Volume 110
Issue 3 *Dickinson Law Review - Volume 110, 2005-2006*

1-1-2006

Cyber-Terrorism: Legal Principle and Law in the United Kingdom

Clive Walker

Cyber-Terrorism: Legal Principle and Law in the United Kingdom

Clive Walker*

I. The Ethics of Responding to Terrorism

The capacity of terrorists to terrorise must be taken seriously. Governments and citizens of the United Kingdom may have become inured to the phenomenon of terrorism by thirty years of Irish political violence. Nevertheless, the impact of September 11th has been striking, not only in the United Kingdom but throughout the world, especially within the United States. The disbelief and incomprehension as to what lies behind the attacks, the wayward calculations of danger, and the reactive destruction of revered norms and processes are all evidence of a traumatised polity.[1] As a result of this evident capacity of terrorism to destabilise and damage otherwise just and democratic societies, those societies have a right to engage in forward planning and counter-measures. In the words of one American judge, a democracy is not a "suicide pact," and measures can be taken against clear and present dangers.[2] This point is also reflected in Article 17 of the European Convention on Human Rights and Fundamental Freedoms of 1950, which states:

> Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided

* Professor of Criminal Justice Studies, Centre for Criminal Justice Studies, School of Law, University of Leeds. The author thanks the organizers and participants at the ESRC Seminar on Cybercrime (Leeds, April 2002) and the Free Speech Forum (Leeds, May 2005).

1. *See generally* LAWYERS COMMITTEE FOR HUMAN RIGHTS, ASSESSING THE NEW NORMAL (2003) (documenting the expansion of executive authority and the abandonment of democratic procedural safeguards).

2. Terminiello v. Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting).

for in the Convention.[3]

So, while terrorism is certainly to be counteracted, we must consider whether there is a need to react to cyber-terrorism and if so, to what extent?

The first step in the argument should be to impose firm principle on any legal initiative. As has been explained elsewhere, full constitutional governance requires continual application of a number of elements.[4] The first is a "rights audit" which means that the rights of individuals are respected according to traditions of the domestic jurisdictions and the demands of international law.[5] The latter will include the periodic review of the very existence of any emergency or special measures.[6] The second element is "democratic accountability" which includes attributes such as information, open and independent debate, and an ability to participate in decision making.[7] The third element is "constitutionalism"—the subjection of government to norms, whether legal or extra legal (such as codes).[8] More specific requirements in the field of special powers include the public articulation of reasons in support of particular actions taken for the public welfare, assurances through effective mechanisms that the crisis cannot be ended by normal means and that powers will not be used arbitrarily and are proportionate to the threat, and adherence to the overall purpose of the restoration of fundamental features of constitutional life.[9] Constitutionalism also requires that, at a more individual level, excesses can be challenged, including through the courts.

Bearing these standards in mind, especially the latter, the nature of the threat of terrorism and cyber-terrorism should next be considered. As for terrorism, it must be borne in mind that resort to violence is almost certainly a breach of law without having any need for special measures to bring about that depiction. Consequently, in light of the need for proportionality under the heading of constitutionalism, let us consider why special laws might be needed. The answer lies not in the motivation

3. European Convention on Human Rights and Fundamental Freedoms, Nov. 4, 1950, ETS 5, 213 U.N.T.S. 17. *See also* COUNCIL OF EUROPE, GUIDELINES ON HUMAN RIGHTS AND THE FIGHT AGAINST TERRORISM (3d ed., Strasbourg 2005).

4. Clive Walker, *Constitutional Governance and Special Powers against Terrorism*, 35 COLUM. J. TRANSNAT'L L. 1, 7-10 (1997). *See also* C. WALKER & J. BRODERICK, THE CIVIL CONTINGENCIES ACT 2004: RISK, RESILIENCE AND THE LAW IN THE UNITED KINGDOM chs. 6-7 (Oxford University Press, Oxford, 2006) [hereinafter WALKER, CIVIL CONTINGENCIES].

5. *Id.* at 7.

6. *Id.* at 8.

7. *Id.* at 9.

8. *Id.*

9. *Id.* at 9-10.

per se. Whilst motivation may be a necessary defining factor in the ascription of the label "terrorism,"[10] it is not a sufficient defining factor in the invocation of a special legal response. A special response may typically be justifiable when terrorism is emanating from a group with capacities to organise collectively on a sustained basis, to engage in sophisticated plans and operations, and to operate independently from normal life or to have the capacity to intimidate normal society into tolerating its presence. If those factors are present, one might concede the need to depart from normal laws of criminal detection and process which often assume (and rely upon) the opposites: lone individuals, inadequate, bungling operations, and individuals who cannot help but leave traces of their wrongdoing and who are powerless to stop being picked up by the forces of law and order. Groups such as the Irish Republican Army (IRA) certainly fall into the former rather than the latter criteria. By contrast, the Unabomber[11] or someone like David Copeland,[12] whose case is discussed below, could be said to engage in terrorism, but lack the capacity to create a threat of a kind which requires special laws. Even organisations which seek political change and use violence to achieve it, but do not have the sophistication, size or threat of the likes of Irish paramilitary groups, should be tackled through normal laws rather than special laws. In practice, this demarcation is recognised by the United Kingdom authorities who have as a matter of policy declined to treat amateurish animal rights extremists as "terrorists" even though they apparently fit the definitional profile[13] and have been described as replicating "a quasi-terrorist cellular structure."[14] It follows that any definitional precision surrounding the term "terrorism" may be more apparent than real and, even if achieved, there would still be a role for further modes of governance over police action in response to terrorism.

These observations in turn lead us to examine the legal definition of "terrorism." An immediate criticism is that concentration upon the legal definition of terrorism is a positivist, facile solution to the problem. There may be three responses. First, the focus of this paper is legal

10. Andrew Silke, *Here Be Dragons*, CYBERCRIME: IMMATERIAL CRIME AND POLICING IMMATERIALITY COLLOQUIUM 3 (Economic and Social Research Council 2002).

11. Theodore Kaczynski was sentenced to life imprisonment in 1998 for bombings over a number of years which killed three people and maimed two others. Giles Whittell, *Unabomber to End His Days in Prison*, THE TIMES (London), May 5, 1998; *see also* THE SACRAMENTO BEE, *Unabomber*, http://www.unabombertrial.com (last visited Nov. 30, 2005).

12. *See infra* notes 96-99 and accompanying text.

13. *See, e.g.*, HOME OFFICE, ANIMAL RIGHTS EXTREMISM 3.75 (2001).

14. UNITED KINGDOM DEPARTMENT OF TRADE AND INDUSTRY, ANIMAL WELFARE—HUMAN RIGHTS: PROTECTING PEOPLE FROM ANIMAL RIGHTS ACTIVISTS, para. 43 (2004).

principle and legal action, so it is already operating within parameters set by the legal system. Those who wish to go outside those parameters must read other papers. Second, the positing of a definition by the legal system is an authoritative process—law is invested with its own majesty which brooks no argument (save amongst lawyers and judges). In other words, like it or not, the legal definition will be played out in court, and real people will suffer real consequences as a result. The same does not necessarily apply to the definitions devised by political scientists or sociologists. Third, those readers who do care to venture into the realms of political or social science will find no end of disagreement and confusion. One author has noted, "Above the gates of hell is the warning that all that enter should abandon hope. Less dire but to the same effect is the warning given to those who try to define terrorism."[15] Having said this, wide currency is given to the concept of terrorism devised by Schmid and Jongman, which states: "Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-)clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby—in contrast to assassination—the direct targets of violence are not the main targets."[16] In addition, the definitions used by the U.S. Department of State in its annual *Patterns of Global Terrorism* are often repeated. According to these definitions,

> The term "terrorism" means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.
>
> The term "international terrorism" means terrorism involving citizens or the territory of more than one country.
>
> The term "terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism.[17]

---

15. DAVID TUCKER, SKIRMISHES AT THE EDGE OF EMPIRE 51 (Praeger, Westport, 1997).

16. ALEX P. SCHMID & ALBERT J. JONGMAN, POLITICAL TERRORISM: A NEW GUIDE TO ACTORS, AUTHORS, CONCEPTS, DATA BASES, THEORIES, AND LITERATURE 28 (North-Holland, Amsterdam, 1988). This formulation was based upon the authors' study of 109 definitions from which they derived 22 word categories. *See id.* at 5-6.

17. U.S. Department of State, Patterns of Global Terorrism, http://www.state.gov/s/ct/rls/pgtrpt/ (last visited Jan. 25, 2006). This series of annual reports to Congress is required by 22 U.S.C. § 2656f(a), and the definition above is used in the reports since it is contained in section 2656f(d). 22 U.S.C. § 2656f(d)(1)-(3) (2005). "Noncombatant" is taken to include off-duty military personnel and attacks on military not in a state of hostilities is likewise included. Under the USA PATRIOT Act of 2001, "domestic terrorism" means activities that:

As for the legal response, the definition adopted in the United Kingdom, in section 1 of the Terrorism Act 2000, states as follows:

(1) In this Act "terrorism" means the use or threat of action where—

(a) the action falls within subsection (2),

(b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and

(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.

(2) Action falls within this subsection if it—

(a) involves serious violence against a person,

(b) involves serious damage to property,

(c) endangers a person's life, other than that of the person committing the action,

(d) creates a serious risk to the health or safety of the public or a section of the public, or

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied.

(4) In this section—

(a) "action" includes action outside the United Kingdom,

(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
(B) appear to be intended—
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or
(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) occur primarily within the territorial jurisdiction of the United States.
18 U.S.C. § 2331 (2005). For the entire PATRIOT Act, *see* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

> (b) a reference to any person or to property is a reference to any person, or to property, wherever situated,
>
> (c) a reference to the public includes a reference to the public of a country other than the United Kingdom, and
>
> (d) "the government" means the government of the United Kingdom, of a Part of the United Kingdom or of a country other than the United Kingdom.
>
> (5) In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation.[18]

The essence of the definition is in section 1(1), which contains three conjunctive legs, all of which must normally be satisfied (subject to section 1(3)). It will be noted from section 1(1)(b) that terrorism may be suffered either by the government, including it agents such as the police, or the public. A suggestion that attacks on the former might amount to political violence but not "terrorism"[19] is at variance with a growing body of international law,[20] with developments in extradition law,[21] and with the rationale for having anti-terrorism laws, which is to deal with forms of organised crime which cannot effectively be handled under "normal" laws.

Lord Lloyd, in his review of United Kingdom counter-terrorism laws in 1996, viewed the definition then set out in section 20 of the Prevention of Terrorism (Temporary Provisions) Act 1989 as too narrow, especially as it did not catch single issue or religious terrorism.[22] Hence, section 1 of the Terrorism Act is intended to expand both the forbidden activities and feared consequences. The Home Office view is that to limit the application of the definition of terrorism to actions contrary to the criminal law will not suffice.[23] It would cause uncertainties in dealing with international terrorism; the police might be unable to act

18. Terrorism Act, 2000, c. 11, § 1 (U.K.). *See* CLIVE WALKER, BLACKSTONE'S GUIDE TO THE ANTI-TERRORISM LEGISLATION 20-21 (Oxford University Press, Oxford, 2002) [hereinafter WALKER, BLACKSTONE'S].

19. NOEL WHITTY ET AL., CIVIL LIBERTIES LAW: THE HUMAN RIGHTS ACT ERA 121 (Butterworths, London, 2001).

20. *See, e.g.*, European Convention for the Suppression of Terrorism, Jan. 27, 1977, 90 E.T.S. 2.

21. *See* GEOFF GILBERT, ASPECTS OF EXTRADITION LAW 113-65 (Nijhoff, Dordrecht, 1991) (discussing application of the political offense exemption).

22. LLOYD OF BERWICK, INQUIRY INTO LEGISLATION AGAINST TERRORISM 5.22 (Cm. 3420, Stationery Office, 1996).

23. *See* 611 PARL. DEB., H.L. (5th ser.) (Apr. 7, 2000) 1484.

unless and until they were sure that the action in question was contrary to the criminal law in the relevant country overseas. In addition, there may be occurrences designed to terrify which are not unlawful, such as a refusal to perform a duty to keep others safe. Lord Bassam, the Ministerial spokesman in the Home Office, offered the following illustration:

> For instance, an employee may advance a political cause and may deliberately omit to update a vital computer programme or omit to put a cleansing agent in a sewerage system, with the result that the health of a section of the public was severely put at risk. In our view that could be terrorism in certain circumstances.[24]

The differences between the formulations in the 1989 and 2000 Acts were the focus of much of the debate concerning the Terrorism Act. The general allegation is that section 1 is significantly broader than its predecessor and will affect legitimate political activity as well as terrorism. In part, it is intentionally broad, as it is mainly the platform for investigative police powers where there must be some margin of error; it is not a term on which any criminal offence is based.[25] Overall, it is submitted that the changes in the terms of the definition are not tremendously significant. Rather, it is the circumstance of how it is then applied later in the Terrorism Act—the remit—which is worrisome. The remit is no longer confined in the main to long-established terrorist groups in Ireland but can potentially affect any domestic or international involvement in terrorism, whether severe and collective political violence or not.

Yet, in some respects section 1 is expressly broader than its predecessor. The Home Office was concerned that the prior focus upon the word "violence" might limit the legislation to a threat to, or endangerment of, personal safety. The result would be to leave out acts which might not be violent in themselves but which can have a devastating impact. These could include disrupting key computer systems or interfering with the supply of water or power where life, health or safety may be put at risk on a broad scale.[26] The bombs in the City of London in 1992 and 1993 and in London Docklands in 1996 may be further illustrations. In a late modern society, the state is "hollowed out," and power is diffused across both public and private sectors.[27]

---

24. 614 PARL. DEB., H.L. (5th ser.) (July 4, 2000) 1448-49.

25. *See* 346 PARL. DEB., H.C. (6th ser.) (Mar. 15, 2000) 410.

26. SECRETARY OF STATE FOR THE HOME DEPARTMENT & SECRETARY OF STATE FOR NORTHERN IRELAND, LEGISLATION AGAINST TERRORISM 10 (Cm. 4178, Stationery Office, 1998).

27. For the concept of "hollowing out," *see* R.A.W. RHODES, UNDERSTANDING

Power relates more to finance, knowledge and security. Consequently, the likely targets of terrorists shift in line with the new centres of power and the new power-holders—such as financial institutions in the City of London. Thus, terrorism becomes less focused upon states and territories, while the terrorist groups themselves become more fluid and hybrid in objectives, forms and tactics.[28] In this light, section 1(2) seeks to protect against (b) risks to property, (d) risks to safety and (e) interference with computer systems.

Yet, it is not certain that the term "violence" as a concept does not include attacks on property, and it is so defined in the United Kingdom's Public Order Act 1986, section 8.[29] The use of the word "violence" in connection with property may usefully carry the implication that trivial forms of damage, such as graffiti, cannot amount to "terrorism."[30] The debates in Parliament on the meaning of "violence" in the context of property attacks were somewhat curtailed when, at the Report stage of the House of Lords, the government simply replaced the word "violence" with the word "damage" in subsection 2(b).[31] At the same time, there was the inclusion of section 1(2)(e), which is designed to take account of cyber-terrorism—"serious disruption to computer systems to advance a political, religious or ideological cause."[32] The emphasis on "serious" is important—"a costly nuisance" should not be dealt with as cyber-terrorism.[33]

Returning to the precepts of constitutional governance, how does this definition fit with the needs of society? It could be argued it is too broad because it is indeterminate as between what were referred to earlier as direct attacks and indirect attacks on the individual. The indirect form is not sufficiently linked to the Millian notion of "harm to others" to warrant intervention. It is true that the forms of intervention, such as arrest under section 41 of the Terrorism Act 2000 and the various forms of investigative powers in Parts IV and V of that Act, do not directly criminalise the activity designated as terrorism. But they do chill such behaviour and demonise it in the eyes of the public. As mentioned

---

GOVERNANCE: POLICY NETWORKS, GOVERNANCE, REFLEXIVITY AND ACCOUNTABILITY (Open University Press, Buckingham, 1997); A. STEWART, THEORIES OF POWER AND DOMINATION: THE POLITICS OF EMPOWERMENT IN LATE MODERNITY (Sage Publications, London, 2001); R.A.W. Rhodes, *The Hollowing Out of the State: The Changing Nature of the Public Services in Britain*, 65 POL. Q. 138 (1994).

28. *See* Xavier Raufer, *New World Disorder, New Terrorisms: New Threats for Europe and the Western World*, 11(4) TERRORISM & POL. VIOLENCE 35 (1999).

29. Public Order Act, 1986, c. 8 (U.K).

30. 613 PARL. DEB., H.L. (5th ser.) (May 16, 2000) 235.

31. *See* 614 PARL. DEB., H.L. (5th ser.) (June 20, 2000) 161.

32. *Id.* at 160.

33. Mohammad Iqbal, *Defining Cyberterrorism*, 22 J. MARSHALL J. COMPUTER & INFO. L. 397, 408 (2004).

at the outset, a state may also be worthy of protection—at least if it has sufficient attributes of legitimacy—but just as laws of subversion and sedition have become increasingly discredited,[34] so they should not be reintroduced by a back door extension of the term "terrorism."

As for definitions of "cyber-terrorism,"[35] the threat potentially emerges through the development of a late modern, information society. As one commentator observed, "Why assassinate a politician or indiscriminately kill people when attack on the electronic switching will produce far more dramatic and lasting results?"[36] But what is meant by the cyber-terrorist threat? We must at the outset distinguish various possible meanings before mapping them onto legal normative standards and actual legal responses. This task can and must be undertaken in the abstract for the purposes of legislative contingency planning, but whether action is taken at any point should also reflect the proportionate seriousness of the challenge.

An important distinction emerges from the literature between the use of the Internet in an ancillary role in furtherance of terrorism ("ancillary cyber-activities") and those uses which do themselves terrorise by using the Internet as the mode or the object of attack ("cyber-attack"). There is a strong line of literature which contends that only the latter fall within the definition of "cyber-terrorism." For example, perhaps the leading analyst of cyber-terrorism, Professor Dorothy Denning, has argued that:[37]

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean 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

34. *See* CLIVE WALKER, THE PREVENTION OF TERRORISM IN BRITISH LAW (2d ed., Manchester University Press, Manchester, 1992) [hereinafter WALKER, PREVENTION].

35. *See generally* DOROTHY DENNING, INFORMATION WARFARE AND SECURITY (ACM Press Books, New York, 1999) [hereinafter DENNING, INFORMATION]; Ralph Stephens, *Cyber-Biotech Terrorism: Going High Tech in the 21st Century*, *in* THE FUTURE OF TERRORISM: VIOLENCE IN THE NEW MILLENIUM (Harvey Kushner ed., Sage Publications, Thousand Oaks, 1998); THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM (Abraham Sofaer & Seymour Goodman eds., Hoover Institution Press, Stanford, 2001).

36. Walter Laqueur, *Postmodern Terrorism*, 75 FOREIGN AFFAIRS 24, 35 (1996).

37. Dorothy Denning, *Cyberterrorism* (2000), http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. *See also* Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, http://www.cs.georgetown.edu/~denning/infosec/nautilus.html (last visited Nov. 24, 2005) [hereinafter Denning, *Activism*].

> or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

This limited range is reflected by Professor Gabriel Weimann, who posits that "cyber-terrorism" means only "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)."[38] Likewise, it is said that "[c]ybercrime and cyberterrorism are not coterminous. . . . Terrorist use of computers as a facilitator of their activities, whether for propaganda, recruitment, datamining, communication, or other purposes, is simply not cyberterrorism."[39]

Based upon these formulations, only a fraction of what is discussed below will fall within the term "cyber-terrorism." One can readily concur that special laws against terrorism should be confined to attacks which result in serious harm to persons or property.[40] Yet, it is increasingly common for the law not only to deal with a core mischief but also with the organization and finance which produces and sustains that core mischief.[41] Consequently, it is necessary for the purposes of this paper to ignore the observations that the wider, more ancillary uses should be viewed as beyond the strict definition. It is not that the strict view is wrong, but rather that, to provide a short-hand for the full range of legal concerns and legal responses, a wider notion of cyber-terrorism will be adopted in this paper. In effect, it will include not only cyber-terrorism as a form of offence or attack, as above, but also the various ways in which the Internet is being used to sustain and further terrorism. This wider ambit is consistent with the uses of terrorism elsewhere—those who assist terrorism through finance or the supply of materials

38. Gabriel Weimann, *Cyberterrorism: The Sum of All Fears?*, 28 STUDIES IN CONFLICT & TERRORISM 129, 130 (2005) [hereinafter Weimann, *The Sum of All Fears*]. *See also* Gabriel Weimann, *Cyberterrorism: How Real is the Threat?*, U.S. INST.OF PEACE, http://www.usip.org/pubs/specialreports/sr119.html (Dec. 2004).

39. *See* Weimann, *The Sum of All Fears, supra* note 39, at 132-33.

40. *See* Iqbal, *supra* note 34, at 408.

41. For post 9/11 laws in the United States which relate to terrorist finances, *see especially* Exec. Order No. 13224, 66 Fed. Reg. 49079 (Sept 23, 2001); USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. Operation Green Quest was created in October 2001 as a multi-agency financial crimes task force to enforce these and other laws. *See* Nina J. Crimm, *High Alert: The Government's War on the Financing of Terrorism and its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 WM. & MARY L. REV. 1341 (2004); Walter Parkel, Note, *Money Laundering and Terrorism: Informal Value Transfer Systems*, 41 AM. CRIM. L. REV. 183 (2004); U.S. Customs Service Office of Investigations, *Green Quest, available at* http://www.ustreas.gov/rewards/pdfs/Green_Quest_Brochure.pdf (Oct. 2002).

become depicted as terrorists and are dealt with accordingly under special legislation.

II. A Typology of Cyber-Terrorism

Moving from definitions to typologies, the variants of cyber-terrorism include both the ancillary and offensive.[42]

A. Information Warfare[43]

In this aspect of activity, information technology is the means and object of attack. This mode of use is how cyber-terrorism is often conceived and is at the heart of Dorothy Denning's definition of "cyber-terrorism" mentioned earlier. An example of this scenario arose in July 1997, when Spanish protestors, who it must be emphasized might fall within the definition of "activist" or "hacktivist" but not "terrorist,"[44] attacked the Institute for Global Communications (IGC)[45] with thousands of bogus e-mail messages which swamped the Internet Service Provider's system and blocked other traffic. The objective was that IGC stop hosting the website for the *Euskal Herria Journal*, a New York-based publication supporting Basque independence, which included reports on the activities of Euskadi Ta Azkatasuna (ETA), the militant Basque group.[46] IGC staff members were reluctant to succumb to the pressure, but they said they had to remove the site because the attack had been crippling the entire service for the company's estimated 13,000 other subscribers.[47] Similar tactics were used in 1998 by Tamil activists who attacked Sri Lankan embassies with an overload of e-mails messages. More insidious was the attempt by Serb sympathizers during the war in Kosovo to target NATO with viruses in 1999.[48] Nevertheless,

---

42. *See* Timothy Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* PARAMETERS, U.S. ARMY WAR C. Q. 112 (Spring 2003); Silke, *supra* note 10, at 4.

43. *See* Frank Cilluffo et al., *Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge?*, 12 DEPAUL BUS. L.J. 131 (1999-2000); Susan Brenner & Marc Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1; Silke, *supra* note 10, at 4.

44. *See* Denning, *Activism, supra* note 37.

45. *See* The Institute for Global Communications, http://www.igc.apc.org (last visited Jan. 13, 2006).

46. *See generally* JOHN SULLIVAN, ETA AND BASQUE NATIONALISM: THE FIGHT FOR EUSKADI, 1890-1986 (Routledge, London, 1988).

47. *Id.*

48. *See* Cilluffo, *supra* note 43, at 149. Likewise, hackers caused an Irish ISP, Connect-Ireland, to suspend the East Timorese domain (.tp) which it hosted. The Indonesian embassy in London denied that the Indonesian government sponsored the attack. *See* THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT 24 (Aegis Research Corporation, Falls Church, 2000).

fears of terrorists' aircraft falling from the sky through sabotaged air traffic control systems or of pharmaceutical products becoming corrupted[49] have not materialized. Systems are generally suitably complex and can be designed against attack. Furthermore, the death of people is seen to have more allure for terrorists than the death of machines. Consequently, there is no clear evidence that more serious attacks on critical infrastructure via the Internet have been perpetrated by terrorists, so that computers are more often the means to achieving terrorist purposes rather than the objects of attack[50]

B. Communications

The Internet is a widely available, fast and cheap mode of communication. It is especially accommodating for those groups which have transnational networks. Its facility for encryption is additionally a boon to those who wish to plot in the shadows. An interesting example arises from the case of Zacarias Moussaoui, who was charged as a conspirator in the September 11th attacks.[51] The FBI only discovered that Moussaoui had utilised three Hotmail accounts through his written pleadings in July and August 2002. Amongst the challenges faced by investigators in that case is the initial problem that the identities of account-holders are not verified by Microsoft, the owners of Hotmail. Provided the account-holder gives a false identity,[52] does not use a traceable IP address (which can be achieved by using an Internet terminal in a public library, Internet cafe[53] or shopping mall), and does not download information to a traceable storage mechanism like a hard-disk or floppy disk,[54] the usage can remain anonymous. Microsoft can in

---

49. Barry Collin, *The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*, INST. FOR SECURITY AND INTELLIGENCE, *available at* http://afgen.com/terrorism1.html (last visited Jan. 13, 2006).

50. *See* Sarah Gordon & Richard Ford, *Cyberterrorism?*, 21 COMPUTERS & SECURITY 636; Weimann, *The Sum of All Fears*, *supra* note 38, at 130.

51. For the indictment against him, *see* U.S. Department of Justice, Moussaoui Indictment, *available at* http://www.justice.gov/ag/moussaouiindictment.htm (Dec. 2001). He entered a guilty plea in April 2005. Jerry Markon, *Moussaoui Pleads Guilty in Terror Plot*, THE WASHINGTON POST, Apr. 23, 2005, at A01. A sentencing trial is pending. *Id.*

52. Moussaoui's accounts were called xdesertman@hotmail.com, pilotz123@hotmail.com and Olimahammed2@hotmail.com, with his registered name in one case as Zuluman Tangotango. *U.S. v. Moussaoui, Government's Response to Court's Order on Computer and Email Evidence*, *available at* http://news.findlaw.com/hdocs/docs/terrorism/usmouss90402grsp.pdf (last visited Jan. 13, 2006).

53. *Id.* Moussaoui was a customer of Kinko's, a company which also strengthens privacy by wiping the memory of their computers every twenty-four hours. Kinko's, http://www.kinkos.com (last visited Jan. 13, 2006).

54. *Id.* The "http" log of the computer that was used will only show that the site

theory trace messages by a combination of IP address and date/time of the message, provided the information has not been erased from its records because an account has been inactive for thirty days; however, the company refuses to do this as a matter of policy. Even this potential path to detection can be defeated by the use of more sophisticated anonymised web browsing systems such as Anonymizer.com.[55] Even Al Qa'ida has fleetingly made an appearance through websites[56] which have either been hosted by unwitting legitimate ISPs or furtively embedded within other websites without the owners' knowledge, with potential readers being informed of their locations through bulletin boards.[57] It is said that these sites are:

> central to al-Qaida's strategy to ensure that its war with the US will continue even if many of its cells across the world are broken up and

---

http://www.hotmail.com was visited and not any e-mail details. *Id.*

55. For attempts to counter these techniques, *see* C. Walker & and Y. Akdeniz, *Anti-Terrorism Laws and Data Retention: War is Over?*, 54 N. IR. LEGAL Q. 159 (2003) (explaining Anti-Terrorism, Crime and Security Act, 2001, c.24, §§ 102-07 (U.K.). *See also* PRIVY COUNSELLOR REVIEW COMMITTEE, ANTI-TERRORISM, CRIME AND SECURITY ACT 2001 REVIEW, 2003-04, H.C. 100 Part D, para. 410; HOME OFFICE, COUNTER TERRORISM POWERS, 2004, Cm. 6147, at para. 145.

56. Thomas, *supra* note 42. According to Thomas, the sites include the following:

- alneda.com, which US officials said contained encrypted information to direct al Qaeda members to more secure sites, featured international news on al Qaeda, and published articles, fatwas (decisions on applying Muslim law), and books.
- assam.com, believed to be linked to al Qaeda (originally hosted by the Scranton company BurstNET Technologies, Inc.), served as a mouthpiece for jihad in Afghanistan, Chechnya, and Palestine.
- almuhrajiroun.com, an al Qaeda site which urged sympathizers to assassinate Pakistani President Musharraf.
- qassam.net, reportedly linked to Hamas.
- jihadunspun.net, which offered a 36-minute video of Osama bin Laden.
- 7hj.7hj.com, which aimed to teach visitors how to conduct computer attacks.
- aloswa.org, which featured quotes from bin Laden tapes, religious legal rulings that "justified" the terrorist attacks, and support for the al Qaeda cause.
- drasat.com, run by the Islamic Studies and Research Center (which some allege is a fake center), and reported to be the most credible of dozens of Islamist sites posting al Qaeda news.
- jehad.net, alsaha.com, and islammemo.com, alleged to have posted al Qaeda statements on their websites.
- mwhoob.net and aljehad.online, alleged to have flashed political-religious songs, with pictures of persecuted Muslims, to denounce US policy and Arab leaders, notably Saudi.

Id.

57. Michelle Delio, *Al Qaeda Website Refuses to Die* (2003), *available at* http://www.wired.com/news/print/ 0,1294,58356,00.html. The domain name, Al Neda was later taken over by a private US citizen, Jon Messner. *Id.*

> its current leaders are killed or captured. The site's function is to deepen and broaden worldwide Muslim support, allowing al-Qaida or successor organisations to fish for recruits, money and political backing.[58]

C. *Personnel and Logistical Support*

Recruitment may be a by-product. The web presence increases public consciousness of the group, but security demands will not normally allow any direct approaches.[59] Nevertheless, some enthusiasts do risk prosecution, such as Sheikh Omar Bakri Mohammed,[60] who is said to have used Internet chat-rooms to encourage support for his organization, Al-Muhajiroun, and for Jihadist groups in general.[61] Likewise, security considerations limit the role of open websites in fund-raising operations, but websites for fund-raising have still been more commonly found than websites for recruitment.[62]

D. *Intelligence Gathering*

Since all manner of life is present on the web, it is possible to obtain information about possible targets, such as defence facilities,[63] as well as the addresses of individual targets.[64] It is also not just a myth that it is possible to find instructions on how to make a nuclear weapon[65] or,

---

58. Paul Eedle, *Terrorism.com: How Does Al_Qaida Stay Organized When its Members are in Hiding and Scattered Across the World?*, THE GUARDIAN, July 17, 2002, at 4.

59. Yariv Tsfati & Gabriel Weimann, *www.terrorism.com: Terror on the Internet*, 25 STUD. IN CONFLICT & TERRORISM 317, 327 (2002). *See also* Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, U.S. INST. OF PEACE (2004), http://www.usip.org/pubs/specialreports/sr116.html.

60. Under pressure from the Home Office because of his activities, Sheikh Omar Bakri Mohammed left the United Kingdom and has taken up residence in Lebanon. As a Syrian national, he was later banned from returning to the United Kingdom on grounds that his return would not be conducive to the public good or to national security. *See* Ben Hall, *Radical Cleric Bakri Barred from Entry,* FINANCIAL TIMES (London), Aug. 13, 2005, at 4; Sean O'Neill, *Radical Cleric Kept Up Inflammatory Rhetoric Despite Becoming an Outcast,* THE TIMES (London), Aug. 9, 2005, at 1.

61. Sean O'Neill, *Radical Cleric Who Has Never Been Prosecuted,* THE TIMES (London), Jan. 17, 2005, at 4.

62. Tsfati, *supra* note 59, at 327.

63. British Army facilities in Northern Ireland used to be listed on Sinn Féin's web-site. The Alfred P. Murrah building in Oklahoma, attacked in 1995, had been listed on U.S. militia sites as a facility especially vulnerable to car bombs. Silke, *supra* note 10, at 15.

64. Section 45 of the Criminal Justice and Police Act of 2001 amends company law to allow the suppression of personal details of directors so as to protect them from animal rights activists. Criminal Justice and Police Act, 2001, c.16, § 45 (U.K.).

65. The Nuclear Weapon Archive: A Guide to Nuclear Weapons,

perhaps more realistically, a pipe or nail bomb.[66] In the case of Mohammed Naeem Noor Khan, who was arrested in Pakistan in July 2004, his computer materials revealed plans to attack targets, especially financial institutions, in London, New York and New Jersey; a degree of panic ensued though it was later confirmed that the plans were three or four years old.[67] Khan is reported to have admitted that "most of al-Qaeda's communication was done through the Internet."[68] Khan, who is also known as Abu Talha, "is said to have helped in evaluating potential American and British targets for terror attacks."[69] It should be noted that the nature of the intended attacks was probably "conventional" rather than a cyber-attack, as was the case with other incriminating data from laptops found in Afghanistan in 2002.[70] Nevertheless, Defense Secretary Donald Rumsfeld observed that an Al Qa'ida training manual recovered in Afghanistan said, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[71]

E. Propaganda

In this section, we are moving from web activities which relate to the preparation or conduct of terror through to the "theater of terror," which is aimed at onlookers rather than at victims.[72] In this way, terrorists can amplify their actions and importance. Some groups operate their own sites.[73] Examples include Harakat ul Mujahideen (HM),[74] a

---

http://nuclearweaponarchive.org (last visited Jan. 14, 2006).

66. Many sites offer a version of the *Anarchist's Cookbook.* The original *Anarchist's Cookbook* by William Powell, is no longer in print, as the author has renounced his former views. *See* Amazon.com Books Page, http://www.amazon.com/exec/obidos/tg/detail/-/0962303208/103-0016069-2583060?v=glance/ (last visited Jan. 14, 2006).

67. *See* Zahid Hussain, *Confessions of a Computer Expert Gave US Vital Clues,* THE TIMES (London), Aug. 3, 2004, at 1; Daniel McGrory, *Al-Qaeda Computer Whizkid with a Flawless English Accent,* THE TIMES (London), Aug. 4, 2004, at 4. In the UK, the files on Khan's computers included a plan of the layout of Heathrow and information from reconnaissance of the Canary Wharf complex. Michael Evans & Sean O'Neill, *How Al-Qaeda's London Plot Was Foiled,* THE TIMES (London), Nov. 24, 2004, at 4. There were also suggestions for "picture postcard" targets, such as the Houses of Parliament and Windsor Castle, and discussions of potential assassination targets. *Id.*

68. *Id.*

69. *Id.*

70. *See* Weimann, *The Sum of All Fears, supra* note 38, at 143.

71. Thomas, *supra* note 42, at 117.

72. *See* GABRIEL WEIMANN & CONRAD WINN, THE THEATER OF TERROR: MASS MEDIA AND INTERNATIONAL TERRORISM (Longman Group, United Kingdom, 1993).

73. A list is provided by Tsfati, *supra* note 59, at app.

74. *See* Harkat-ul-Mujahideen: Latest News & Articles on Jihad & Kashmir, http://www.harkatulmujahideen.org (last visited Jan. 14, 2006).

militant group based in Pakistan and operating primarily in Kashmir, which was formed in 1993 as Harakat ul-Ansar. Its prime goal is to oppose Indian security forces, but it has also attacked civilians and Western tourists. It is claimed that HM has supporters in several areas of the United Kingdom, as a result of which its actions are proscribed by Part II of the Terrorism Act 2000. Another example is the Kurdistan Workers' Party (Partiya Karkerên Kurdistan or PKK).[75] The PKK was founded in 1974 and seeks an independent Kurdish state in south-eastern Turkey. It engaged in armed attacks from 1984 until after the capture of its leader, Abdullah Őcalan,[76] following which a ceasefire was called for on September 1, 1999, though it broke down (save for a short period) after 2004. The Liberation Tigers of Tamil Eelam, which was founded in 1972 and is the most powerful group in Sri Lanka fighting for a distinct Tamil state, has maintained a website since 1997.[77] Likewise, Hizbollah (The Party of God) is the Lebanese-based Islamic movement founded after the Israeli military seizure of Lebanon in 1982. It seeks the creation of an Iranian-style Islamic republic in Lebanon and the removal of all Israeli and Western influences in the area, including by kidnappings and suicide bombs. It has in the past maintained a website,[78] though the site has now ceased to operate. The webmaster made the following comments concerning the site's value to the organization:

> "In this technological revolution," explained Hussein Naboulsi, who runs the website, "one is obliged to get involved in it one way or another—we can't live outside our era or time. The use of websites has become like water to human beings, thus it is more than necessary to keep pace with the means of expression in our time."
>
> Asked if the site has made a difference to the way that Hezbollah is perceived in the world, Naboulsi was philosophical.
>
> "We don't expect to gain support and sympathy overnight," he replied by e mail, "though the feedback is great. The good thing is that thousands of westerners are able to get a picture about the party directly from our mouth. We receive thousands of e-mails, and we answer the questions of the people. I remember a westerner, an old man, wrote to me saying: 'I need you to answer my questions.' His questions were aggressive, but after a week of exchanging Q&A e-mails, he wrote to me saying: 'Thanks to God that I know the truth

75. *See* Partiya Karkerên Kurdistan Worker's Party, http://www.pkk.org (last visited Jan. 14, 2006).

76. Őcalan v Turkey, App. No. 46221/99, Judgment 12 May 2005.

77. *See* Tamil Eelam Home Page, http://eelam.com (last visited Jan. 14, 2006).

78. The now defunct website was originally located at www.hizbollah.org.

before I die.'"[79]

The objective of these sites is primarily informational. They contain details of history, ideology, leadership and news; violent activities tend to be downplayed, although their vindication is explained.[80] The audience includes both supporters and "the international 'bystander' public and surfers," with some sites even seeking to enter the homes and minds of the "enemy."[81]

Because of harassment and threats from the authorities, which often translate into closure proceedings taken by Internet Service Providers (ISPs), the sites are operated by sympathisers who speak in more guarded language. In addition to sites related to organizations, the "propaganda of the deed"[82] has been very much adopted by some insurgent groups in Iraq who have used websites to show the killings of western hostages. These postings often vanish quickly, but not before they have been publicized and replicated by legitimate sources as well as the more outlandish inhabitants of the Internet.[83]

The series began with Nick Berg in May 2004.[84] The web addresses that posted the Nick Berg decapitation video were based on a web server in Malaysia with webmasters in London, England and Nurnberg, Denmark.[85] The technique was borrowed from the case of U.S. reporter Daniel Pearl, who was beheaded by Islamists in Pakistan in February 2002; a video was released of his killing.[86] Another widely publicised event was the killing of Ken Bigley, the first British hostage to be killed,

79. A. Mueller, *Propaganda Skirmishes in Cyberspace,* THE SUNDAY TIMES (London), Mar. 23, 2003, at 52.

80. Tsfati, *supra* note 59, at 321.

81. *Id.* at 326.

82. "Propaganda of the Deed" derives from the doctrine that spectacular action by an individual or an activist group may inspire further action by others. *See* A.H. Garrison, *Defining Terrorism: Philosophy of the Bomb, Propaganda by Deed and Change Through Fear and Violence,* 17 CRIM. JUST. STUD.: A CRITICAL J. OF CRIME, L. AND SOC. 259 (2004). It was associated with anarchists such as Kropotkin, who is associated with the epigram that "[a] single deed is better propaganda than a thousand pamphlets." *Id.*

83. *See, e.g.,* Ogrish.com: Uncover Reality, http://www.ogrish.com/index.html/ (last visited Jan. 14, 2006); World of Death, http://www.everwonder.com/david/worldofdeath/ (last visited Jan. 14, 2006).

84. *See, e.g.*. Camera/Iraq: The War of Images in the Middle East, Nicholas Berg Beheading (May 8, 2004), http://www.camerairaq.com/2004/05/nick_berg_video.html; Encoderx: Nick Berg Execution, http:// encoderx.co.uk/nickberg/ (last visited Jan. 14, 2006).

85. The sites were originally located at www.al-asnar.net and www.al-asnar.biz. *See also* Alex Jones, Prison Planet.tv, http://www.prisonplanet.tv/articles/may2004/051104beheadsuscivilian.htm (last visited Jan. 14, 2006).

86. Omar Sheikh was convicted of the murder. *See* Zahid Hussain, *A Lonely Wait for the Hangman,* THE TIMES (London), Jul. 16, 2002, at 3 (describing Sheikh's pending appeal); *Video Shows Reporter Killed Then Beheaded,* IRISH NEWS, Feb. 23, 2002, at 13; IRISH TIMES, Feb. 25, 2005, at 21.

by the group Tawhid wa al-Jihad, which proclaimed allegiance to Abu Musab al-Zarqawi in October 2004.[87] Bigley was seized along with Americans Eugene Armstrong and Jack Hensley, who were also beheaded. The drama was enhanced by the dressing of Bigley in orange overalls and placing him in a cage, intended to be reminiscent of equivalent uniforms worn by prisoners of the U.S. Government in Guantánamo Bay's Camp Delta.[88]

III. Legal Responses

In terms of legal reactions, we can again corral them into just two headings: hostile cyber-attacks and ancillary cyber-activities. There is a legal reaction to each, and the danger in each case is that the legal reaction may be excessive because of a failure to adhere to the legal principles adduced earlier.

A. Hostile Cyber-Attack

The first category of cyber-terrorism contemplates various forms of hostile activity. In short, this category encompasses "information warfare." Information warfare is terrorist activity designed seriously to interfere with or to harm or disrupt communication. Information warfare might involve direct incursions on computer systems which could trigger threats to life, such as interference with air traffic control systems or hospital records. However, information warfare is more likely to involve the defacing of website text or images, the use of viruses, or the denial of service attacks through multiple key striking software, called "ping" engines, or through e-mail bombs, none of which causes physical damage but may fundamentally compromise the provision of information and services.[89]

Does all of this activity have the capacity to terrorise as opposed to damage or offend or inconvenience? In legal principle, only the truly terrorising should require a special legal response. One should

87. *See* Stephen Farrell & Michael Evans, *'Help Me Now, Mr. Blair. You Are the Only Person on God's Earth Who Can,'* THE TIMES (London), Sept. 23, 2004, at 6; Daniel McGrory, *Briton's Family Waits in Fear as US Hostage is Beheaded,* THE TIMES (London), Sept. 21, 2004, at 1; Daniel McGrory & James Hider, *Ken Bigley is Beheaded,* THE TIMES (London), Oct. 9, 2004, at 1.

88. *Id.*

89. *See* DENNING, INFORMATION, *supra* note 35; V. Mitliaga, *Cyberterrorism* LEGAL EXECUTIVE 4 (2002); J.M. Post et. al, *From Car Bombs to Logic Bombs,* 12(2) TERRORISM & POL. VIOLENCE 97 (2002); L. Valeri & M. Knights, *Affecting Trust: Terrorism, Internet and Offensive Information Warfare,* 12(1) TERRORISM & POL. VIOLENCE 15 (2002); Winn Schwartan, Infowar.com, http://www.infowar.com (last visited Jan. 14, 2006).

distinguish the direct from the indirect threat and should identify a threat to the well-being of an individual rather than to a machine. A direct threat might include interference which could cause aircraft to collide or cause hospitals to administer the wrong treatment. These could be paralysing challenges to the capacity of the state to run civil life and, if carried out, could harm individuals. To the contrary, activities such as defacing, corrupting or denying are unlikely to have the same impact on the lives of individuals, even if the potential disruption to the capacities of state agencies remains large and of increasing significance. These activities also shade into forms of political activism which we should hesitate to demonise with the title "terrorism" even if they infringe such elements of the criminal law as the Computer Misuse Act 1990[90] or the Criminal Damage Act 1971.[91] Is it "terrorism" for teachers to go on strike and thus deny to the public important public services any more than it is terrorism for animal rights protestors to try to bring down a website? While the direct and indirect may sometimes be conflated in political discourse,[92] it would ignore principles of various rights (such as the right to protest and to express opinions) and of proportionality to use draconian anti-terrorism powers against the latter.

Bearing these criticisms in mind, there is greater justification for offences relating to intelligence-gathering, including intelligence-gathering via the Internet, where the outcome could be some kind of murderous attack on individuals. There are two overlapping offences in the Terrorism Act 2000[93] which deal with this activity. One is section 58 of the Act—offences of the collecting or recording or possessing information of a kind likely to be useful to a person committing or preparing an act of terrorism.[94] A "record" includes photographic or electronic formats as well as writings and drawings, but mental notes and knowledge which is not recorded in any form are not covered.[95]

The main controversy surrounding section 58 concerns the equivocal nature of the actions involved and the fact that it is left to the defendant to prove as a defence, under sub-section (3), that he had a reasonable excuse for his action or possession.[96] The indeterminate range of the offence has also given rise to alarm on the part of journalists: "What journalist worth his or her salt does not have a contacts book? A cuttings file? A file on the activities and personal

90. Computer Misuse Act, 1990, c.18 (U.K.).
91. Criminal Damage Act, 1971, c.48 (U.K.).
92. Silke, *supra* note 10, at 17.
93. Terrorism Act, 2000, c. 11 (U.K.).
94. *Id.* § 58.
95. *Id.*
96. *Id.*

details of prominent public figures?"[97]

Indeed, one could add that a wide range of people, including academic scholars, can become effective investigators and collators of information by using Internet sources such as the website directory 192.com[98] or by using documents freely available on the web, such as *The Terrorist's Handbook* and *The Big Book of Mischief.* It follows that it is not necessary under section 58 to show that the information was obtained or held in breach of the law; the possession of Army manuals was the basis for conviction in *R v. Lorenc.*[99]

Section 58 is augmented for Northern Ireland by section 103 which relates to the protection of specified security force personnel and other public officials.[100] For example, the possession of Army manuals was the basis for conviction in *R v. Lorenc*[101] and the possession of planning and training materials was the basis in *Re Kerr's Application.*[102] Though the penalties are the same, section 103 is broader than section 58 in several respects. For example, the *actus reus* includes publishing, communicating or attempting to elicit, as well as collecting or recording.[103] As with section 58, the main controversy concerns the equivocal nature of the actions involved and the fact that it is left to the defendant to prove as a defence, under sub-section (5), that he had a reasonable excuse for his action or possession.[104] In *R v. McLaughlin*,[105] a radio enthusiast was able to show reasonable excuse for possessing a list of RUC radio frequencies. There is the further presumption in sub-section (4) that if it is proved a document or record: "(a) was on any premises at the same time as the accused, or (b) was on premises of which the accused was the occupier or which he habitually used otherwise than as a member of the public," the court may assume that the accused possessed the document or record, unless he proves that he did not know of its presence on the premises or that he had no control over it.[106] According to section 118, which applies to both sub-sections (4) and (5), if evidence is adduced which is sufficient to raise an issue, the court shall treat it as proved unless the prosecution disproves it beyond reasonable doubt.[107]

97. L. Hickman, *Press Freedom and New Legislation,* 151 NEW L. J. 716 (2001).
98. 192.com Home Page, http://192.com (last visited Jan. 14, 2006).
99. R v. Lorenc, [1988] N.I. 94.
100. Terrorism Act, 2000, c. 11, § 103 (U.K.).
101. R v. Lorenc, [1988] N.I. 94.
102. *Re* Kerr's Application, [1997] N.I. 225.
103. Terrorism Act, 2000, c. 11, § 103 (U.K.).
104. *Id.*
105. R v. McLaughlin, [1993] N.I. 28.
106. Terrorism Act, 2000, c. 11, § 103 (U.K.).
107. *Id.* § 118.

The case of David Copeland might be considered as a test for whether there should be offences against intelligence-gathering activities.[108] David Copeland carried out a series of three bombings in London in 1999 out of racist and homophobic motives.[109] Part of the evidence at his trial was that he had obtained the information on how to make bombs from Internet sources, such as *The Terrorists' Handbook* and *How to Make Bombs Book Two*. These and other relevant materials, like *The Anarchist's Cookbook* and *The Big Book of Mischief*, are readily available through any search engine. There are, however, two caveats. The first is that such information is also available in books, including books written for lay-people.[110] Second, it turned out that David Copeland could not assemble the necessary ingredients indicated in the web-based guides and instead resorted to an even less sophisticated bomb made out of fireworks material.[111] Further reflection shows the dangers of overreaching. If possession of the addresses of government buildings amounts to terrorist intelligence, then are we to ban telephone directories and the use of the Internet to provide government services? Inevitably, an open society may be more vulnerable to attack than a closed society, but the better strategies against terrorism lie in activities such as state intelligence-gathering rather than in shutting down the open society.

B. Support Cyber-Activities

Other forms of computer use by terrorist groups exist to support their political or military objectives. The use includes internal and external communications, fund-raising, recruitment and propaganda.[112] These activities do not terrorise *per se*, so only if they are linked to a terrorist group should legal action be taken under special laws. In other words, legal action should be taken not because of a direct capacity to terrorise but because of the need to reduce the viability of organisations with the capacity to terrorise by other means. However, if these

108. Silke, *supra* note 10, at 17.

109. Stewart Tendler & Tim Reid, *Soho Bomber Was Wicked Not Insane,* THE TIMES (London), July 1, 2000, at 1.

110. *See e.g.,* G. GRIVAS-DIGNHENIS, GUERILLA WARFARE AND EOKA'S STRUGGLE (Longmans, London, 1964).

111. M. Wolkind & N. Sweeney, *R v. David Copeland,* 41 MED. SCI. L. 185, 190 (2001). Likewise, the perpetrators of the London suicide bombings of July 7 and July 21, 2005, allegedly manufactured their bombs from peroxide materials which can be derived from common household goods. Daniel McGrory & Sean O'Neill, *Inside the Hunt for London Bombers,* THE TIMES (London), Aug. 6, 2005, at 11.

112. *See* K.R. Damphousse & B.L. Smith, *The Internet, in* THE FUTURE OF TERRORISM (H.W. Kushner ed., Sage Publications, Thousand Oaks, 1998).

activities are not linked to a terrorist, and preferably proscribed,[113] group, then there is again the danger of crossing over into political activism which, palatable or not, or even legal or not, should not be equated with terrorism.

The Terrorism Act 2000 does deal with support cyber-activities relating to proscribed organisations in section 12 of the Act.[114] Part III of the Act is wider and deals with "Terrorist Property" even if the organisation is not proscribed.[115] There are again some elements of overreaching. One example is the offence of possession of items useful to terrorism under section 57 of the Terrorism Act 2000.[116]

The offence of possession of items for terrorist purposes in section 57 had been an offence in Northern Ireland since the time of section 30 of the Northern Ireland (Emergency Provisions) Act 1991[117] and was later set out in section 32 of the Emergency Provisions Act 1996.[118] The offence originated pursuant to the recommendation of the Review of the Northern Ireland (Emergency Provisions) Acts 1978 and 1987,[119] though the idea was then confined to possession in public places. Then, section 63 of the Criminal Justice and Public Order Act 1994 extended a possession offence to Britain by way of section 16A of the Prevention of

113. Proscription is allowed under Part I of the Terrorism Act, 2000, c. 11, § 103 (U.K.). Some groups (both Irish based and foreign) are listed in the Act itself (section 3(1)). Others (all foreign based) have been added by statutory instruments on the authority of the relevant government Minister (section 3(3)). *See* WALKER, BLACKSTONE'S, *supra* note 18, at ch. 2. This form of proscription triggers offences in sections 11 to 13 against membership or speaking or organising on behalf of the proscribed group. The Act therefore includes, but goes well beyond, the prohibition on the funding of listed non-domestic groups in Title IIIA of the Anti-terrorism and Effective Death Penalty Act, 18 U.S.C. § 2339B (2005). The grounds for proscription under the Terrorism Act 2000 are to be further widened by the Terrorism Bill, 2005-06, H.L. Bill [56], cl. 21.

114. Terrorism Act, 2000, c. 11, § 12 (U.K.).

115. *Id.* §§ 14-31.

116. *Id.* § 57. *See also* THE PRIVY COUNSELLOR REVIEW COMMITTEE, ANTI-TERRORISM, CRIME AND SECURITY ACT 2001 REVIEW, 2003-4, H.C. 100 Part D, at para. 276 (expressing no objections to the offences in Part VI of ATCSA). The penalties under section 57 are to be increased by the Terrorism Bill, 2005-06, H.L. Bill [56], cl. 13. Furthermore, a new offence is proposed under clause 5(1) of the Bill: "A person commits an offence if, with the intention of (a) committing acts of terrorism, or (b) assisting another to commit such acts, he engages in any conduct in preparation for giving effect to his intention." *Id.* at cl. 5(1). The new offence covers forms of intangible preparations—giving information or advice—wheras section 57 demands that the preparation offence involve some tangible item. *See also* JOINT COMMITTEE ON HUMAN RIGHTS, COUNTER TERRORISM POLICY AND HUMAN RIGHTS, 2005-06, H.L. 75-I/H.C. 561.

117. Northern Ireland (Emergency Provisions) Act, 1991, c. 24, § 30 (U.K.).

118. Northern Ireland (Emergency Provisions) Act, 1996, c. 22, § 32 (U.K.).

119. REVIEW OF THE NORTHERN IRELAND (EMERGENCY PROVISIONS) ACTS 1978 & 1987, 1990, Cm. 1115, at para. 2.9.

Terrorism Act.[120] Continuance was supported by Lord Lloyd as allowing early police intervention,[121] and so the offence now appears as section 57 of the Terrorism Act for the whole of the United Kingdom.[122] It has become one of the most controversial debating points during its passage, even though it remains largely unchanged since 1994.

According to section 57(1), a person commits an offence if he "possesses an article in circumstances which give rise to a reasonable suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism."[123] The penalties are the same as for section 54.[124] There is no need for any proof of a terrorist purpose in the mind of the possessor. It is notable that there is again no link to proscribed organisations, so the perpetrators may include, in accordance with the definition in section 1, animal liberation activists seeking to attack a laboratory.[125] The articles concerned will be lawful in themselves and even commonplace; in this regard, section 57 differs markedly from offences such as possession of an offensive weapon or going equipped for theft. There is no need for section 57 to deal with those caught red-handed in possession of explosives and firearms. Rather, items such as wires, batteries, rubber gloves, scales, electronic timers, overalls, balaclavas, agricultural fertilizer and gas cylinders, especially in conjunction, are the concern of section 57. The wide range of articles which may attract suspicion highlights the problematic nature of section 57. The actions of the suspects at this stage are highly equivocal—persons with overalls and balaclavas may be preparing for an attack on a police patrol or on a rabbit warren. In this way, there is an extension of the criminal law to put people in the dock for activities which do not require actions directly related to terrorism or the intention of being involved in terrorism.

Proof of "possession" is aided by sub-section (3). If it is proved that an article: "(a) was on any premises at the same time as the accused, or (b) was on premises of which the accused was the occupier or which he habitually used otherwise than as a member of the public," the court may assume that the accused possessed the article, unless he proves that he did not know of its presence on the premises or that he had no control over it.[126]

120. Criminal Justice and Public Order Act, 1994, c. 33, § 63 (U.K.); Prevention of Terrorism Act, 2005, c. 2, § 16A (U.K.).

121. INQUIRY INTO LEGISLATION AGAINST TERRORISM 14.6 (Cm. 3420, Stationery Office, 1996).

122. Terrorism Act, 2000, c. 11, § 57 (U.K.).

123. *Id.* § 57(1).

124. *Id.* § 54.

125. *Id.* §§ 1, 57.

126. *Id.* § 57(3).

Recognising the possible overreach of section 57, sub-section (2) offers a defence for a person charged with an offence to prove that "his possession of the article was not for a purpose connected with the commission, preparation or instigation of an act of terrorism."[127] In addition, under section 57(3), it is open to the defendant to show that he either did not know of the presence of the item on the premises or had no control over it.[128] It has been argued that this defence does not alleviate the unfairness of the offence and in fact perpetrates another by switching the burden of proof to the defence, contrary to Article 6(2) of the European Convention on Human Rights and Fundamental Freedoms.[129]

The meaning of the offence and its possible breach of article 6(2) by undermining the presumption of innocence have been considered by the House of Lords in *R v. Director of Public Prosecutions,* ex parte *Kebilene.*[130] Their Lordships ultimately decided the case on the technical ground of the non-reviewability of prosecution decisions, but opinions were divided between the House of Lords and the Court of Appeal on the complaint of a breach of Article 6(2).[131] An illuminating analysis of the problem was provided in the speech of Lord Hope:

> It is necessary in the first place to distinguish between the shifting from the prosecution to the accused . . . the "evidential burden," or the burden of introducing evidence in support of his case, on the one hand and the "persuasive burden," or the burden of persuading the jury as to his guilt or innocence, on the other. A "persuasive" burden of proof requires the accused to prove, on a balance of probabilities, a fact which is essential to the determination of his guilt or innocence. It reverses the burden of proof by removing it from the prosecution and transferring it to the accused. An "evidential" burden requires only that the accused must adduce sufficient evidence to raise an issue before it has to be determined as one of the facts in the case. The prosecution does not need to lead any evidence about it, so the accused needs to do this if he wishes to put the point in issue. But if it is put in issue, the burden of proof remains with the prosecution. The accused need only raise a reasonable doubt about his guilt.
>
> Statutory presumptions which place an "evidential" burden on the accused, requiring the accused to do no more than raise a reasonable doubt on the matter with which they deal, do not breach the presumption of innocence. They are not incompatible with article

127. *Id.* § 57(2).
128. *Id.* § 57(3).
129. European Convention on Human Rights and Fundamental Freedoms, art. 6(2), Nov. 4, 1950, ETS 5, 213 U.N.T.S. 17.
130. R v. Director of Public Prosecutions, *ex parte* Kebilene, [2000] 2 AC 326.
131. *Id.*

6(2) of the Convention. They take their place alongside the common law evidential presumptions which have been built up in the light of experience. They are a necessary part of preserving the balance of fairness between the accused and the prosecutor in matters of evidence. It is quite common in summary prosecutions for routine matters which may be inconvenient or time-consuming for the prosecutor to have to prove but which may reasonably be supposed to be within the accused's own knowledge to be dealt with in this way. It is not suggested that statutory provisions of this kind are objectionable.

Statutory presumptions which transfer the "persuasive" burden to the accused require further examination. Three kinds were identified by the applicants in their written case.... First, there is the "mandatory" presumption of guilt as to an essential element of the offence. As the presumption is one which must be applied if the basis of fact on which it rests is established, it is inconsistent with the presumption of innocence. This is a matter which can be determined as a preliminary issue without reference to the facts of the case. Secondly, there is a presumption of guilt as to an essential element which is "discretionary." The tribunal of fact may or may not rely on the presumption, depending upon its view as to the cogency or weight of the evidence. If the presumption is of this kind it may be necessary for the facts of the case to be considered before a conclusion can be reached as to whether the presumption of innocence has been breached. In that event the matters cannot be resolved until after trial.

The third category of provisions which fall within the general description of reverse onus clauses consists of provisions which relate to an exemption or proviso which the accused must establish if he wishes to avoid conviction but is not an essential element of the offence....

These provisions may or may not violate the presumption of innocence, depending on the circumstances.

Two further important points need to be made about this classification. The first is that this is not an exact science. The provisions vary so widely in their detail as to what the prosecutor must prove before the onus shifts, and their effect on the presumption of innocence depends so much on circumstances. These matters may not be capable of being fully assessed until after the trial. The best that can be done, by way of a preliminary examination, is to see whether the legislative technique which has been adopted imposes a persuasive or merely an evidential burden, whether it is mandatory or

> discretionary and whether it relates to an essential element of the offence or merely to an exception or proviso. The second is that, even if the conclusion is reached that prima facie the provision breaches the presumption of innocence, that will not lead inevitably to the conclusion that the provision is incompatible with article 6(2) of the Convention. The European jurisprudence, which I shall examine later, shows that other factors need to be brought into consideration at this stage.[132]

In this way, it is desirable to ensure that the interpretation of section 57(3) imposes an initial evidential burden—a requirement to raise evidence in support of an issue in a case—on the defence but thereafter the burden is taken up by the prosecution to disprove there is any defence. It is also important to emphasise that the final burden of proof of guilt beyond a reasonable doubt, including proof of all essential facts, such as possession and reasonable suspicion of a terrorist purpose, remains on the prosecution. Such restraint is more likely to satisfy article 6(2) as interpreted in the jurisprudence of the European Court of Human Rights, which does allow for some flexibility in the issue of proof, especially where it can be shown that important social concerns are at stake and that the defendant has ready access to the information required for the defence.[133]

In light of these concerns and conflicting factors, section 118 was added to the Terrorism Act and affects both sections 57(2) and 57(3).[134] According to section 118, if evidence is adduced which is sufficient to raise an issue, the court "shall treat it as proved unless the prosecution disproves it beyond reasonable doubt."[135] This formula was intended to be merely declaratory.[136] In so far as it does impact on the problem, however, it would seem to prevent section 57 from placing any "legal" or "persuasive" burden upon the defendant by ensuring that, once raised, the issue remains for the prosecution to prove.[137] It may also slightly ease the evidential burden placed on the defendant by requiring simply that the issue be raised to negate the presumption in the statute, unless the prosecution can prove otherwise.[138]

---

132. *Id.* at 378-80.

133. *See* Salabiaku v. France, App. No. 10519/83, Ser. A 141-A (1988); Brown v. Stott (Procurator Fiscal, Dunfermline) and another, [2003] 1 A.C. 681; R v. Benjafield, [2002] UKHL 2; R v. Lambert, [2001] UKHL 37.

134. Terrorism Act, 2000, c. 11, § 118 (U.K.).

135. *Id.* § 118(4).

136. 613 PARL. DEB., H.L. (5th ser.) (May 16, 2000) 754.

137. *See* B. EMMERSON & A. ASHWORTH, HUMAN RIGHTS AND CRIMINAL JUSTICE para. 9-59 (Sweet & Maxwell, London, 2001); J.J. Rowe, *The Terrorism Act 2000,* [2000] CRIM. L.R. 527, 540.

138. EMMERSON, *supra* note 137, at para. 9-59; Rowe, *supra* note 137, at 540.

Some commentators suggest that the dispute in *Kebilene* was misconceived on the grounds that the prosecution must prove beyond a reasonable doubt not only the possession of the items relevant to section 57 but also reasonable suspicion of the terroristic purpose.[139] In other words, the burden of proof is not shifted at all.[140] A comparison is made with other offences relating to preparatory stages, such as going equipped for theft or possession of an offensive weapon. It is suggested that these analogies are misplaced. The presence of items covered by section 57 is far less suggestive of crime than is the presence of items covered by the other offence. In other words, being in charge of false identity documents, counterfeit credit cards and a three-band radio[141] is much less suggestive of terrorism than possession of a knife or a jemmy is suggestive of an offence against the person or against property. These are not necessarily acts which are "not wrongful at all,"[142] though they are less wrongful than using the items in a further crime.

The fact that the offence of possession is based around, in its second leg, reasonable suspicion only serves to emphasise rather than constrain its breadth. This does not at all mean that the prosecution has "its work cut out to prove the required suspicion beyond reasonable doubt."[143] Proof beyond a reasonable doubt of a reasonable suspicion harboured in the minds of the forces of law and order (and not even a guilty mindset on the part of the accused) is a long way away from proof, in classical Millian terms, of a harm being actually perpetrated by a wrongdoer. Rather, the presence of items can be linked, for example, to associations or expressed beliefs to weave a charge. Thus, the same commentator concedes that section 57 might be said to trivialise the prosecution's burden, especially because it also requires no direct proof of a terroristic purpose.[144] Quite so. The fact that the defendant has to respond to such a relatively light burden is surely not much different at the end of the day than a criticism that the burden of proof is shifted. It is true an offence has to be proven at the outset by the prosecution, but if that takes no great effort, then the real task in court is for the defence, which of course was always the intention of the legislation. It should be part of the

139. *See* R v. Director of Public Prosecutions, *ex parte* Kebilene, [2000] 2 AC 326.

140. P. Roberts, *The Presumption of Innocence Brought Home,* 118 L.Q.R. 41 (2002).

141. For a graphic illustration in the case of Baghdad Meziane and Brahmin Benmerzouga, *see* Steve Bird, *Quiet Existence in Leicester Suburb Masked Complex Terrorist Network,* THE TIMES (London), Apr. 2, 2003, at 11; Leicestershire Constabulary Library, *available at* http://www.leics.police.uk/library/magnesium_information_pack.pdf (last visited Jan. 14, 2006).

142. Paul Roberts, *The Presumption of Innocence Brought Home? Kebilene Deconstructed,* 118 L.Q.R. 41, 56 (2002).

143. *Id.* at 51.

144. *Id.* at 67.

prosecution's burden to show direct proof of a terroristic purpose in the mind of the accused as opposed to a reasonable suspicion in the mind of the police or prosecutor.

A further argument to be considered is that, if the real issue is about the formulation of criminal offences rather than burdens of proof, the European Convention has little relevance since it has nothing to say about substantive criminal law.[145] Yet this narrow stance is by no means assured. It is true that elements of criminal liability are substantive rather than procedural and so fall outside English conceptions of the presumption of innocence, but the European Convention's sense of fairness does seem to be much wider in that it is linked to the overall fairness of process. As was stated in another context in *(John) Murray v. United Kingdom*:

> Although not specifically mentioned in Article 6 of the Convention, there can be no doubt that the right to remain silent under police questioning and the privilege against self-incrimination are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6.
>
> . . .
>
> . . . [I]t is self-evident that it is incompatible with the immunities under consideration to base a conviction solely or mainly on the accused's silence or on a refusal to answer questions or to give evidence himself.[146]

This *dictum* suggests that an offence which made it unlawful, say, to be suspected of murder and then fail to answer police questions in response to those suspicions would not be acceptable. Is that not a statement about substantive criminal law?

It should be realised that there are inchoate offences aplenty in this field. Most obvious is conspiracy to cause explosions under section 3 of the Explosive Substances Act 1883.[147] Surely it is fairer and more convincing to prove "conspiracy" rather than "possession" and a specific wrongful intent—for example, causing explosions rather than terrorism, which is not *per se* an offence.

Adding to the debate is the case of *Attorney General's Reference (No 1 of 2004),*[148] which arose from the impact of section 35 of the

145. *Id.* at 50. *See also* Richard Buxton, *The Human Rights and the Substantive Criminal Law*, [2000] CRIM. L.REV. 331, 332.

146. App. No. 18731/91, Reports 1996-I at paras. 45, 47.

147. Explosive Substances Act, 1883, c. 3, § 3 (U.K.).

148. [2004] EWCA Crim. 1025.

Criminal Procedure and Investigations Act 1996 (procedural points concerning the holding of preparatory hearings).[149] The Court of Appeal gave the firm guidance that the common law and article 6(2) of the European Convention had the same effect—both permitted legal reverse burdens of proof or presumptions in the appropriate circumstances.[150] The overall burden of proof must remain on the prosecution, but there could be exceptions provided they created proportionate evidentiary burdens and were justifiable.[151] Justifiability would be judged by the realistic effects of the reverse burden, including how easy it was for the accused to discharge or how difficult it would be for the prosecution to establish the facts, bearing in mind the seriousness of the offences and the level of penalties.[152]

Arguably more important than the interpretation of section 57 has been the considerable increase in its usage over the past three years. The offence had been charged thirty times in Britain before the Terrorism Act came into force in 1996. In 2000 and 2001, there were no recorded charges.[153] Since then, there have been twenty-two charges in 2002 and twenty-nine in 2003.[154] In effect, we are now close to an offence of terrorism—an offence of involvement rather than commission.

The controversial nature of section 57 is illustrated by the case of Baghdad Meziane and Brahmin Benmerzouga, as described earlier.[155] In addition, it is not clear why section 58 was not invoked against Babar Ahmad, a computer analyst who worked at Imperial College London.[156] He has been accused of material support of terrorism, support of the Taliban and Chechen rebels, conspiracy to kill (including the possession of plans for attacking U.S. warships in the Straits of Hormuz), money laundering, solicitation of funds, and conspiracy.[157] He was also under

149. Criminal Procedure and Investigations Act, 1996, c. 25, § 35 (U.K.).

150. Attorney General's Reference (No 1 of 2004), [2004] EWCA Crim. 1025, at para. 52.

151. *Id.*

152. *Id.*

153. 522 PARL. DEB., H.C. (6th ser.) (Oct. 30, 2003) 966W.

154. HOME OFFICE, REPORT ON THE OPERATION IN 2002 AND 2003 OF THE TERRORISM ACT 2000 Annex D (2004).

155. Bird, *supra* note 141, at 11.

156. Daniel McGrory et al., *Briton 'Had Plans to Attack US Warship'*, THE TIMES (London), Aug. 7, 2004, at 1, 4. Ahmad's web sites were based in Connecticut. *Id.* For further details of his case, *see* FREE Babar Ahmad, http://www.freebabarahmad.com (last visited Jan. 25, 2006).

157. *Id.* The details of the warrant for arrest are set out at http://news.findlaw.com/cnn/docs/ahmad/usahmad72804cmp.pdf (July 28, 2004). The warrant document reveals that Ahmad used PGP encryption but that the keys were readily recovered from data in his residence and in his office at Imperial College, London. *Id.* The offence of material support has in part been declared unconstitutional. *See* Humanitarian Law Project v. Ashcroft, 309 F. Supp. 2d 1185, 1200 (C.D. Cal. 2004);

suspicion for raising money for terrorists through the websites www.azzam.com, www.qoqaz.com and www.waaqiah.com, which Ahmad ran until their closure in November 2001 through internet service providers in Nevada and then Connecticut.[158] He was arrested by British authorities in December 2003 but then released, following which the U.S. authorities commenced extradition proceedings.[159] His extradition was ordered by the Bow Street Magistrates' Court, after a diplomatic note sent to Foreign Secretary Jack Straw by the U.S. Government was produced in court, stating that Mr. Ahmad would not face the death penalty or be sent to Guantánamo Bay.[160] The decision to extradite was confirmed by the Home Secretary in November 2005.

Moving towards legislative action against propaganda, there is an incitement offence in section 59 of the Terrorism Act, which followed a government review[161] and which potentially requires the United Kingdom to protect every crazy government in the world. According to section 59, a person commits an offence if: "(a) he incites another person to commit an act of terrorism wholly or partly outside the United Kingdom, and (b) the act would, if committed in England and Wales, constitute one of the offences listed in subsection (2)."[162] The listed offences are:

> (a) murder,
>
> (b) an offence under section 18 of the Offences against the Person Act 1861 (wounding with intent),
>
> (c) an offence under section 23 or 24 of that Act (poison),
>
> (d) an offence under section 28 or 29 of that Act (explosions), and

---

David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1 (2003). Sami Omar Al-Hussayen, a student at the University of Idaho, was acquitted of providing material support to terrorist groups through websites that prosecutors alleged, in circumstances similar to the case of Babar Ahmad, were used to recruit and raise money for Hamas and other groups. Richard B. Schmitt, *Acquittal in Internet Terrorism Case Is a Defeat for Patriot Act*, LOS ANGELES TIMES, June 11, 2004, at A20.

158. *Id.*

159. *Id.*

160. Daniel McGrory, *Terror Suspect Loses US Extradition Battle*, THE TIMES (London), May 18, 2005, at 6. In the meantime, he had come in fourth in the general election of May 2005 in the Brent North constituency. *Id.*

161. SECRETARY OF STATE FOR THE HOME DEPARTMENT & SECRETARY OF STATE FOR NORTHERN IRELAND, LEGISLATION AGAINST TERRORISM 16 (Cm. 4178, Stationery Office, 1998).

162. Terrorism Act, 2000, c. 11, § 59(1) (U.K.).

(e) an offence under section 1(2) of the Criminal Damage Act 1971 (endangering life by damaging property).[163]

According to sub-section (4), it is expressly "immaterial whether or not the person incited is in the United Kingdom at the time of the incitement."[164] This differs from the extension of conspiracy offences under sections 5 to 7 of the Criminal Justice (Terrorism and Conspiracy) Act 1998 which give the United Kingdom courts jurisdiction over acts of conspiracy in the United Kingdom relating to any offences committed or intended to be committed abroad.[165] If, however, the conspiracy as well as the substantive offence takes place outside the jurisdiction, the conspirators cannot be prosecuted.[166] Corresponding offences to section 59 are set out in section 60 for Northern Ireland[167] and section 61 for Scotland.[168] Incitement via the Internet is likely to be the commonest form of address under this offence.

Sections 59 to 61 turn certain offences into universal crimes when they are not recognised as such elsewhere and in relation to foreign states which are not within the scope of the Suppression of Terrorism Act 1978.[169] Within the context of an incitement from the United Kingdom to intended perpetrators within a foreign country, how can it be said that the "incitement" possibly creates an immediate risk of unlawful serious violence to persons? The immediacy and causal link are diminished from what one normally thinks of as incitement. It is suggested that the offences should at least be confined in two ways. First, in terms of persons, the scope should relate to either the activities of British citizens or incitements to persons who are in the United Kingdom. This would leave a wide offence, given the indiscriminate nature of the Internet and other modern means of communications. Second, in terms of actions, the list of offences should be more clearly politically related and should not go much beyond such internationally recognised offences as hijacking, attacks on internationally protected persons (which already provide for universal jurisdiction for incitement offences) and perhaps even the wider range of terrorist bombing offences under section 62.[170] If confined in these ways, the list of offences would then more clearly reflect the core of terrorism than the current list.

In response, the Home Secretary has argued that sections 59 to 61

163. *Id.* § 59(2).
164. *Id.* § 59(4).
165. Criminal Justice (Terrorism and Conspiracy) Act, 1998, c. 40, §§ 5-7 (U.K.).
166. *Id.*
167. Terrorism Act, 2000, c. 11, § 60 (U.K.).
168. *Id.* § 61 (U.K.).
169. Suppression of Terrorism Act, 1978, c. 26 (U.K.).
170. Terrorism Act, 2000, c. 11, § 62 (U.K.).

resolve anomalies. The aim of the incitement offences is to deter those who seek to use the United Kingdom as a base from which to promote terrorist acts abroad. It is claimed that under the Suppression of Terrorism Act 1978, there is already extra-territorial jurisdiction over a number of serious offences including murder, manslaughter, kidnapping, wounding with intent, and causing explosions, and incitement to any of those offences. It is then argued that, given the limitations of the treaty, "[t]here is no obvious justification for incitement to commit murder in Turkey or India to be an offence in the United Kingdom, whereas incitement to commit murder in Japan or Australia is not an offence."[171] But, as already mentioned, the incitement of many designated terrorist offences (hijacking and so on) already carry universal jurisdiction. Further, one wonders how many cases of incitements have resulted in prosecution instead of extradition under the 1978 Act?[172] From reported cases at least, the answer would appear to be zero, and this is also the figure given in debates by the Minister.[173]

Evidential difficulties may also arise, whereby dissident groups will find it difficult to adduce evidence from overseas as to their true nature and intentions.[174] On the other hand, repressive regimes will be able to present evidence obtained by all kinds of unconscionable means.

The government was of the view that there was a need to balance free speech interests against the unacceptability of "encouraging and glorifying acts of terrorism."[175] However, this is one of the areas where a mature democracy should have maintained its patience with the politically immature and intemperate. Any prosecutions under sections 59 to 61 will be open to challenge under article 10 of the European Convention,[176] especially if made by a person who could be designated as a politician and especially if made against a government.[177]

171. 341 PARL. DEB., H.C. (6th ser.) (Dec. 14, 1999) 163.

172. *See generally* Suppression of Terrorism Act, 1978, c. 26 (U.K.).

173. H.C. STANDING COMMITTEE D DEB., TERRORISM BILL (6th ser.) (Feb. 1, 2000) 262 (statement of Minister of State Charles Clarke).

174. *See* JUSTICE, RESPONSE TO *LEGISLATION AGAINST TERRORISM* paras. 3.6, 3.7 (1999).

175. SECRETARY OF STATE FOR THE HOME DEPARTMENT & SECRETARY OF STATE FOR NORTHERN IRELAND, LEGISLATION AGAINST TERRORISM 16 (Cm. 4178, Stationery Office, 1998). Exactly these forms of activities are to be forbidden by clause 1(1) of the Terrorism Bill, 2005-06, H.L. Bill [56]: "This section applies to a statement that is likely to be understood by members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences." *See also* JOINT COMMITTEE ON HUMAN RIGHTS, COUNTER TERRORISM POLICY AND HUMAN RIGHTS, 2005-06, H.L. 75-I/H.C. 561.

176. European Convention on Human Rights and Fundamental Freedoms, art. 10, Nov. 4, 1950, ETS 5, 213 U.N.T.S. 17.

177. *See* Incal v. Turkey, App. No. 22678/93, Reports 1998-IV (2000); Castells v. Spain, App. No. 11798/85, Ser. A 236 (1992).

It is commonly claimed that the use of cyberspace for propaganda purposes is its most significant terrorist use, but the notion of "propaganda" is wider than the forms of incitement in the Terrorism Act.[178] So, if, for example, PKK efforts are diverted into humanitarian protests about the torture and summary execution of Öcalan by the Turkish government, is that still terrorism? Even the occupation of an embassy is not usually considered to be terrorism. The idea that "once a terrorist, always a terrorist" is belied by history, including the life stories of at least one Prime Minister of Israel (Begin), one President of Cyprus (Makarios) and one President of South Africa (Mandela), assuming open attacks against colonial and racist regimes would be counted as "terrorism" in the first place.[179]

In reality, few terrorist groups have been able to run websites without attacks in turn from government agencies putting pressure on ISPs or triggering other forms of counteraction. For example, the Sinn Féin site, originally at the University of Texas, moved after protests in May 1996.[180] Sites favouring ETA have been closed down in this way, as described earlier.[181] No proscribed Irish group has any website anywhere in the world, though a few of the foreign proscribed groups do have a direct web presence.[182] Of course, it is not necessarily the case that the law enforcement world would want these websites to be shut down—electronic intelligence-gathering works both ways. Indeed, communications, whether internal or external, can of course provide evidence of conspiracy and have indeed been used as evidence in court proceedings involving Al Qa'ida suspects.[183] One should not assume that encryption is always effectively used by terrorists.

Other offences likely to involve the Internet are more justifiable as

178. Silke, *supra* note 10, at 7, 18.

179. *See* Diplomatic Conference on Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict: Protocols I and II to the Geneva Conventions art. 49, June 8, 1977, 16 I.L.M. 1391.

180. The site (http://uts.cc.utexas.edu/~sponge/aprn/SFhome.html) moved to a commercial internet service provider located in Philadelphia. *See* Sinn Féin Online, http://www.serve.com/rm/sinnfein/index.html (last visited Jan. 14, 2006). The site is now on an Irish internet service provider. *See* Sinn Féin: Building an Ireland of Equals, http://sinnfein.ie/ (last visited Jan. 14, 2006). *See* Stuart Tendler, *Ulster Security Details Posted on the Internet*, TIMES (London), Mar. 25, 1996.

181. *See supra* notes 46-47 and accompanying text.

182. *See, e.g.* Harkat-ul-Mujahideen: Latest News & Articles on Jihad & Kashmir, http://www.harkatulmujahideen.org (last visited Jan. 14, 2006); Markazdawa.org, http://www.markazdawa.org/ (last visited Jan. 14, 2006); Tamil Eelam Home Page, http://eelam.com (last visited Jan. 14, 2006); Partiya Karkerên Kurdistan Worker's Party, http://www.pkk.org (last visited Jan. 14, 2006). Other recently defunct websites include http://www.hizballah.org/ and http://www.ozgurluk.org/dhkc/.

183. *See* Al Fawwaz v. Governor of Brixton Prison, [2001] UKHL 69 (involving evidence from a facsimile).

closer to the concept of violence than politics. These include section 54, which deals with weapons training.[184] Under this section, a person commits an offence if he "provides instruction or training in the making or use of—(a) firearms, (aa) radioactive material or weapons designed or adapted for the discharge of any radioactive material, (b) explosives, or (c) chemical, biological or nuclear weapons."[185] This offence has its origins in successive Northern Ireland (Emergency Provisions) Acts (latterly section 34 of the 1996 version),[186] but it has now been extended throughout the United Kingdom, despite the recommendation otherwise by Lord Lloyd.[187] It is correspondingly an offence under section 54(2) to receive instruction or training, or, under section 54(3), to invite another to receive instruction or training contrary to sub-sections (1) or (2) even if the activity is to take place outside the United Kingdom.[188] In this way, the offence currently also pertains to recruitment for training as well as to the training itself. These changes arose mainly from concerns about groups seeking to recruit British Muslims, often through the Internet, for military training in madrassas (Islamic religious schools) in Afghanistan, Pakistan and elsewhere. By way of interpretation, under section 54(4), "instructions" and "invitations" can be general, such as by a pamphlet or via the Internet, or "addressed to one or more specific persons."[189] In this way, no identifiable recipient is needed for the offence to be committed.

Sulayman Balal Zainulabidin, a chef from Greenwich, south-east London,was charged under section 54 in October 2001 arising from his activities in running an enterprise called Sakina Security Services, which has advertised on the web training for Muslim recruits to prepare for "The Ultimate Jihad Challenge" (some of which was to occur at a facility called Ground Zero in Marion, Alabama).[190] He was acquitted of all charges in August 2002; there was no evidence to link him to al Qa'ida and, over a period of two years, only one person had even applied for the

184. Terrorism Act, 2000, c. 11, § 54 (U.K.). Any form of training relevant to terrorism, whether related to weapons or not, will be penalised by the offence in clause 6 of the Terrorism Bill, 2005-06, H.L. Bill [56]. Attendance at a place of terrorist training is an offence under clause 8. *See also* JOINT COMMITTEE ON HUMAN RIGHTS, COUNTER TERRORISM POLICY AND HUMAN RIGHTS, 2005-06, H.L. 75-I/H.C. 561.

185. *Id.*

186. *See* Northern Ireland (Emergency Provisions) Act, 1991, c. 24 (U.K.); Northern Ireland (Emergency Provisions) Act, 1996, c. 22, § 36 (U.K.).

187. INQUIRY INTO LEGISLATION AGAINST TERRORISM 14.28 (Cm. 3420, Stationery Office, 1996).

188. Terrorism Act, 2000, c. 11, § 54 (U.K.).

189. *Id.*

190. A mirror of the website is produced at http://www.warbirdforum.com/webarchi.htm (last visited Jan. 25, 2006).

course via the website.[191]

Just as the offence of weapons training has been extended to cover chemical, biological and nuclear weapons and materials, so sections 113 to 115 of the Anti-terrorism, Crime and Security Act 2001 extend offences relating to uses of weapons and threats and hoaxes concerning them from traditional areas, such as firearms and explosives, to chemical, biological and nuclear weapons and materials.[192] By section 113(1), it becomes an offence for a person to use or threaten to use a noxious substance or thing to cause serious harm in a manner designed to influence the government or to intimidate the public.[193] The serious harm is defined further by sub-section (2) as an action that:

> (a) causes serious violence against a person anywhere in the world;
>
> (b) causes serious damage to real or personal property anywhere in the world;
>
> (c) endangers human life or creates a serious risk to the health or safety of the public or a section of the public; or
>
> (d) induces in members of the public the fear that the action is likely to endanger their lives or create a serious risk to their health or safety; but any effect on the person taking the action is to be disregarded.[194]

The list overall is reflective of section 1(2) of the Terrorism Act,[195] save that there is understandably no reference to electronic systems. By section 113(3), it is an offence to make a threat to carry out an action which constitutes an offence under subsection (1) with the intention "to induce in a person anywhere in the world the fear that the threat is likely to be carried out."[196]

Section 114 deals with hoaxes with reference to "a noxious substance or other noxious thing."[197] The law as it stood before the 2001 Act, in section 51 of the Criminal Law Act 1977 (as amended by the Criminal Justice Act 1991), made it an offence for someone to place or send any article intending to make another person believe that it is likely to explode or ignite and thereby cause personal injury or damage to

191. Tania Branigan, Cleared Chef Says He was Terror Case Scapegoat: Jury Dismisses First UK Charges Since Attacks on September 11, THE GUARDIAN, Aug. 10, 2002, at 6.

192. Anti-terrorism, Crime, and Security Act, 2001, c. 24, §§ 113-115 (U.K.).

193. *Id.* § 113(1).

194. *Id.* § 113(2).

195. Terrorism Act, 2000, c. 11, § 1(2) (U.K.).

196. Anti-terrorism, Crime, and Security Act, 2001, c. 24, § 113(3) (U.K.).

197. *Id.* § 114.

property.[198] It was also an offence under section 51 for someone to communicate any information which he knows or believes to be false intending to make another person believe that a bomb is likely to explode or ignite.[199] There were corresponding offences in Scotland[200] and in Northern Ireland.[201] A related offence is food contamination contrary to section 38 of the Public Order Act 1986.[202] It is an offence under subsection (1) to intend to cause alarm, injury or loss by contamination or interference with goods or by making it appear that goods have been contaminated or interfered with "in a place where goods of that description are consumed, used, sold or otherwise supplied."[203] It is also an offence to make threats or claims along these lines[204] (section 38(2)) or to possess materials with a view to the commission of an offence (section 38(3)).[205] Section 38 responded to a small number of well-publicised incidents of consumer terrorism, a minority of which involved animal liberationists. It follows that there was a substantial range of offences in existence before 2001, but it was felt that there remained gaps. The offences in section 51 related only to hoax devices which are "likely to explode or ignite."[206] The section 38 offences protected only the integrity of goods.[207] Post-September 11, 2001, a scare arose from the mailing of anthrax powder in the U.S. and the fear that groups like Al Qa'ida had possession of other biological or nuclear materials which could be extremely dangerous and harmful not just in the consumer chain but through any form of contact or distribution.[208] Accordingly, section 114(1) widens the offence by extending the *actus reus* to placing or sending any substance or article intending to make others believe that it is likely to be or contain a noxious substance or thing which could endanger human life or health.[209] By subsection (2), it is an offence for a person to falsely communicate any information to another person

198. *See* WALKER, PREVENTION, *supra* note 34, at ch. 12.

199. Criminal Law Act, 1977, c. 45, § 51 (U.K.)., *amended by* Criminal Justice Act, 1991, c. 53 (U.K.).

200. *Id.* § 63 (U.K.).

201. Criminal Law (Amendment) (Northern Ireland) Order, 1977, SI 1977/1249, art. 3.

202. Public Order Act, 1986, c. 64, § 38 (U.K.). *See also* S. Watson, *Consumer Terrorism*, 137 NEW L. J. 84 (1987); S. Watson, *Product Contamination,* 84 L. SOCIETY'S GAZETTE 13 (1987).

203. Public Order Act, 1986, c. 64, § 38(1) (U.K.).

204. *Id.* § 38(2).

205. *Id.* § 38(3).

206. Criminal Law Act, 1977, c. 45, § 51 (U.K.), *amended by* Criminal Justice Act, 1991, c. 53 (U.K.).

207. Public Order Act, 1986, c. 64, § 38 (U.K.).

208. *See* Clive Walker, *Biological Attack, Terrorism and the Law*, 17 J. OF TERRORISM AND POL. VIOLENCE 175 (2004).

209. Anti-terrorism, Crime, and Security Act, 2001, c. 24, § 114(1) (U.K.).

anywhere in the world that a noxious substance or thing is or will be in a place and so is likely to cause harm or to endanger human life or health.[210]

For the purposes of both sections 113 and 114, section 115 makes clear that for a person to be guilty of an offence, it is not necessary for him to have any particular person in mind as the person in whom he intends to induce the belief in question.[211] Thus, threats and hoaxes issued to the whole world, such as via the Internet, can be penalised.

IV. Conclusion

Cyber-terrorism is a potential threat, and the United Kingdom state is justified in seeking to guard against it. As part of its commitment to that objective, it has set up the National Technical Assistance Centre, a surveillance advice and interception facility in the Security Services London headquarters.[212]

In the realm of asymmetric warfare, the processor can be mightier than the sword in the hands of terrorist groups. It follows that a flexible "digital realist" response[213] is appropriate. This approach may be rather more subtle than the mantra of Lawrence Lessig that "code is law,"[214] in that it recognizes that code (Internet technical architecture) is subject to law and that code is as malleable as is law. A digital realist approach to cyber-terrorism would consider all applicable modalities of control—law and architecture as well as social factors.

First, in terms of law, the foregoing survey suggests that there are few gaps and that the difficulties of prosecution are often evidential rather than substantive. The wish to maintain the secrecy of sources and surveillance techniques are prominent amongst these, as well as the problems inevitably caused by having to deal with terrorist networks which spill into many jurisdictions, some either unsophisticated or uncooperative, and whose languages are foreign. Subject to that reservation, one possible strengthening of criminal law might comprise a

---

210. *Id.* § 114(2).

211. *Id.* § 115.

212. Home Office, National Technical Assistance Centre, http://www.homeoffice.gov.uk/about-us/organisation/directorates-units/ crcsg/ntac.html?version=1 (last visited Nov. 29, 2005). For a statement of U.S. policy, *see* The White House, *The National Strategy to Secure Cyberspace* (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf [hereinafter *National Strategy*]. For further discussion of the strengthening of technological resilience, *see* WALKER, CIVIL CONTINGENCIES, *supra* note 4, at ch. 4.

213. *See* G. Greenleaf, *An Endnote on Regulating Cyberspace,* 21 U. NEW S. WALES L.J. 593 (2003).

214. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books, New York, 1999).

new specific offence of denial of service, as suggested by the All Parliamentary Internet Group.[215] Most Denial of Service attacks already fall within the Computer Misuse Act 1990[216] offences, but a specific new offence of rendering data "inaccessible" would send a useful signal as well as avoiding technicalities about the exact mechanism used.[217] Aspects of civil law may also be relevant as a discipline against those who seek to profit from, or simply enjoy, the theatre of terrorism. One might for example, provide for special funds for the victims of terrorism and their families so they can bring actions in tort[218] against those who reproduce executions and other distressing episodes of terrorism.

Second, Internet architecture points towards the ability to warn and to filter, techniques which have proven so successful against other unwanted cyber-intrusions such as spam.[219] Finally, social action would involve the education of the general public as to this aspect of terrorism. The vigilance of the British public has been a key factor in dealing with IRA bombings. The same could apply to attacks via the Internet. Possible outcomes might be the more effective use of filters, warnings and reporting systems akin to those relating to child pornography (focused on the Internet Watch Foundation),[220] and even the formation of counter sites. The Internet Watch Foundation model also reminds us that the world of cyberspace, most of which rests in private hands, requires the encouragement of networks of security. This point is explicit in the U.S. government's National Strategy to Secure Cyberspace, which states that "[t]he cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."[221]

---

215. *See* All Party Parliamentary Internet Group, *"Revision of the Computer Misuse Act": Report of an Inquiry by the All Party Internet Group, available at* http://www.apig.org.uk/archive/activities-2004/computer-misuse-inquiry/CMAReport FinalVersion1.pdf (last visited Nov. 29, 2005) [hereinafter *Computer Misuse Inquiry*]. The subsequent Computer Misuse Act 1990 (Amendment) Bill, 2004-05, H.C. Bill [102], sponsored by the chair of the All Party Parliamentary Internet Group (APIG), fell when Parliament was prorogued in April 2005. In the U.S., changes after 9/11 included the Cyber Security Enhancement Act of 2002, 6 U.S.C.A. § 145 (2004), which primarily increases penalties for computer related offences, and the Cyber Security Research and Development Act of 2002, 15 U.S.C. A. § 7401 (2004), which provides for funding for research. *See also* T.M. Raghawan, *In Fear Of Cyberterrorism: An Analysis of the Congressional Response*, 2003 U. ILL. J.L. TECH. & POL'Y 297 (2003).

216. Computer Misuse Act, 1990, c. 18 (U.K.).

217. *Computer Misuse Inquiry, supra* note 215, at paras. 66, 74.

218. *See* Wainwright v. Home Office, [2003] UKHL 53; Wilkinson v. Downton, [1897] 2 Q.B. 57.

219. *See* D. S. Wall, *Digital Realism and the Governance of Spam As Cybercrime*, 10 EUR. J. CRIM. POL'Y & RES. 309 (2005).

220. Internet Watch Foundation Home Page, http://www.iwf.org.uk (last visited Nov. 29, 2005).

221. *National Strategy, supra* note 212, at iv.

Nevertheless, any or all of these levels of response ought to be circumspect for two reasons. First, the most effective measures against any form of terrorism are, on the one hand, intelligence-gathering and surveillance and, on the other hand, security counter-measures. Sweeping legislation has the distinct disadvantages not only of being unproductive but also of giving a signal of undue alarm and potentially criminalising the political rather than the violent. We must avoid the panicked conclusion that society's reliance on technology creates an unalloyed fragility. Instead, we must see it as a strength which often contains the facility for its own protection.

Next, the urge to restrict, prohibit and to curtail must be resisted. Aside from the need to encourage dialogue with those so disaffected that they resort to political violence, websites can be a vital open intelligence source for the authorities, especially because propaganda is one of the main aspects of cyber-terrorism. Furthermore, closed sources derived from information and communication sources are also vital. The ESCHELON[222] system is alleged to be able to "sniff" key switch points on the Internet and, in that way, intercept a huge amount of traffic. Given the absence of informants in most cases involving Al Qa'ida and other tight-knit Jihadist groups, it may be deduced that a fair proportion of the successes of the authorities in thwarting attacks and undertaking prosecutions may have been assisted by background signals intelligence. The pursuit of intelligence may be assisted by the fact that the terrorists are not as sophisticated as sometimes presented. For example, even Moussaoui did not use the encryption facilities which are offered by the popular e-mail services.[223] Another revealing case is that of Mohammed Naeem Noor Khan, whose seized computer materials are reported to have led to a number of further arrests.[224] His laptop was described as a "treasure trove" for Western intelligence agencies.[225] Moreover, cell

222. *See* Cyber-Rights and Cyber-Liberties Home Page, http://www.cyber-rights.org/interception/echelon/ (last visited Nov. 29, 2005; American Civil Liberties Union, *Echelon Watch, available at* http://www.echelonwatch.org/; 2001/2098(INI)) FINAL, A5-0264/2001 Parl.

223. *See supra* notes 52-54 and the accompanying text.

217. Zahid Hussein et al., *Al-Qaeda's "British Chief" Is Seized in Police Raids,* THE TIMES (London), Aug. 5, 2004, at 1.

225. Michael Evans, *Al-Qaeda Agent's Laptop Yields Vital Intelligence Clues,* THE TIMES (London), Aug. 7, 2004, at 4. Charges were brought against eight individuals: Dhiren Barot, for possessing reconnaissance plans of the U.S. financial buildings and having notebooks with information on explosives, poisons, chemicals and related matters; Qaisar Shaffi, for owning an extract from a terrorist's handbook, which explains the use of chemicals and explosive devices; Mohammed Naveed Bhatti; Abdul Aziz Jalil; Omar Abdul Rehman; Junade Feroze; Zia ul Haq; and Nadeem Tarmohammed. Stewart Tendler et al., *Gang Charged with Plot to Hit U.K. with "Dirty Bomb,"* THE TIMES (London), Aug. 18, 2004, at 1.

phones have been used to track terrorists and to provide evidence against them.[226]

Closing off modes of communication which in some eyes might amount to "propaganda" must always give liberal democracies pause for thought. One might especially recall the furious reaction to the broadcasting of "Death on the Rock" about the Gibraltar shootings in 1988. Even before this time, Prime Minister Margaret Thatcher coined a key phrase in the summer of 1985 after the TWA airline hijack in Beirut. She told the American Bar Association in London, "We try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend."[227] Outright censorship was explicitly imposed only in November 1988 under broadcast licensing powers.[228] The Home Secretary, Douglas Hurd, based his actions on concern for victims, as well as on more general political concerns about the creation of fear and intimidation.[229] The ban included proscribed organizations as well as Sinn Féin, Republican Sinn Féin, and the Ulster Defence Association. The ban was upheld as lawful in *R v. Secretary of State for the Home Department, ex parte Brind.*[230] Likewise, the European Commission of

226. *See* E. Philips, *Mobile Phone—Friend or Foe?,* 42 SCI. & JUST. 225 (2002). However, the conviction of Colm Murphy for aiding those who bombed Omagh in August 1998 by providing mobile phones has been overturned on evidence that police interview notes had been falsified. David Lister, *Omagh Bomb Retrial after Police "Faked Evidence,"* THE TIMES (London), Jan. 22, 2005, at 20.

227. Peter Evans, *Thatcher Unfolds Strateg to Beat Hijack Terror/ British Premier Addresses American Bar Association Meeting in London,* THE TIMES (London), July 16, 1985.

228. *See* L. HENDERSON ET AL., SPEAK NO EVIL: THE BRITISH BROADCASTING BAN, THE MEDIA AND THE CONFLICT IN IRELAND (Glasgow University Media Group, London, 1990); D. MILLER, DON'T MENTION THE WAR (Pluto, London, 1994); LORD WINDLESHAM AND R. RAMPTON, THE WINDLESHAM/RAMPTON REPORT ON DEATH ON THE ROCK (Faber & Faber, London, 1989); C. Banwell, *The Courts' Treatment of the Broadcasting Bans in Britain and the Republic of Ireland,* 16 J. MEDIA L. & PRAC. 21 (1995); M. Halliwell, *Judicial Review and Broadcasting Freedom,* 42 N.I.L.Q. 246 (1991); J. Jowell, *Broadcasting and Terrorism, Human Rights and Proportionality,* PUB. L. 149 (1990); J. Michael, *Attacking the Easy Platform,* 138 N.L.J. 786 (1988); D.G. Morgan, *Section 31: The Broadcasting Ban* (1990-92), 25-27 IRISH JURIST 117 (1990-92); N. J. Parpworth, *Terrorism and Broadcasting,* 15 J. MEDIA L. & PRAC. 50 (1994); B. Thompson, *Broadcasting and Terrorism,* PUB. L. 527 (1989); R. L. Weaver and G. Bennett, *Banning Broadcasting—A Transatlantic Perspective,* 13 J. MEDIA L. & PRAC. 179 (1992); R. L. Weaver and G. Bennett, *The Northern Ireland Broadcasting Ban: Some Reflections on Judicial Review,* 22 VAND. J. TRANSNAT'L L. 1119 (1989). The ban was lifted on September 16, 1994 shortly after the IRA had called a ceasefire.

229. *See* 139 PARL. DEB., H.C. (6th ser.) (1988) 1082.

230. [1991] 1 A.C. 696. *See In re* McLaughlin's Application, 1 B.N.I.L. n. 36 [1991], 6 N.I.J.B 4 (1990); R v. BBC ex p. McAliskey, Q.B. (Crown Office List), CO/3032/92 (May 27, 1994); Commentaries, Pub. L. 527 (1989); Pub. L. 149 (1990); N.I.L.Q. 246 (1990).

Human Rights upheld limited broadcasting bans.[231] One wonders whether the ban was helpful in preparing the public, especially the Unionist/Loyalist population of Northern Ireland, for the idea of accommodation and consocialism, which became the hallmark of the Belfast "Good Friday" Agreement of 1998.

Of course, some would argue that Millian concepts of harm are inadequate. There is sympathy for this view in the Canadian *Keegstra* judgment:

> [W]ords and writings that wilfully promote hatred can constitute a serious attack on persons belonging to a racial or religious group. . . .
>
> [A] response of humiliation and degradation from an individual targeted by hate propaganda is to be expected. A person's sense of human dignity and belonging to the community at large is closely linked to the concern and respect accorded the groups to which he or she belongs. . . . The derision, hostility and abuse encouraged by hate propaganda therefore have a severely negative impact on the individual's sense of self-worth and acceptance.[232]

Ideally, another reaction altogether is to be encouraged. In the words of Supreme Court Justice Brandeis, "[the] remedy to be applied is more speech, not enforced silence."[233] Especially since the Internet facilitates easy, free and instantaneous public discourse, self-assertion is available to all. The need for cultural education and promotion regarding the Islamic communities is suggested by the European Monitoring Centre on Racism and Xenophobia's[234] study of Islamophobia in the European Union after 9/11 and also by the House of Commons Home Affairs Committee.[235] In particular, rather than the sole pursuit of a policy of repression, "the Government must engage British Muslims in its anti-terrorist strategy."[236] That engagement should take place in cyberspace, since it has become one of the front lines in the fight against terrorism.

---

231. Purcell v. Ireland, App. No. 15404/89, D.R., 70, 262 (1991); Brind v. UK, App. No. 18714/91, D.R., 77-A, 42 (1994); McLaughlin v. UK, App. No. 18759/91, 18 Eur. H.R. Rep. CD84 (1994).

232. R. v. Keegstra, [1990] S.C.R 697, 746 (opinion by Dickson, C.J.).

233. Whitney v. California, 274 U.S. 357, 377 (1927).

234. The EUMC was set up in 1997 by Council Regulation (EC) No. 1035/97. There are proposals to reconstitute it as the Fundamental Rights Agency of the European Union (COM(2004)693 Final).

235. TERRORISM AND COMMUNITY RELATIONS, 2004-05, H.C. 165.

236. *Id.* at para. 225.

***