TERRORISM & NEW MEDIA: THE CYBER BATTLE SPACE

Maura Conway

Introduction

This chapter has very little to contribute about so-called 'cyberterrorism' (i.e. acts of terrorism carried out using the Internet and/or against Internet infrastructures);[1] instead, it is centrally concerned with what Resnick describes as 'Political uses of the Net': the employment of the Internet by ordinary citizens, political activists, organised interests, governments and others to achieve political goals which has little or nothing to do with the Internet *per se*.[2] Specifically, the focus here is on the use(s) made of the Internet by terrorist groups. What are terrorist groups attempting to do by gaining a foothold in cyberspace? A small number of researchers have addressed this question in the past five years.[3] Probably the best known of these analyses is Gabriel Weimann's report for the US Institute of Peace entitled *www.terrorism.net: How Modern Terrorism Uses the Internet*.[4] Weimann identifies eight major ways in which, he says, terrorists currently use the Internet. These are psychological warfare,

[1] For more on cyberterrorism, see Maura Conway, "Cyberterrorism: Hype and Reality." In *Information Warfare: Hype and Reality*, edited by Leigh Armistead (Virginia: Potomac Books, 2006); Maura Conway, "What is Cyberterrorism? The Story so Far," *Journal of Information Warfare* 2 (2003); Maura Conway, "Cyberterrorism," *Current History* 101 (2002).
2 David Resnick. "Politics on the Internet: The Normalization of Cyberspace." In *The Politics of Cyberspace*, edited by Chris Toulouse and Timothy W. Luke. London: Routledge, 1999, pp. 55–56.
[3] See Fred Cohen, "Terrorism and Cyberspace," *Network Security* 5 (2002); Stephen Furnell and Matthew Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers and Security* 18 (1999); Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters* Spring (2003), available online at http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm
[4] Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet* (Washington DC: United States Institute of Peace, 2004). Full text available online at http://www.usip.org/pubs/specialreports/sr116.pdf.

publicity and propaganda, data mining, fund raising, recruitment and mobilization, networking, information sharing and planning and coordination.[5] Having considered Weimann's categorisation in conjunction with those suggested by Cohen, Furnell and Warren, and Thomas,[6] the present analysis is concerned with what have been determined to be the current five core terrorist uses of the Net: information provision, recruitment, financing, networking and information gathering. Each of these is described and analysed in more detail below. The available responses to this increased terrorist reliance on the Internet are also considered in some detail in the second half of this chapter. Initially, however, a brief explanation as to why the Internet is viewed by terrorists as such an attractive tool is in order.

Why the Internet?

Thomas Friedman has argued that contemporary globalization "goes farther, faster, cheaper, and deeper."[7] He might have been describing the Internet.

The Internet is a powerful tool, which is used and manipulated by actors to accomplish a wide variety of tasks. The networked nature of the Internet allows users to access a nearly limitless supply of information and data that can be shared across the network. People can use the Internet to educate themselves, to entertain themselves, to conduct business, to shop, or to engage in political action. There is no *a priori* reason, however, why actors should use the Internet to engage in these activities over any other potential tool that will garner the same result. As with any tool, the Internet does not exist in a vacuum; rather, actors are presented with different

[5] Gabriel Weimann, pp.5-11.

[6] For additional discussion see Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security* 18 (2006).

[7] As quoted in Joseph Nye, *The Paradox of American Power* (Oxford: Oxford University Press, 2002), p.85; see also Joseph Nye *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), p. 31.

options and make choices based on relative advantages. If actors are to use the Internet, it must offer relative advantages over other potential tools. If no such comparative benefit exists, actors will see no utility in using the Internet, opting instead for some other, more effective, option.

There are nine key properties of the Internet that render it different from traditional media and a key instrumental power source:

- Volume: far larger volumes of information can be transferred easily compared with previous modes of communication.
- Speed: the ability to compress data and more space for transmitting data decrease the amount of time it takes to exchange information.
- Format: the ability to combine text, graphics, audio, and video means that in-depth, dynamic, and visually stimulating communication is possible simultaneously.
- Direction: the possibilities for two-way interactive communication are greatly expanded on the WWW as a result of the greater space and speed, but also due to the enhanced horizontal or lateral links arising out of hypertext linkage between sites.
- Individual Control: the opening up of control over direction in the sending and receiving of information means that power is decentralized to the individual user who has the choice of not only what to view, but also what to publish.
- Anonymity: Internet users enjoy a large measure of anonymity. There are numerous information security applications that allow customers to conceal their identity, the content of their communications, or the details of their

transactions. These include free e-mail services, electronic remailers, anonymizers, and widely available encryption and steganographic tools.

- Evasion of Government Control: the primary way in which actors may evade government control is through operating their Web site(s) in jurisdictions with high levels of free speech protection. The various tools identified above may also be used to avoid censorship.
- Reduced Transaction Costs: registering a Web site costs less than US$50 and many Internet sites allow users to create Web sites at no cost at all. Free e-mail services are commonplace on the Internet while newsgroups and message postings are likewise available at no cost.
- Globality: perhaps most importantly, these low-cost Internet technologies allow users to transmit and share information globally nearly instantaneously. The networked structure of the Internet finds the quickest and most effective route for information flows. Web sites from anywhere in the world take only seconds to load while e-mails can circle the globe in an instant.

In summary, then, Web-based communication has the potential to be a more immediate, individual, dynamic, in-depth, interactive, anonymous, unedited, cheaper, and far-reaching process than is possible in conventional media. Terrorists are well aware of these properties of the Internet and this explains why they have taken to the medium with such alacrity.

The Five Core Terrorist Uses of the Internet

Information Provision

This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. “In the modern era, the truism that ‘information is power’ is very clearly understood by the media and governments; it is also understood by terrorists, their audiences, and their adversaries.”[8] The Internet, and the advent of the World Wide Web in particular, have significantly increased the opportunities for terrorists to secure publicity. This can take the form of historical information, profiles of leaders, manifestos, etc. But terrorists can also use the Internet as a tool of psychological warfare through spreading disinformation, delivering threats, and disseminating horrific images, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist Daniel Pearl in Pakistan via their Web sites.[9] These functions are clearly improved by the Web’s enhanced volume, increased speed of data transmission, low-cost, relatively uncontrolled nature, and global reach.

In the past, those characterised as ‘terrorists’ were rarely accepted by the mass media as legitimate or authoritative sources of news in their own right. Neither were they accepted as reliable commentators upon the political situation that had given rise to the violence: “Certainly, on the few occasions when the BBC or ITV interviewed Republican para-militaries in the 1970s and 1980s, they were emphatically not, as a matter of policy, treated as individuals whose opinions could be accorded the same respect and due consideration as others.”[10] By concentrating almost exclusively on the violent dimension of terrorism, making no attempt to contextualise its causes, media reports often leave readers, viewers, or listeners mystified as to the motivation of violent acts.[11] The upshot of this is that many in the media audience take these acts to

[8] Gus Martin, *Understanding Terrorism: Challenges, Perspectives, and Issues* (Thousand Oaks, CA: Sage, 2003), p.279.
[9] Gabriel Weimann, p.5.
[10] Susan L. Carruthers, *The Media at War* (Hampshire: Palgrave, 2000), p.191.
[11] Gus Martin, p.280.

be simply the senseless, inexplicable behaviour of psychotic fundamentalists or extremist lunatics.[12]

The establishment of dedicated Websites, on the other hand, offers terrorist groups an unprecedented level of direct control over the content of their message(s). It considerably extends their ability to shape how different target audiences perceive them and to manipulate not only their own image, but also the image of their enemies. Although, for many groups, their target audience may be small, an Internet presence is nonetheless expected. Regardless of the number of hits a site receives, a well-designed and well-maintained Web site gives a group an aura of legitimacy while also seeking to advance the organization's political and ideological agenda. The latter is a core function in and of itself, but clearly the sites' information provision role also evidences significant overlaps with the other terrorist uses of the Net outlined below, particularly recruitment.

Recruitment

This refers to groups' efforts to recruit and mobilize sympathizers to more actively support terrorist causes or activities. The Web offers a number of ways for achieving this: it makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format; the global reach of the Web allows groups to publicize events to more people; and by increasing the possibilities for interactive communication, new opportunities for assisting groups are offered, along with more chances for contacting the group directly. Finally, through the use of discussion forums, it is also possible for members of the public--whether supporters or detractors of a group--to engage in debate with one another. This may assist the

[12] George Gerbner, "Violence and Terrorism in and By the Media." In *Media, Crisis and Democracy: Mass Communication and the Disruption of Social Order*, edited by Mark Raboy & Bernard Dagenais (London: Sage, 1992), p.96.

terrorist group in adjusting their position and tactics and, potentially, increasing their levels of support and general appeal.[13]

Online recruitment by terrorist organizations is said to be widespread. Harris *et al* provide the example of an Iranian site that boasts an application for suicide bombers guaranteeing that the new 'martyr' will take seventy relatives with him into heaven. If the recruit is unsure about joining, or if the group is unsure about the recruit, he is directed to a chat room where he is 'virtually' vetted. If he passes muster, he will be directed to another chat room for further vetting, and finally contacted personally by a group member. This process is said to be aimed at weeding out 'undesirables' and potential infiltrators.[14] It is more typical, however, for terrorist groups to actively solicit for recruits rather than waiting for them to simply present themselves. Weimann suggests that terrorist recruiters may use interactive Internet technology to roam online chat rooms looking for receptive members of the public, particularly young people. Electronic bulletin boards could also serve as vehicles for reaching out to potential recruits.[15]

Financing

This refers to efforts by terrorist groups to raise funds for their activities. Money is terrorism's lifeline; it is "the engine of the armed struggle."[16] The immediacy and interactive nature of Internet communication, combined with its high-reach properties, opens up a huge potential for increased financial donations as has been demonstrated

[13] Rachel Gibson and Stephen Ward, "A Proposed Methodology for Studying the Function and Effectiveness of Party and Candidate Web Sites," *Social Science Computer Review* 18 (2000): 305-306; Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival* 39 (1997): 140; Weimann, p.8.

[14] Kathryn Fritz, Lindsay Harris, Daniel Kolb, Paula Larich, & Kathleen Stocker, *Terrorist Use of the Internet and National Response* [Unpublished Paper] (College Park: University of Maryland, 2004), p.9. Full text available online at http://www.wam.umd.edu/~larich/735/index.html.

[15] Weimann, p.8.

[16] Loretta Napoleoni, "Money and Terrorism," *Strategic Insights* 3 (2004): 1. Full text available online at http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf.

by a host of non-violent political organizations and civil society actors. Terrorists seek financing both via their Web sites and by using the Internet infrastructure to engage in resource mobilization using illegal means.

Numerous terrorist groups request funds directly from Web surfers who visit their sites. Such requests may take the form of general statements underlining the organizations need for money, more often than not however requests are more direct urging supporters to donate immediately and supplying either bank account details or an Internet payment option. For example, the IRA's main Web site contains a page on which visitors can make credit card donations.[17] While, at one time, the Ulster Loyalist Information Service, which was affiliated with the Loyalist Volunteer Force (LVF), and accepted funds via PayPal, invited those who were "uncomfortable with making monetary donations" to donate other items, including bullet-proof vests. Another way in which groups raise funds is through the establishment of online stores and the sale of items such as books, audio and video tapes, flags, t-shirts, etc.

The Internet facilitates terrorist financing in a number of other ways besides direct solicitation via terrorist Web sites. According to Jean-Francois Ricard, one of France's top anti-terrorism investigators, many Islamist terror plots are financed through credit card fraud.[18] Imam Samudra, sentenced to death for his part in the Bali bombing of 2002, has published a prison memoir of some 280 pages, which includes a paper that acts as a primer on 'carding.'[19] According to Dutch experts, there is strong evidence from international law enforcement agencies such as the FBI that at least some terrorist groups are financing their activities via advanced fee fraud, such as Nigerian-style scam e-mails. To date, however, solid evidence for such claims has not

[17] Weimann, p.7.

[18] Thomas, p.117.

[19] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," *Washington Post* 14 December 2004, A19. Full text available online at http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

entered the public realm.[20] There is ample evidence, however, to support the contention that terrorist-affiliated entities and individuals have established Internet-related front businesses as a means of raising money to support their activities. For example, in December 2002, InfoCom, a Texas-based ISP, was indicted along with its individual corporate officers on thirty-three counts relating to its provision of communication services, in-kind support, and funds to terrorist organizations including Hamas and its affiliate the Holy Land Foundation for Relief and Development (HLFRD). InfoCom's capital was donated primarily by Nadia Elashi Marzook, wife of Hamas figurehead Mousa Abu Marzook.[21]

Terrorist organizations have a history of exploiting not just businesses, but also charities as undercover fundraising vehicles. This is particularly popular with Islamist terrorist groups, because of the injunction that observant Muslims make regular charitable donations. In some cases, terrorist organizations have actually established charities with allegedly humanitarian purposes. Examples of such undertakings include Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation, and Help The Needy. Along with advertising in sympathetic communities' press, these 'charities' also advertised on websites and chat rooms with Islamic themes, pointing interested parties to their Internet homepages.

Terrorists have also infiltrated branches of existing charities to raise funds clandestinely. Many such organizations provide the humanitarian services advertised:

[20] Jan Libbenga, "Terrorists Grow Fat on E-Mail Scams," *The Register* 28 September 2004. Full text available online at http://www.theregister.co.uk/2004/09/28/terrorist_email_scams/.

[21] Todd Hinnen, "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet," *Columbia Science and Technology Law Review* 5 (2004): 18, online at http://www.stlr.org/html/volume5/hinnenintro.html; see also Steven Emerson's testimony before the House Committee on Financial Services, "Fund-Raising Methods and Procedures for International Terrorist Organizations," on 12 February 2002, pp.11-12 & 16, online at http://financialservices.house.gov/media/pdf/021202se.pdf.

feeding, clothing, and educating the poor and illiterate, and providing medical care for the sick. However, some such organizations, in addition to pursuing their publicly stated mission of providing humanitarian aid, also pursue a covert agenda of providing material support to militant groups. These organizations' Web-based publicity materials may or may not provide hints as to their secret purposes.

Networking

This refers to groups' efforts to flatten their organizational structures and act in a more decentralized manner through the use of the Internet, which allows dispersed actors to communicate quickly and coordinate effectively at low cost. The Internet allows not only for intra-group communication, but also inter-group connections. The Web enhances terrorists' capacities to transform their structures and build these links because of the alternative space it provides for communication and discussion and the hypertext nature of the Web, which allows for groups to link to their internal sub-groups and external organizations around the globe from their central Web site.

Transforming Organizational Structures

Rand's John Arquilla, David Ronfeldt, and Michele Zanini have been pointing to the emergence of new forms of terrorist organization attuned to the information age for some time. They contend, "terrorists will continue to move from hierarchical toward information-age network designs. More effort will go into building arrays of transnationally internetted groups than into building stand alone groups."[22] This type of organizational structure is qualitatively different from traditional hierarchical

[22] John Arquilla, David Ronfeldt & Michele Zanini, "Networks, Netwar and Information-Age Terrorism.' In *Countering the New Terrorism,* edited by Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini, and Brian Michael Jenkins (California: Rand, 1999), p.41. Full text available online at http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf.

designs. Terrorists are ever more likely to be organized to act in a more fully networked, decentralized, 'all-channel' manner. Ideally, there is no single, central leadership, command, or headquarters. Within the network as a whole there is little or no hierarchy and there may be multiple leaders depending upon the size of the group. In other words, there is no specific heart or head that can be targeted. To realize its potential, such a network must utilize the latest information and communications technologies. The Internet is becoming an integral component of such organizations, according to the Rand analysts.[23]

Planning and Coordination

"Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the Internet."[24] Several reasons have been put forward to explain why modern IT systems, especially the Internet, are so useful for terrorists in establishing and maintaining networks. As already discussed, new technologies enable quicker, cheaper, and more secure information flows. In addition, the integration of computing with communications has substantially increased the variety and complexity of the information that can be shared.[25]

This led Michele Zanini to hypothesize that "the greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decision making."[26] Zanini's hypothesis appears to be borne out by recent events. For example, many of the terrorists indicted by the United States

[23] Arquilla *et al*, pp.48-53.

[24] Pater Margulies, "The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment," *UCLA Journal of Law and Technology* 8 (2004): 2. Full text available online at http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf.

[25] Weimann, p.9.

[26] Michele Zanini, "Middle Eastern Terrorism and Netwar," *Studies in Conflict and Terrorism* 22 (1999), p.251.

government since 9/11 communicated via e-mail. The indictment of four members of the Armed Islamic Group (Gama'a al-Islamiyya) alleges that computers were used "to transmit, pass and disseminate messages, communications and information between and among IG leaders and members in the United States and elsewhere around the world."[27] Similarly, six individuals indicted in Oregon in 2002 allegedly communicated via e-mail regarding their efforts to travel to Afghanistan to aid al-Qaeda and the Taliban in their fight against the United States. [28]

The Internet has the ability to connect not only members of the same terrorist organizations but also members of different groups. For example, hundreds of so-called 'jihadist' sites exist that express support for terrorism. According to Weimann, these sites and related forums permit terrorists in places as far-flung as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions, but also practical information about how to build bombs, establish terror cells, and ultimately perpetrate attacks.[29]

Mitigation of Risk

As terrorist groups come under increasing pressure from law enforcement, they have been forced to evolve and become more decentralized. This is a structure to which the Internet is perfectly suited. The Net offers a way for like-minded people located in different communities to interact easily, which is particularly important when operatives may be isolated and having to 'lie low.' Denied a physical place to meet and organize, many terrorist groups are alleged to have created virtual communities through chat rooms and Web sites in order to continue spreading their propaganda,

[27] Indictment, United States v. Sattar, No. 02-CRIM-395, 11 (S.D.N.Y Apr. 9, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf.
[28] Indictment, United States v. Battle, No. CR 02-399 HA, 5 (D.Or. Oct. 2, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/usbattle100302ind.pdf.
[29] Weimann, p.9.

teaching, and training. Clearly, “information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility.”[30] It “puts distance between those planning the attack and their targets…[and] provides terrorists a place to plan without the risks normally associated with cell or satellite phones.”[31]

Information Gathering

This refers to the capacity of Internet users to access huge volumes of information, which was previously extremely difficult to retrieve as a result of its being stored in widely differing formats and locations. Today, there are literally hundreds of Internet tools that aid in information gathering; these include a range of search engines, millions of subject-specific email distribution lists, and an almost limitless selection of esoteric chat and discussion groups. One of the major uses of the Internet by terrorist organizations is thought to be information gathering. Unlike the other uses mentioned above terrorists’ information gathering activities rely not on the operation of their own Web sites, but on the information contributed by others to “the vast digital library” that is the Internet.[32] There are two major issues to be addressed here. The first may be termed ‘data mining’ and refers to terrorists using the Internet to collect and assemble information about specific targeting opportunities. The second issue is ‘information sharing,’ which refers to more general online information collection by terrorists.

Data Mining

[30] Patrick S. Tibbetts, *Terrorist Use of the Internet and Related Information Technologies* [Unpublished Paper] (Fort Leavenworth, Kansas: United States Army Command and General Staff College, 2002), p.5.

[31] Thomas, p.119.

[32] Weimann , p.6.

In January 2003, US Defence Secretary Donald Rumsfeld warned in a directive sent to military units that too much unclassified, but potentially harmful material was appearing on Department of Defence (DoD) Web sites. Rumsfeld reminded military personnel that an al-Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty percent of information about the enemy." He went on to say, "at more than 700 gigabytes, the DoD Web-based data makes a vast, readily available source of information on DoD plans, programs and activities. One must conclude our enemies access DoD Web sites on a regular basis."[33]

In addition to information provided by and about the armed forces, the free availability of information on the Internet about the location and operation of nuclear reactors and related facilities was of particular concern to public officials post 9/11. Roy Zimmerman, director of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response, said the 9/11 attacks highlighted the need to safeguard sensitive information. In the days immediately after the attacks, the NRC took their Web site entirely off line. When it was restored weeks later, it had been purged of more than 1,000 sensitive documents. Initially, the agency decided to withhold documents if "the release would provide clear and significant benefit to a terrorist in planning an attack." Later, the NRC tightened the restriction, opting to exclude information "that could be useful or could reasonably be useful to a terrorist."

[33] As quoted in Declan McCullagh, "Military Worried About Web Leaks," *C|Net News* 16 January 2003. Full text available online at http://news.com.com/2100-1023-981057.html.

According to Zimmerman, “it is currently unlikely that the information on our Web site would provide significant advantage to assist a terrorist.”[34]

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[35] since 9/11 thousands of documents and tremendous amounts of data have been removed from US government sites. The irony, however, is that much of the same information remains available on private sector Web sites.[36] Patrick Tibbetts points to the Animated Software Company's Web site which has off-topic documents containing locations, status, security procedures and other technical information concerning dozens of U.S. nuclear reactors,[37] while the Virtual Nuclear Tourist site contains similar information. The latter site is particularly detailed on specific security measures that may be implemented at various nuclear plants worldwide[38] (Tibbetts 2002, 15). Many people view such information as a potential gold mine for terrorists. Their fears appear well founded given the capture of al-Qaeda computer expert Muhammad Naeem Noor Khan in Pakistan in July 2004, which yielded a computer filled with photographs and floor diagrams of buildings in the U.S. that terrorists may have been planning to attack.[39]

Sharing Information

[34] As quoted in Mike M. Ahlers, “Blueprints for Terrorists?” *CNN.com* 19 November 2004. Full text available online at http://www.cnn.com/2004/US/10/19/terror.nrc/.

[35] OMB Watch is a watchdog group based in Washington DC. Their home page is online at http://www.ombwatch.org.

[36] Gary D. Bass and Sean Moulton, *The Bush Administration’s Secrecy Policy: A Call to Action to Protect Democratic Values* [Working Paper] (Washington DC: OMB Watch, 2002). Full text available online at http://www.ombwatch.org/rtk/secrecy.pdf.

[37] See http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm.

[38] See http://www.nucleartourist.com/.

[39] Douglas Jehl and David Johnston, “Reports That Led to Terror Alert Were Years Old, Officials Say,” *New York Times* 3 August 2004; Dan Verton and Lucas Mearian, “Online Data a Gold Mine for Terrorists,” *ComputerWorld* 6 August 2004. The full text of the latter is available online at http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html.

Policymakers, law enforcement agencies, and others are also concerned about the proliferation of ‘how to’ Web pages devoted to explaining, for example, the technical intricacies of making homemade bombs. Many such devices may be constructed using lethal combinations of otherwise innocuous materials; today, there are hundreds of freely available online manuals containing such information. As early as April 1997, the US Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts.[40]

As an example, Jessica Stern points to *Bacteriological Warfare: A Major Threat to North America* (1995), which is described on the Internet as a book for helping readers survive a biological weapons attack and is subtitled ‘What Your Family Can Do Before and After.’ However, it also describes the reproduction and growth of biological agents and includes a chapter entitled ‘Bacteria Likely To Be Used By the Terrorist.’ The text is available for download, in various edited and condensed formats, from a number of sites while hard copies of the book are available for purchase over the Internet from major online booksellers for as little as $13 (Stern 1999, 51).

More recently, an Al Qaeda laptop found in Afghanistan had been used to visit the Web site of the French Anonymous Society (FAS) on several occasions. The FAS site publishes a two-volume *Sabotage Handbook* that contains sections on planning an assassination and anti-surveillance methods amongst others.[41] A much larger manual, nicknamed *The Encyclopedia of Jihad* and prepared by al Qaeda, runs to thousands of

[40] US Department of Justice, *Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution* (Washington DC: US Department of Justice, 1997), pp.15-16. Full text available online at http://cryptome.org/abi.htm.

[41] Thomas, p.115; Weimann, p.9.

pages; distributed via the Web, it offers detailed instructions on how to establish an underground organization and execute terror attacks.[42]

This kind of information is sought out not just by sophisticated terrorist organizations but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas. In 1999, for instance, right-wing extremist David Copeland planted nail bombs in three different areas of London: multiracial Brixton, the largely Bangladeshi community of Brick Lane, and the gay quarter in Soho. Over the course of three weeks, he killed three people and injured 139. At his trial, he revealed that he had learned his deadly techniques from the Internet by downloading copies of *The Terrorist's Handbook* and *How to Make Bombs: Book Two.* Both titles are still easily accessible.[43]

The Open Source Threat?

The threat posed by the easy availability of bomb-making and other 'dangerous information' is a source of heated debate. Patrick Tibbetts warns against underestimating the feasibility of such threats. He points out that captured Al Qaeda materials include not only information compiled on 'home-grown explosives,' but also indicate that this group are actively pursuing data and technical expertise necessary to pursue CBRN weapons programs. According to Ken Katzman, a terrorism analyst for the Congressional Research Service, much of the material in these captured documents was probably downloaded from the Internet.[44] As a result, many have called for laws restricting the publication of bomb-making instructions on the Internet. Others, however, have pointed out that this material is already easily

[42] Weimann, p.9.
[43] Weimann, p.10.
[44] Tibbetts, p.17.

accessible in bookstores and libraries.[45] In fact, much of this information has been available in print media since at least the late 1960s, with the publication of William Powell's *The Anarchist Cookbook* and other, similar titles.

Jessica Stern has observed: "In 1982, the year of the first widely reported incident of tampering with pharmaceuticals, the Tylenol case, only a few poisoning manuals were available, and they were relatively hard to find."[46] This is doubtless true; they were hard to find, but they *were* available. As Stern herself concedes, currently how-to manuals on producing chemical and biological agents are not just available on the Internet, but are advertised in paramilitary journals sold in magazine shops all over the United States.[47] According to a US government report, over fifty publications describing the fabrication of explosives and destructive devices are listed in the Library of Congress and are available to any member of the public, as well as being easily available commercially.[48] Despite assertions to the contrary,[49] the infamous *Anarchist Cookbook* (1971) is not available online, although it is easily purchased from bookstores or online retailers. The anonymous authors of Web sites claiming to post the *Cookbook* and similar texts often include a disclaimer that the processes described should not be carried out. This is because many of the 'recipes' have a poor reputation for reliability and safety.

Perhaps the most likely 'recipes' to be of use to terrorists are those related to hacking tools and activities. Such information is also likely to be considerably more accurate than bomb making information, for example; this is because the Internet is

[45] Anti-Defamation League, "Terrorist Activities on the Internet," *Terrorism Update* (Winter 1998).Full text available online at http://www.adl.org/Terror/focus/16_focus_a.asp.
[46] Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), p.50.
[47] Stern, p.51.
[48] (US Department of Justice, p.5); the same report mentions that one Kansas bomber got his bomb instructions from the August 1993 *Reader's Digest* (pp.6-7).
[49] See, for example, Weimann, p.9.

both the domain and tool of hackers. In testimony before the US House Armed Services Committee in 2003, Purdue University professor and information assurance expert, Eugene Spafford said bulletin boards and discussion lists teach hacking techniques to anyone: "We have perhaps a virtual worldwide training camp," he testified.[50] Terrorists have been known to exploit this resource. Imam Samudra's instructions regarding the use of chat rooms favored by hackers to obtain information about 'carding' have already been mentioned. In 1998, Khalid Ibrahim, who identified himself as an Indian national, sought classified and unclassified US government software and information, as well as data from India's Bhabha Atomic Research Center, from hackers communicating via Internet Relay Chat (IRC). Using the online aliases RahulB and Rama3456, Ibrahim began frequenting online cracker hangouts in June 1998. In conversations taken from IRC logs, Ibrahim claimed to be a member of Harkat-ul-Ansar, a militant Kashmiri separatist group.[51]

Finally, it is important to keep in mind that removal of technical information from public Web sites is no guarantee of safeguarding it. In essence, this effort is akin to 'closing the barn door after the horse has bolted.' Intelligence and technical data obtained by terrorist operatives prior to 9/11 can be archived, stored and distributed surreptitiously irrespective of government or private attempts to squelch its presence on the Internet in 2005. Indeed, these materials can be loaded onto offshore or other international Web servers that cannot be affected by US legislation, rendering any attempt to halt their spread outside the reach of American law enforcement.[52]

[50] See Eugene Spafford's testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities on 24 July 2003, p.31. Full text available online at http://commdocs.house.gov/committees/security/has205260.000/has205260_0f.htm.
[51] Niall McKay, "Do Terrorists Troll the Net?" *Wired* 4 November 1998.
Full text available online at http://www.wired.com/news/politics/0,1283,15812,00.html
[52] Tibbetts, p.17.

Fighting Back

In his 1996 assessment of the Internet Charles Swett suggested that as more foreign officials, military officers, business people, and journalists got e-mail addresses, the Internet could be used as a medium for psychological operations campaigns. The Internet, he said, could rapidly convey the official government perspective on a host of important issues to a wide and influential audience.[53] To date, however, most official government Web sites are limited to routine public affairs whereas it is commonplace on the Web to see public diplomacy conducted on behalf of a host of political dissenters, including terrorists. Use of the Internet is a double-edged sword for terrorists, however. They are not the only groups 'operating' the Net, which can act as a valuable tool for anti-terrorist forces also. The more terrorist groups use the Internet to move information, money, and recruits around the globe, the more data that is available with which to trail them. Since 9/11 a number of groups have undertaken initiatives to disrupt terrorist use of the Internet, although a small number of such efforts were also undertaken previous to the attacks. Law enforcement agencies have been the chief instigators of such initiatives, but they have been joined in their endeavors by other government agencies as well as concerned individuals and various groups of hacktivists.

The Role of Law Enforcement and Intelligence Agencies

Intelligence Gathering

[53] Charles Swett, *Strategic Assessment: The Internet* (Washington DC: Department of Defense, 1995). Full text available online at http://www.fas.org/cp/swett.html.

The bulk of this chapter has been concerned with showing how the Internet can act as a significant source of instrumental power for terrorist groups. Use of the Internet can nonetheless also result in significant undesirable effects for the same groups. First, unless terrorists are extremely careful in their use of the Internet for e-mail communication, general information provision, and other activities, they may unwittingly supply law enforcement agencies with a path direct to their door. Second, by putting their positions and ideological beliefs in the public domain, terrorist groups invite opposing sides to respond to these. The ensuing war of words may rebound on the terrorists as adherents and potential recruits are drawn away.[54] Perhaps most importantly, however, the Internet and terrorist Web sites can serve as a provider of open source intelligence for states' intelligence agencies. Although spy agencies are loathe to publicly admit it, it is generally agreed that the Web is playing an ever-growing role in the spy business.

According to the 9/11 Commission's *Staff Statement No. 11*, "open sources--the systematic collection of foreign media--has always been a bedrock source of information for intelligence. Open source remains important, including among terrorist groups that use the media and the Internet to communicate leadership guidance."[55] By the 1990s the US government's Foreign Broadcast Information Service (FBIS) had built a significant translation effort as regards terrorism-related media. Thus many now believe that terrorists' presence on the Internet actually works against them. "A lot of what we know about al-Qaida is gleaned from [their] websites," according to Steven Aftergood, a scientist at the Federation of American Scientists in Washington, D.C., and director of the nonprofit organization's Project on

[54] Soo Hoo, Goodman & Greenberg , p.140.

[55] Staff Statement No. 11, *The Performance of the Intelligence Community* (Washington DC: 9/11 Commission, 2004), p.9. Full text available online at http://www.9-11commission.gov/staff_statements/staff_statement_11.pdf.

Government Secrecy.[56] "They are a greater value as an intelligence source than if they were to disappear."[57] For example, Web sites and message boards have been known to function as a kind of early warning system. Two days before the 9/11 attacks, a message appeared on the popular Dubai-based Alsaha.com discussion forum proclaiming that "in the next two days," "a big surprise" would come from the Saudi Arabian region of Asir. The remote province adjacent to Yemen was where most of the nineteen hijackers hailed from.[58]

Innovations such as the FBIS, while useful, do not tell the whole story, however. The problem begins with the sheer volume of information floating about in cyberspace. According to the 9/11 Commission's *Staff Statement No. 9*, prior to 9/11 the FBI did not have a sufficient number of translators proficient in Arabic and other relevant languages, which by early 2001 had resulted in a significant backlog of untranslated intelligence intercepts. In addition, prior to 9/11, the FBI's investigative activities were governed by Attorney General Guidelines, first put in place in 1976 and revised in 1995, to guard against the misuse of government power. The Guidelines limited the investigative methods and techniques available to FBI agents conducting preliminary investigations of potential terrorist activities. In particular, they prohibited the use of publicly available source information, such as that found on the Internet, unless specified criteria were present.[59] These guidelines have since been modified and terrorist Web sites are thought to be under increased surveillance since

[56] The project's Web site is online at http://www.fas.org/sgp/.

[57] As quoted in John Lasker, "Watchdogs Sniff Out Terror Sites," *Wired News* 25 February 2005. Full text available online at http://www.wired.com/news/privacy/0,1848,66708,00.html.

[58] John R.Bradley, "Website Postings Give Away Terror Activities," *The Straits Times* 5 May 2004. http://www.asiamedia.ucla.edu/article.asp?parentid=10916

[59] Staff Statement No. 9, *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11* (Washington DC: 9/11 Commission, 2004), p.8. Full text available online at http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf.

9/11, especially by Western intelligence agencies.[60] This task remains gargantuan, however; information gleaned from the Net must be corroborated and verified before it can be added to the intelligence mix. This requires significant input of operatives and resources.

Technological Fixes

Given the above, it is unsurprising that many US officials and commentators are recommending that any additional funds that become available to the intelligence agencies be spent on human intelligence capabilities, rather than new technology. Others, however, are convinced that new technologies need to be developed and deployed in the fight against terrorism. They bemoan the fact that prior to 9/11, "Signals intelligence collection against terrorism, while significant, did not have sufficient funding within the NSA. The NSA's slow transformation meant it could not keep pace with advances in telecommunications."[61] Although DCS-1000--more commonly known as Carnivore--the FBI's e-mail packet-sniffer system has not been employed since 2002, Bureau officials have instead employed commercially available monitoring applications to aid in their investigations. Intelligence agencies are also said to be deploying the classic spy tactic of establishing so-called 'honey pots' with a high-tech twist: in this case, setting up bogus Web sites to attract those people they are seeking to monitor.[62] Numerous other technological fixes are also in the works.

Other Innovations

[60] Dan Verton, *Black Ice: The Invisible Threat of Cyberterrorism*. New York: McGraw Hill, 2003), p.220.
[61] Staff Statement No. 11, p.10.
[62] Bernhard Warner, "Intelligence Experts Comb Web for Terror Clues," *The Washington Post* 12 November 2003. Full text available online at http://cryptome.org/web-panic.htm.

It should be clear at this stage that the events of 9/11 impacted intelligence and law enforcement agencies not just in the United States, but around the world. For example, in the UK MI5 took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites. The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including 'Islah.org,' a Saudi Arabian opposition site, and 'Qoqaz.com,' a Chechen site which advocated *jihad*. The message read:

> The atrocities that took place in the USA on 11 September led to the deaths of about five thousand people, including a large number of Muslims and people of other faiths. MI5 (the British Security Service) is responsible for countering terrorism to protect all UK citizens of whatever faith or ethnic group. If you think you can help us to prevent future outrages call us in confidence on 020-7930 9000.

MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 9/11 to want to contact the agency. The agency had intended to post the message on a further fifteen sites known to be accessed by radicals, but many of these were shut down by the FBI in the aftermath of the attacks.[63] The events of 9/11 prompted numerous states' intelligence agencies to reappraise their online presence. Since 2001, MI5 has substantially enhanced its Web site while in 2004, Israel's Mossad spy agency launched a Web site aimed at recruiting staff.

[63] Stephanie Gruner and Gautam Naik, "Extremist Sites Under Heightened Scrutiny," *The Wall Street Journal Online* 8 October 2001, online at http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn; Richard Norton-Taylor, "MI5 Posts Terror Appeal on Arab Websites," *The Guardian* 26 October 2001.

Other Agencies: Sanitising Government Sites

US government Web sites were vital repositories of information for Internet users in the days and weeks following the 9/11 attacks. The sites became important venues for those both directly and indirectly affected by the events of 9/11, members of the public wishing to donate to the relief efforts, and the various agencies' own employees, some of whom were victims of the attacks (or later of the anthrax scares).[64]

While some agencies were uploading information onto the Net, however, others were busy erasing information from their sites. To avoid providing information that might be useful to terrorists planning further attacks, federal agencies, as well as some state and private Web page operators, took large amounts of material off the Internet in the wake of the 9/11 attacks. Some of the erasures were voluntary; others were carried out following requests from US government departments. As mentioned earlier the Nuclear Regulatory Commission, which regulates American nuclear power plants, closed its Web site down for a period following a request from the Department of Defence that it do so. Although no other agency removed its entire site, pages were erased from the Web sites of the Department of Energy, the Interior Department's Geological Survey, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Aviation Administration, the Department of Transportation's Office of Pipeline Safety, the National Archives and Records Administration, the NASA Glenn Research Centre, the International Nuclear Safety Centre, the Los Alamos National Laboratory, the Bureau of Transportation Statistics' Geographic Information Service, and the National Imagery and Mapping Agency.[65]

[64] See Pew Internet and American Life Project, *One Year Later: September 11 and the Internet* (Washington DC: Pew Internet and American Life Project, 2002), pp.33-37. Full text available online at http://www.pewinternet.org/pdfs/PIP_9-11_Report.pdf.

[65] Lucy A. Dalglish, Gregg P. Leslie, and Phillip Taylor, *Homefront Confidential:*

What sorts of information was removed from the sites? The Environmental Protection Agency (EPA) removed thousands of chemical industry risk management plans dealing with hazardous chemical plants from its site. Department of Transportation officials removed pipeline mapping information as well as a study describing risk profiles of various chemicals, while the Bureau of Transportation Statistics removed the National Transportation Atlas Databases and the North American Transportation Atlas, which environmentalists had used to assess the impact of transportation proposals. The Center for Disease Control and Prevention removed a *Report on Chemical Terrorism* that described industry's shortcomings in preparing for a possible terrorist attack.[66] Many of the agencies posted notices that the information had been removed because of its possible usefulness to terrorists.

Hackers and Hacktivists

Hackers also took to the Net in the aftermath of the terror attacks, some to voice their rage, others to applaud the attackers. A group calling themselves the Dispatchers proclaimed that they would destroy Web servers and Internet access in Afghanistan and also target nations that support terrorism. The group proceeded to deface hundreds of Web sites and launch Distributed Denial of Service (DoS) attacks against targets ranging from the Iranian Ministry of the Interior to the Presidential Palace of Afghanistan. Another group, known as Young Intelligent Hackers Against Terror

How the War on Terrorism Affects Access to Information and the Public's Right to Know (Arlington, VA: Reporters Committee for Freedom of the Press, 2002), p.25, online at http://www.rcfp.org/news/documents/Homefront_Confidential.pdf; Pew, pp.8-9; see also Baker, John C., Beth E. Lachman, Dave Frelinger, Kevin O'Connell, Alex Hou, Michael S. Tseng, David T. Orletsky, and Charles Yost, *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (California: Rand, 2004), online at http://www.rand.org/publications/MG/MG142/.

[66] Dalglish, Leslie, & Taylor, p.2; Guy Gugliotta, "Agencies Scrub Web Sites of Sensitive Chemical Data," *Washington Post* 4 October 2001, p.A29, online at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A2738-2001Oct3; Pew, pp.8-9; Julia Scheeres, "Blacklisted Groups Visible on Web," *Wired News* 19 October 2001, online at http://www.wired.com/news/politics/0,1283,47616,00.html.

(YIHAT) claimed, in mid-October 2001, to be negotiating with one European and one Asian government to 'legalize' the groups hacking activities in those states. The group's founder, Kim Schmitz, claimed the group breached the systems of two Arabic banks with ties to Osama Bin Laden, although a spokesperson for the bank denied any penetration had occurred. The group, whose stated mission is to impede the flow of money to terrorists, issued a statement on their Web site requesting that corporations make their networks available to group members for the purpose of providing the "electronic equivalent to terrorist training camps." Later, their public Web site was taken offline, apparently in response to attacks from other hackers.[67]

Not all hacking groups were supportive of the so-called 'hacking war.' On 14 September 2001, the Chaos Computer Club, an organization of German hackers, called for an end to the protests and for all hackers to cease vigilante actions. They called instead for global communication to resolve the conflict: "we believe in the power of communication, a power that has always prevailed in the end and is a more positive force than hatred."[68] A well-known group of computer enthusiasts, known as Cyber Angels, who promote responsible behaviour, also spoke out against the hacking war. They sponsored television advertisements in the US urging hackers to help gather information and intelligence on those who were participating in this hacktivism.[69] In any event, the predicted escalation in hack attacks[70] did not materialize. In the weeks following the attacks, Web page defacements were well

[67] Dorothy Denning, "Is Cyber Terror Next?' In *Understanding September 11*, edited by Craig Calhoun, Paul Price, and Ashley Timmer (New York: New Press, 2001), online at http://www.ssrc.org/sept11/essays/denning.htm; National Infrastructure Protection Center, *NIPC Daily Report* 3 December 2001.

[68] As quoted in Charles Hauss & Alexandra Samuel, "What's the Internet Got to Do With It? Online Responses to 9/11," paper presented at the American Political Science Association Annual (APSA) Annual Convention, Boston, 29 September-1 August 2002.

[69] National Infrastructure Protection Center, *NIPC Daily Report*, 11 December 2001.

[70] Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth College: Institute for Security Technology Studies, 2001). Full text available online at http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm.

publicized, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers--particularly those located in the US--were wary of being negatively associated with the events of 9/11 and curbed their activities as a result.

Since 9/11 a number of Web-based organisations have been established to monitor terrorist Web sites. One of the most well-known of such sites is Internet Haganah,[71] self-described as "an internet counterinsurgency." Also prominent is the Washington DC-based Search for International Terrorist Entities (SITE) Institute[72] that, like Internet Haganah, focuses on Islamic terror groups. Clients of SITE's fee-based intelligence service are said to include the FBI, Office of Homeland Security, and various media organizations. SITE's co-founder and director, Rita Katz, has commented: "It is actually to our benefit to have some of these terror sites up and running by American companies. If the servers are in the US, this is to our advantage when it comes to monitoring activities."[73] Aaron Weisburd, who runs Internet Haganah out of his home in Southern Illinois, says his goal is to keep the extremists moving from address to address: "The object isn't to silence them--the object is to keep them moving, keep them talking, force them to make mistakes, so we can gather as much information about them as we can, each step of the way."[74]

Conclusion

[71] In Hebrew, 'Haganah' means defense. Internet Haganah's homepage is at http://www.haganah.org.il/haganah/index.html.
[72] The SITE Web site is at http://www.siteinstitute.org/.
[73] As quoted in Lasker.
[74] As quoted in Lasker.

Terrorism is generally conceived as physical acts of violence intended to produce fear, and conjures up images of exploding bombs and mutilated bodies. The cyberterrorist threat as portrayed in the mass-media builds upon this aspect of terrorism by seeking to convince the public that cyberterrorism will ultimately result in mass casualties. There is another dimension to terrorism, however: the information dimension. And terrorists exploit it every bit as much as the physical. Death and destruction is not terrorists' ultimate goal; it is power and influence. Terrorists seek political and social change, and their objective is to influence populations in ways that support that change. To accomplish this, they engage not just in physical, but also information operations, and the integration of these.

Up until very recently, cyberterrorism was presented as the sole intersection of terrorism and the Internet, even in the face of contrary evidence. The one-sided nature of the analysis only became apparent to many when, in a little over four weeks in April and May 2004, one Abu Musab-al Zarqawi "rocketed to worldwide fame, or infamy, by a deliberate combination of extreme violence and Internet publicity." In early April 2004, Zarqawi posted online a thirty minute audio recording which explained who he was, why he was fighting, and details of the attacks for which he and his group were responsible. Paul Eedle has described the latter as "a comprehensive branding statement":

> The Internet gave Zarqawi the means to build a brand very quickly. Suddenly the mystery man had a voice, if not a face, and a clear ideology which explained his violence… But what is the point of an insurgent group building a brand, establishing a public profile in this way? The answer is to magnify the impact of its violence.

Prior to the instigation of his Internet-based PR campaign, each of Zarqawi's attacks had to kill large numbers of people in order to get noticed in the chaos and mounting daily death toll in Iraq. By going online, however, Zarqawi was able to both control the interpretation of his violent message and achieve greater impact with smaller operations. By the end of April 2004, his group were regularly issuing communiqués via the Net. The first claimed responsibility for a suicide speedboat attack on Iraq's offshore oil export terminal in the Gulf which, although the operation failed, still shook oil markets because of Zarqawi's efforts at publicising the attack through the Internet.

In May 2004 Zarqawi took things a step further when he used the Internet's force multiplying effect to the maximum effect for the first time when

> …he personally cut off the head of an American hostage live on video, and had the footage posted on the Internet….The entire purpose of the beheading was to video it, to create images that would grip the imaginations of friends and enemies alike. It worked. Zarqawi risked almost nothing in this operation; but he started a withdrawal of foreign contractors which has paralysed reconstruction in Iraq and done as much if not more to undermine US plans as a bomb that killed 100 people in Najaf. And he made himself a hero to jihadis across the world.[75]

The free availability of this and other grisly 'snuff movies' on the Internet led to a realisation that the most important aspect of the terrorism-Internet relationship was

[75] Paul Eedle, "Al Qaeda's Super-Weapon: The Internet," paper presented at *Al-Qaeda 2.0*, New America Foundation, Washington DC, 1-2 December 2004. Full text available online at http://www.outtherenews.com/modules.php?op=modload&name=News&file=article&sid=89&topic=7

not the much vaunted 'cyberterrorism,' but those more mundane and everyday terrorist uses of the Net, from information provision to recruitment, which have a pedigree stretching back for many years before Zarqawi's appearance on the online scene.

The most popular contemporary terrorist sites draw tens of thousands of visitors each month. Obviously, the Internet is not the only tool that a terrorist group needs to 'succeed.' However, the Net can add new dimensions to existing assets that groups can utilize to achieve their goals as well as providing new and innovative avenues for expression, fundraising, recruitment, etc. At the same time, there are also tradeoffs to be made. High levels of visibility increase levels of vulnerability, both to scrutiny and security breaches. Nonetheless, the proliferation of official terrorist sites appears to indicate that the payoffs, in terms of publicity and propaganda value, are understood by many groups to be worth the risks and Zarqawi's exit from the terrorism scene emphatically does not mark the end of the evolution of the terrorism-Internet relationship.

FURTHER READING

Gabriel Weimann's *Terror and the Internet: The New Arena, The New Challenges* (Washington DC: United States Institute of Peace Press, 2006) is the major scholarly text dealing with the issues discussed here. For a list of useful newspaper and magazine reports and a smattering of scholarly articles--all of which are freely accessible online--see the bibliography entitled "Terror Online: Developments in the Use of New Media Technologies by Terrorist Organizations," produced by the USC Center on Public Diplomacy in 2006 and available online at http://uscpublicdiplomacy.com/pdfs/Terror_online.pdf. In terms of other useful online resources, Bob Cromwell's list of *Separatist, Para-military, Military, Intelligence, and Political Organizations*, at http://www.cromwell-intl.com/security/netusers.html, is unfortunately very outdated at this stage, but updated links to the sites of many radical Islamic groups are accessible via Weisburd's *Internet Haganah* site at http://haganah.org.il/haganah/index.html, while the Jamestown Foundation's *Terrorism Focus* bulletins regularly contain analysis of the exchanges taking place on jihadi Internet forums and provide links to same. The latter may be accessed at http://www.jamestown.org.