Terrorism and the Internet: New Media—New Threat?

Maura Conway

School of Law & Government
Dublin City University
Glasnevin
Dublin 9
Ireland

maura.conway@dcu.ie

ABSTRACT The Internet is a powerful political instrument, which is increasingly employed by terrorists to forward their goals. The five most prominent contemporary terrorist uses of the Net are information provision, financing, networking, recruitment, and information gathering. This article describes and explains each of these uses and follows up with examples. The final section of the paper describes the responses of government, law enforcement, intelligence agencies, and others to the terrorism-Internet nexus. There is a particular emphasis within the text on the UK experience, although examples from other jurisdictions are also employed.

"Terrorists use the Internet just like everybody else"
- Richard Clarke (2004) [1]

INTRODUCTION

With over 600 million Internet users worldwide in 2005, today the Internet is recognized as a powerful political instrument. David Resnick has identified three types of Internet politics:

[1] As quoted in New 2004. Clarke was the White House cyber security chief during the tenures of both Bill Clinton and George W. Bush. He resigned in January 2003.

1. Politics Within the Net: This refers to the political life of cyber-communities and other Internet activities that have minimal impact on life off the Net.
2. Politics Which Impacts the Net: This refers to the host of public policy issues raised by the Internet both as a new form of mass communication and a vehicle for commerce.
3. Political Uses of the Net: This refers to the employment of the Internet by ordinary citizens, political activists, organised interests, governments, and others to achieve political goals having little or nothing to do with the Internet *per se* (i.e. to influence political activities offline) (1998, 55-56).

This article is centrally concerned with 'Political Uses of the Net,' specifically the use(s) made of the Internet by terrorist groups, with a particular focus on the United Kingdom's experience in this regard. 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 (see Cohen 2002; Furnell & Warren 1999; Thomas 2003). Probably the best known of these analyses is Gabriel Weimann's report for the US Institute of Peace entitled *www.terrorism.com: How Modern Terrorism Uses the Internet* (2004). Weimann identifies eight major ways in which, he says, terrorists currently use the Internet. These are psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination (2004, 5-11). Having considered Weimann's categorization in conjunction with those suggested by Fred Cohen, Steve Furnell and Matthew Warren, and Timothy L.

Thomas (see Conway forthcoming 2006), the analysis below relies upon what have been determined to be the five core terrorist uses of the Net: information provision, financing, networking, recruitment, and information gathering. Each of these is explained and analyzed in more detail below.

CORE TERRORIST USES OF THE INTERNET

Information Provision

This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. 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.

The most well-known example of the latter in the UK is the kidnap and murder of Liverpudlian Kenneth Bigley who was snatched from his house in Baghdad, along with two American colleagues, on 16 September, 2004. On 18 September, the Tawhid and Jihad group, allegedly headed by Abu Musab al-Zarqawi, released a video of the three men kneeling in front of a Tawhid and Jihad banner; the kidnappers said they would kill the men within 48 hours if their demands for the release of Iraqi women prisoners held by coalition forces were not met. Armstrong was beheaded on September 20 when the

deadline expired, Hensley some 24 hours later; videos of these killings were posted on the Internet shortly after the events took place.

A second video was released by Bigley's captors on 22 September. In this video Bigley is shown pleading for his life; he directly petitions the British Prime Minister saying, “I need you to help me now, Mr Blair, because you are the only person on God’s earth who can help me.” The video was posted on a number of Islamist websites and shown on Arab satellite television station al-Jazeera. A third video was released on 29 September showing Bigley, wearing an orange boiler suit, chained inside a small chicken-wire cage. In this video, Bigley is heard saying, “Tony Blair is lying. He doesn't care about me. I’m just one person.” Bigley was beheaded on 7 October, 2004. The kidnappers filmed Bigley’s murder and these images were subsequently posted on a number of Islamist sites and on at least one US ‘shock’ website. According to news reports, the video shows Bigley reading out a statement, before one of the kidnappers steps forward and cuts off his head with a knife.

Another Briton, Margaret Hassan, was kidnapped on 19 October, 2004 and is thought to have been murdered some weeks later. In a video released of her in captivity, Hassan pleads for the withdrawal of British troops from Iraq, stating “these might be my last hours…Please help me. The British people, tell Mr Blair to take the troops out of Iraq and not bring them here to Baghdad.” She also says “I don’t want to die like Bigley.” In November 2004, al-Jazeera reported that it had received a tape allegedly showing Hassan’s murder, but was unable to confirm its authenticity. The video shows a woman, referred to as Hassan, being shot by a masked gunman. Margaret Hassan’s body was never recovered. The kidnaps, video-based appeals, and subsequent murders and

attendant video footage of both Bigley and Hassan received widespread attention on the Internet and in the mass media, both in Britain and worldwide.

Until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. Such attention remains attractive but, as Weimann points out, "these traditional media have 'selection thresholds' (multistage processes of editorial selection) that terrorists often cannot reach" (2004a, 6). The same criteria do not, of course, apply to the terrorists' own websites. The Internet thus 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 and increasingly attracts attention from the mass media in and of itself.

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" (Napoleoni 2004, 1). 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 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.

Direct Solicitation Via Terrorist Web Sites

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. At one time, indeed, 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 bulletproof 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. In a twist on this scenario, a website linked to the 32 County Sovereignty Movement, an organization regarded as the political wing of the Real IRA, carried a link to the Internet-based book retailer Amazon.com on its top page, which asked visitors to "support our prisoners by shopping through the following link;" commissions generated by any purchases generated through linking from the site--between three and five per cent of sales prices--would have been contributed from Amazon to the site owners. The link was removed in November 2000 shortly after it had gone live. A spokesperson for the retailer was reported to have said "no purchases were made via its web page so no money--not

one penny--has been paid or will be paid by Amazon to the group" (Hyde 2000, 2).

Exploitation of E-Commerce Tools & Entities

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 (Thomas 2003, 117). 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 chapter that acts as a primer on 'carding' (Sipress 2004, A19). 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 entered the public realm (Libbenga 2004).

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 (Hinnen 2004, 18; see also Emerson 2002, 11-12 & 16).

Exploitation of Charities and Fronts

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, probably 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.

The case of Benevolence International Foundation (BIF) stands out as this charity had links to Babar Ahmad, the British man currently held in Belmarsh prison, awaiting extradition to the United States. BIF was based in Chicago and run by Enaam Arnaout. A Web site maintained by Ahmad, Qoqaz.net, was used to solicit funds to support the mujahideen in Chechnya, which were subsequently funnelled through BIF. At that time, the leader of the Chechen mujahideen was one Ibn al Khattab who, through the Qoqaz

website, told supporters to wait until a “trustworthy aid organization” to work with them could be identified. The Qoqaz site later posted the following:

> There is one trusted agency that has set up operations in the region and we will be posting their contact and bank details, etc. on the Internet very soon insha-Allah. This is the only aid agency that the Qoqaz web-sites trust and recommend the people to give their donations to.

Shortly after this posting, the Qoqaz site created active donations links to two charities; one was BIF. Between January and April of 2000, BIF wire-transferred nearly $700,000 to Chechen separatist-linked bank accounts in Georgia, Azerbaijan, Russia, and Latvia. Arnaout was indicted, along with BIF, in the US in 2002 on a number of charges, including perjury and racketeering. Prosecutors said they had proof, in the form of correspondence and photos, of ties between Arnaout and Osama bin Laden. In February 2003, Arnaout reached a plea agreement with prosecutors: he pled guilty to one count of racketeering conspiracy, related to directing BIF donations to purchase clothing and equipment for ‘fighters’ in Bosnia and Chechnya, without disclosing this use of funds to donors (ISTS 2004, 31-32).

Terrorists have also infiltrated branches of existing charities to raise funds clandestinely. Many such organizations provide the humanitarian services advertised: feeding, clothing, and educating the poor and illiterate, and providing medical care for the sick. As Todd Hinnen has pointed out, “it is important not to presume that charitable organizations have terrorist affiliations simply because they serve regions or religious or

ideological communities with which terrorism may be associated" (2004, 17; see also Emerson 2002, 3). For example, Rachel Ehrenfeld (2004) and others (see, for example, Emerson 2002, 25) have claimed that the most active Hamas front organization worldwide is the London-based Palestinians Relief and Development Fund (Interpal). [2] In 2003 alone, according to Ehrenfeld, this organization sent more than $20 million to different Hamas organizations in the Palestinian territories.[3] Recently, however, the UK's Charity Commission has cleared this charity of any wrongdoing (UK Charity Commission 2004). As a result, Interpal's trustees have said that they will now seek to have their organization removed from the US Treasury Department's list of terror organizations. Nonetheless, 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' 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

[2] http://www.interpal.org/index.html.
[3] According to the UK Charity Commission, Interpal's income for 2001 was around £4 million.

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" (Arquilla *et al* 1999, 41). This type of organizational structure is qualitatively different from traditional hierarchical 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 (Arquilla *et al* 1999, 48-53; Arquilla & Ronfeldt 2001a).

Planning and Coordination

"Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the Internet" (Margulies 2004, 2). 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. New technologies clearly 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. (Weimann 2004a, 9).

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" (1999, 251). Zanini's hypothesis appears to be borne out by recent events. For example, many of the terrorists indicted by the United States 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."[4] 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 (Hinnen 2004, 38). [5]

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

[4] 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.
[5] 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.

'jihadist' sites exist that express support for terrorism. 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. An early example of such a site was that established by Egyptian Islamic Jihad in 2000, which illustrates not just the Internet contacts amongst radicals alluded to above, but also the integration of high-tech and what might be termed 'no-tech' communicative circuits amongst the latter. According to reports in the *Wall Street Journal*, Abu Qatada--a Muslim preacher of Jordanian citizenship and Palestinian origin who is currently being held in the high-security Belmarsh prison in south-east London--was one of those responsible for uploading information onto the jihadi Web site; Qatada is said to have received instructions about uploading the information via e-mail, but to have received the actual content for posting on a computer disc that was hand-delivered to his London home. The newspaper report goes on to say that a computer retrieved by the *Wall Street Journal* in Kabul indicated that Qatada had extensive contacts with radicals in Afghanistan and, further, that "European investigators say Abu Qatada acted as both a spiritual guide and a liaison officer, passing messages between scattered al Qaeda cells" (Higgins, Leggett & Cullison 2002).

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, teaching, and training. Clearly, "information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility" (Tibbetts 2002, 5). 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" (Thomas 2003, 119).

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 terrorist group in adjusting their position and tactics and, potentially, increasing their levels of support and general appeal (Gibson & Ward 2000, 305-306; Soo Hoo, Goodman & Greenberg 1997, 140; Weimann 2004a, 8). Online recruitment by terrorist organizations is said to be widespread. 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 (2004a, 8).

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 (Weimann 2004a, 6). 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

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” (McCullagh 2003).

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 US 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." According to Zimmerman, "it is currently unlikely that the information on our Web site would provide significant advantage to assist a terrorist" (Ahlers 2004).

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[6] since 9/11 thousands of documents and tremendous amounts of data have been removed from US government sites. The difficulty, however, is that much of the same information remains available on private sector Web sites (McCullagh 2003; Bass & Moulton 2002). 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,[7] 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[8] (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 (Jehl & Johnston 2004; Verton & Mearian 2004). The Australian press

[6] OMB Watch is a watchdog group based in Washington DC. Their home page is at http://www.ombwatch.org.
[7] See http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm.
[8] See http://www.nucleartourist.com/.

has also reported that a man charged with terrorism offences there had used Australian government Web sites to get maps, data, and satellite images of potential targets. The government of New South Wales was said to be considering restricting the range of information available on their Web sites as a result (ABC 2004).

Terrorists can also use the Internet to learn about antiterrorism measures. Gabriel Weimann suggests that a simple strategy like conducting word searches of online newspapers and journals could allow a terrorist to study the means designed to counter attacks, or the vulnerabilities of these measures (2004b, 15).

Sharing Information

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 (US Department of Justice 1997, 15-16).

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 sites such as Barnesandnoble.com 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 (Thomas 2003, 115; Weimann 2004a, 9). A much larger manual, nicknamed *The Encyclopedia of Jihad* and prepared by al Qaeda, runs to thousands of pages; distributed via the Web, it offers detailed instructions on how to establish an underground organization and execute terror attacks (Weimann 2004a, 9).

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 (Weimann 2004a, 10). It has also been suggested that Kamel Bourgass, convicted of conspiring to cause a public nuisance in relation to the British ‘ricin terror

plot,' may have downloaded his flawed ricin recipe from the Web site of an American extremist group (Dodd 2005; Phillips 2005; Riddell 2005).

FIGHTING BACK

Use of the Internet is a double-edged sword for terrorists. They are not the only groups utilizing the Net to forward their goals, which can act as a valuable instrumental power source 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 groups of hacktivists.

The Role of Law Enforcement and Intelligence Agencies

Intelligence Gathering

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 (Soo Hoo, Goodman & Greenberg 1997, 140). 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.

The July 2005 London bombings provided the spur for the British government to act against terrorist Web sites operating out of the UK. In the immediate aftermath of the attacks Charles Clarke, the British Home Secretary, indicated in a parliamentary speech that he would be seeking to extend the state's powers "to deal with those who foment terrorism, or seek to provoke others to commit terrorist acts." In his speech Clarke referred specifically to the inclusion within the ambit of these new powers "running websites or writing articles that are intended to foment or provoke terrorism."[9] His plans were endorsed by Britain's Association of Chief Police Officers who themselves requested new legislation be drawn up giving law enforcement agencies "powers to attack identified websites."[10] The UK Prevention of Terrorism Bill 2005, which narrowly avoided defeat in Westminster in October, will be subject to a second reading in March

[9] The full text of Clarke's remarks may be accessed online at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050720/debtext/50720-04.htm.
[10] The APCO proposals are outlined in a press release available online at http://www.acpo.police.uk/asp/news/PRDisplay.asp?PR_GUID={423FD3C2-2791-403A-B5D0-8FC6B5476B0B}.

2006. Opposition centers on two key measures: new police powers to detain suspects for up to 90 days without charges, and a proposed offense of "encouragement or glorification of terrorism." One of the main reasons suggested for the former was that suspects needed to be detained without charge for longer than 14 days because of the difficulty and complexity of decrypting computer hard drives, a suggestion which has been challenged by both the UK Intelligence Services Commissioner and the UK Interception of Communications Commissioner. With regard to the glorification of terrorism, such a measure would clearly criminalize the establishment, maintenance, and hosting of many Web sites currently operational within the UK. The major criticism, of course, is that the latter clause may serve to stifle legitimate political speech. Several other measures included in the Bill that may also impact terrorist Internet use in the UK, such as the outlawing of "acts preparatory to terrorism" and the giving or receiving of "terrorism training," went largely uncontested in the parliamentary debate.

Other Innovations

Shortly after 9/11, 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 (Gruner & Naik 2001; Norton-Taylor 2001).

More recently, British intelligence agencies are said to have been planning the infiltration of Islamic extremist networks via the Internet. In April 2005, documents leaked to *The Observer* newspaper revealed details of the proposals, which were contained in a letter from the head of the intelligence arm of the British Foreign Office (FCO). The confidential 2004 letter[11] from the Foreign Office's top intelligence official, William Ehrman, to the government's security and intelligence co-ordinator, Sir David Omand, proposed that intelligence agents should infiltrate extremist chat rooms posing as radicals and work to dissuade extremists from resorting to violence. It was suggested that while radicals would not listen to the traditional calls for peace in the Middle East, they might listen to religious arguments about the nature of jihad that, while anti-Western,

[11] A pdf copy of the letter is available online at http://image.guardian.co.uk/sys-files/Observer/documents/2005/09/04/Confidential.pdf.

eschewed terrorism. Ehrman's major concerns were that similar operations during the Cold War "had a mixed record" and that he might not have the linguists and Islamic experts necessary to follow through with the plan.

The events of 9/11 also prompted numerous states' intelligence agencies to reappraise their online presence. Since 2001, MI5 has substantially enhanced its Web site, while MI6 launched its very first site in 2005.

Hackers and Hacktivists

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,[12] self-described as "an internet counterinsurgency." Also prominent is the Washington DC-based Search for International Terrorist Entities (SITE) Institute[13] 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" (as quoted in Lasker 2005). 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,

[12] In Hebrew, 'Haganah' means defense. Internet Haganah is online at http://www.haganah.org.il/haganah/index.html.
[13] The SITE Web site is at http://www.siteinstitute.org/.

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" (as quoted in Lasker 2005). In the UK, Niall Doyle has come to prominence as a result of his book *Terror Tracker* (2005) in which he claims to have used the Internet, particularly Muslim fundamentalist Web sites and chat rooms, to track suspected Islamic militants operating out of the UK.

CONCLUSION

With regard to analyses of terrorism and the Internet, in the wake of 9/11 the question on many people's lips was 'Is Cyberterrorism Next?' (Denning 2001). The potential threat posed by cyberterrorism received a great deal of attention in the media, particularly in the United States, both before and after 9/11. In November 2002, for example, Omar Bakri Muhammed, a UK-based Muslim cleric and leader of Al Muhajiroun, granted an exclusive interview to *Computerworld* magazine, in which he claimed that al-Qaeda was planning to use cyber attack techniques against economic targets, specifically the New York, London, and Tokyo stock markets. Muhammed's remarks received wide coverage in the news media, but the veracity of his alleged links to Osama bin Laden and al-Qaeda were questioned by a number of experts, including former top CIA counterterrorism official Vince Cannistraro who called Muhammed "a fire-breather" with no special knowledge of al-Qaeda's plans (ISTS 2004, 50). The focus has since shifted from cyberterrorism to terrorist use of the Net.

The case of Babar Ahmad is an interesting one in this regard. Ahmad, a British citizen, was the publisher of two prominent jihadi Web sites, azzam.com and qoqaz.com, which were hosted in the United States, and through which he is accused of raising money for Islamic militants in Chechnya and elsewhere. The UK government has agreed to a US extradition request and Ahmad is to be tried in the US on charges relating to a number of the terrorist uses of the Internet identified in this article, which fall under the heading of "conspiracy to provide material support to terrorists." This includes not just the solicitation of financial support referred to above but also, according to an affidavit filed in US District Court in Connecticut in 2004, urging all Muslims to "use every means at their disposal to undertake military and physical training for jihad," and providing "explicit instructions" about how to raise funds and funnel these to violent fundamentalist organizations through conduits such as BIF, which was referred to earlier.

Similar charges as those pending against Ahmad have been brought against US residents who engaged in similar activities in the recent past; however, due to high levels of speech protection in the United States, at least two defendants have so far been tried and freed without charge. These are Sami Omas Al-Hussayen, a PhD candidate in computer science at the University of Idaho, who established and maintained a radical Web site, and Sami Amin Al-Arian, a Professor at the University of South Florida, who was tried on charges relating to, amongst other things, his utilization of the Internet to publish and catalogue acts of violence committed by Palestinian Islamic Jihad. Babar Ahmad's trial will serve as yet another test of the new US antiterrorism law that makes it a crime to provide material support in the form of expert advice or assistance to terrorists,

including IT support. Clearly, Ahmad's case will be one to watch in terms of its impact on terrorism-related Internet-based speech.

In the meantime, researchers are still unclear whether the ability to communicate online worldwide has contributed to the increase in terrorist violence. It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful, and reach a mass audience. The most popular 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.

REFERENCES

Australian Broadcasting Corporation (ABC). 2004. 'NSW Considers Limits on Government Website.' *ABC Online* 28 April.

Ahlers, Mike M. 2004. 'Blueprints for Terrorists?' *CNN.com* 19 November. http://www.cnn.com/2004/US/10/19/terror.nrc/

Arquilla, John, David Ronfeldt & Michele Zanini. 1999. 'Networks, Netwar and Information-Age Terrorism.' In Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini & Brian Michael Jenkins, *Countering the New Terrorism.* Santa Monica, Calif.: Rand. http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf

Bass, Gary D. & Sean Moulton. 2002. 'The Bush Administration's Secrecy Policy:

A Call to Action to Protect Democratic Values' [Working Paper]. Washington DC: OMB Watch. http://www.ombwatch.org/rtk/secrecy.pdf

Cohen, Fred. 2002. 'Terrorism and Cyberspace.' *Network Security* Vol. 5.

Conway, Maura. 2006. 'Terrorist "Use" of the Internet and Fighting Back.' *Information & Security* Vol. 18 (forthcoming).

Denning, Dorothy. 2001. *Is Cyber Terror Next?* New York: US Social Science Research Council. http://www.ssrc.org/sept11/essays/denning.htm.

Dodd, Vikram. 2005. 'Doubts Grow Over al-Qaida Link in Ricin Plot.' *The Guardian* 16 April.

Emerson, Steven. 2002. 'Fund-Raising Methods and Procedures for International Terrorist Organizations.' Testimony before the House Committee on Financial Services, 12 February. http://financialservices.house.gov/media/pdf/021202se.pdf

Furnell, Steve & Matthew Warren. 1999. 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium.' *Computers and Security* 18(1).

Gibson, Rachel and Stephen Ward. 2000. 'A Proposed Methodology for Studying the Function and Effectiveness of Party and Candidate Web Sites.' *Social Science Computer Review* Vol. 18(3).

Gruner, Stephanie & Gautam Naik. 2001. 'Extremist Sites Under Heightened Scrutiny.' *The Wall Street Journal Online* 8 October. http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn.

Higgins, Andrew, Karby Leggett, & Alan Cullison. 2002. 'How Al Qaeda Put Internet to Use.' *Wall Street Journal* 11 November. http://www.msnbc.com/avantgo/833533.htm

Hinnen, Todd M. 2004. 'The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet.' *Columbia Science and Technology Law Review* Vol. 5. http://www.stlr.org/html/volume5/hinnenintro.html

Institute for Security Technology Studies (ISTS). 2001. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Dartmouth College: Institute for Security Technology Studies. http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm.

Jehl, Douglas & David Johnston. 2004. 'Reports That Led to Terror Alert Were Years Old, Officials Say.' *New York Times* 3 August.

Lasker, John. 2005. 'Watchdogs Sniff Out Terror Sites.' *Wired News* 25 February. http://www.wired.com/news/privacy/0,1848,66708,00.html

Libbenga, Jan. 2004. 'Terrorists Grow Fat on E-Mail Scams.' *The Register* 28 September. http://www.theregister.co.uk/2004/09/28/terrorist_email_scams/

Margulies, Peter. 2004. 'The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment.' *UCLA Journal of Law and Technology* 8(2). http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf

McCullagh, Declan. 2003. 'Military Worried About Web Leaks.' *C|Net News* 16 January. http://news.com.com/2100-1023-981057.html

Napoleoni, Loretta. 2004. 'Money and Terrorism.' *Strategic Insights* 3(4). http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf

New, William. 2004. 'Former Cybersecurity Chief Opposes New Regulations.' *GovExec.com* 24 May. http://www.govexec.com/dailyfed/0504/052404tdpm2.htm

Norton-Taylor, Richard. 2001. 'MI5 Posts Terror Appeal on Arab Websites.' *The Guardian* 26 October.

Phillips, Melanie. 2005. 'This Trial Was Not a Success. It's a Disaster.' *The Sunday Telegraph* 17 April.

Riddell, Mary. 2005. 'Comment: With Poison in Their Souls.' *The Observer* 17 April

Resnick, David. 1999. 'Politics on the Internet: The Normalization of Cyberspace.' In Chris Toulouse & Timothy W. Luke (Ed.s), *The Politics of Cyberspace*. New York & London: Routledge.

Sipress, Alan. 2004. 'An Indonesian's Prison Memoir Takes Holy War into Cyberspace.' *Washington Post* 14 December. http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html

Soo Hoo, Kevin, Seymour Goodman, & Lawrence Greenberg. 1997. 'Information Technology and the Terrorist Threat.' *Survival* 39(3).

Stern, Jessica. 1999. *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press.

Thomas, Timothy L. 2003. 'Al Qaeda and the Internet: The Danger of "Cyberplanning."' *Parameters* Spring. http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm

Tibbetts, Patrick S. 2002. *Terrorist Use of the Internet and Related Information Technologies*. [Unpublished Paper]. Fort Leavenworth, Kansas: United States Army Command and General Staff College. http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf

US Department of Justice. 1997. *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. http://cryptome.org/abi.htm.

Verton, Dan & Lucas Mearian. 2004. 'Online Data a Gold Mine for Terrorists.' *ComputerWorld* 6 August. http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html

Weimann, Gabriel. 2004a. *WWW.terror.net: How Modern Terrorism Uses the Internet*. Washington DC: United States Institute of Peace. http://www.usip.org/pubs/specialreports/sr116.pdf

Weimann, Gabriel. 2004b. 'Terror on the Internet: The New Arena, The New Challenges.' Paper presented at the *International Studies Association (ISA) Annual Conference*, Montreal, Quebec, Canada, 17-20 March.

Zanini, Michele. 1999. 'Middle Eastern Terrorism and Netwar.' *Studies in Conflict and Terrorism* 22(3).