisme. De la combinació d'ambdues classes d'instruments internacionals, podem obtenir una regulació gairebé completa del fenomen ciberterrorista.

Com bé assenyala l'informe dels experts, el problema més important se centra en la falta de ratificacions dels instruments ja existents. Una participació com més àmplia millor tant en la Convenció sobre Cibercrim, com en la Convenció sobre la Supressió del Terrorisme, resulta essencial per a combatre el ciberterrorisme i altres usos d'Internet amb propòsits terroristes. I aquest és el camp en el qual cal treballar, més que estar pensant en les seves virtuals reformes. Evidentment, tots els instruments analitzats tenen coses millorables i a molts d'ells tampoc no els vindria malament una posada al dia.

50. Decisió marc 2008/919/JAI del Consell, de 28 de novembre de 2008, per la qual es modifica la Decisió marc 2002/475/JAI sobre la lluita contra el terrorisme, DG. L 330 de 9.12.2008, pàg. 21.

Quan ens endinsem en el camp de les noves tecnologies, és difícil decidir si tot el que hem tractat aquí és fruit d'una exagerada «ciberpor» o el ciberterrorisme és una amenaça veraç i imminent. Hi ha opinions per a tots els gustos: alguns pensen que un atac d'aquestes característiques no ha tingut lloc mai i l'amenaça no existeix perquè les conseqüències serien de relleu molt escàs,[51] mentre que d'altres es mostren molt més cauts i asseguren que el risc és autèntic.[52]

Sens dubte, les conductes conegudes com a «ciberterrorisme» tenen molt més a veure amb l'apologia, el reclutament i, en menor mesura, l'entrenament terrorista, així com amb l'adquisició d'informació, la comunicació interna i l'anàlisi d'objectius utilitzant la Xarxa de xarxes, que amb un atac de «*hacker*-terroristes» que posi en perill el sistema electrònic de comunicacions mundial que significa Internet i les diverses infraestructures que en depenen.[53]

Tanmateix, no hem de subestimar el potencial de l'amenaça ciberterrorista. Tenim davant de nosaltres una nova generació de joves terroristes que ha crescut en l'era digital, familiaritzats amb els ordinadors. Les capacitats i eines necessàries per a un atemptat cibernètic estan a la seva disposició de manera gratuïta i són fàcils de manejar. Tampoc no falten patrocinadors entre ciutadans «altruistes», empreses, organitzacions i, fins i tot, governs, que garantiran el finançament. L'anonimat, la dificultat en la persecució i la innecessària presència física al lloc de l'atemptat continuen essent avantatges que han considerar de manera molt positiva els terroristes. La possibilitat d'atacs a gran escala i amb conseqüències que es poden fàcilment anar allargant en el temps converteix els assalts digitals en altament atractius.[54] La creativitat humana aplicada al costat fosc del mal és il·limitada, la qual cosa es va demostrar amb els tortuosos mètodes terroristes utilitzats l'11-S i l'11-M, impensables per a la majoria de nosaltres.

Bibliografia

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

BENDRATH, R. (2003). «The American cyber-angst and the real world: Any link?». A: R. LATHAM (ed). *Bombs and bandwidth: the emerging relationship between information technology and security*. Nova York: The New Press. Pàg. 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». A: *11th Annual International Symposium on Criminal Justice Issues* (Chicago: University of Illinois at Chicago) [ponència en línia]. [Data de consulta: 30 d'abril de 2009].

‹http://afgen.com/terrorism1.html›

51. Vegeu GREEN, J. (2002). «The myth of cyberterrorim», *Washington Monthly*, vol. 34, núm. 11, pàg. 8-13; SANDWELL, B. (2006). «Monsters in cyberespace, cyberphobia and cultural panic in the information age», *Information, Communication & Society*, vol. 9, núm. 1, pàg. 39-61.
52. WEIMANN, G. (2005). «Cyberterrorism: the sum of all fears?», *Studies in Conflict & Terrorism*, vol. 28, pàg. 129-149.
53. La majoria dels experts coincideix a assenyalar aquest fet, posant en dubte la possibilitat pràctica d'un atac de ciberterrorisme amb resultats catastròfics, la qual cosa s'ha anomenat electronic *Pearl Harbor*. Denning deia en un article publicat unes quantes setmanes abans de l'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*, estiu, pàg. 6. Vegeu també CONWAY, *op. cit.*, pàg. 5. Tanmateix, Verton imagina i descriu com seria un atac ciberterrorista, alhora que alerta sobre el seu perill en els nostres dies; VERTON, D. (2003). *Black ice: the invisible threat of cyberterrorism*, Nova York: McGraw-Hill, pàg. 13-15.
54. Vegeu GERCKE, M. (2007). «Cyberterrorismus -Aktivitäten terroristischer organisationen im Internet», *Computer und Recht*, vol. 23, núm. 1, pàg. 62-68.

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*. Núm. 2008-5. Centre for International Studies, Dublin City University, Irlanda.

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

DAUKANTAS, P. (2001). «Professors hash out emergency response, cyberterrorism strategies». *Government Computer News* [article en línia]. [Data de consulta: 30 d'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]. A: John ARQUILLA, David RONFELDT (ed.) (2003). *Networks and Netwars. The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand Corporation. [Data de consulta: 30 d'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, núm. 6, pàg. 1033-1043.

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

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

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

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, núm. 4, pàg. 179-187.

SCHWARTAU, W. (ed.) (1994). *Information warfare. Cyberterrorism: protecting your personal security in the electronic age*. Nova 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 pàg.

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

Citació recomanada

CHICHARRO, Alicia (2009). «La tasca legislativa del Consell d'Europa davant la utilització d'Internet amb finalitats terroristes» [article en línia]. *IDP. Revista d'Internet, Dret i Política*. Núm. 9. UOC. [Data de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_chicharro/n9_chicharro_cat›

ISSN 1699-8154

Sobre l'autora

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

Doctora en Dret per la Universitat Pública de Navarra. De 1995 a 1999, beca FPI (MEC). De 2001 a 2003, va ser col·laboradora externa de l'editorial Aranzadi com a analista de sentències del TJCE, i entre l'any 2002 i el 2009, professora ajudant a l'UPNA. Actualment, és professora associada al Departament de Dret Públic d'aquesta Universitat i jutge substituta als jutjats de Navarra. Ha participat en estades de recerca en centres estrangers, com la Universitat d'Oxford, el Max-Planck-Institut o la Comissió Europea. Autora d'algunes publicacions, com «La lucha contra el terrorismo internacional: regulación internacional y europea» (2007), a *Temas Actuales de Derecho*, Pamplona: UPNA, i *El principio de subsidiariedad en la Unión Europea* (2001), Pamplona: Aranzadi.

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