# TERRORIST 'USE' OF THE INTERNET AND FIGHTING BACK

Maura CONWAY

**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 is illustrated with examples of each. The final section of the paper describes the responses of government, law enforcement, intelligence agencies, and others to the terrorism-Internet nexus.

**Keywords:** Terrorism, Internet, Terrorist Financing, Terrorist Networking, Terrorist Recruitment, Counter-Terrorism.

*"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 [2]:

- *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.
- *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.
- *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).

*INFORMATION & SECURITY. An International Journal, Vol.19, 2006, 9-30.*

This paper is centrally concerned with 'Political Uses of the Net,' specifically the use(s) made of the Internet by terrorist groups, a subject that to date has been the focus of only a very small amount of substantive social science research.

What are terrorist groups attempting to do by gaining a foothold in cyberspace? In 1997, Wayne Rash, in his *Politics on the Nets*, posited eight uses of the Net that he foresaw political groups adopting. He described these as tactical communications, organization, recruitment, fundraising, strategic positioning, media relations, affinity connections, and international connections.[3] Although Rash did not identify terrorists as a specific political Internet user group, his list of uses is broadly similar to those later developed by authors concerned with the narrower issue of terrorist use of the Net (see Table 1). In 1999, for example, Steve Furnell and Matthew Warren described the core terrorist uses of the Net as propaganda/ publicity, fundraising, information dissemination, and secure communications.[4] Fred Cohen presents his readers with a broadly similar list of uses.[5] Timothy Thomas, on the other hand, presents a more detailed rendition of terrorist uses of the Net. In his article 'Al Qaeda and the Internet: The Danger of "Cyberplanning,"' which appeared in the US Army journal *Parameters* in 2003, Thomas discusses some sixteen potential uses of the Internet by terrorists.[6] Thomas does not adopt the use paradigm but refers instead to what he dubs "cyberplanning"—"the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed" [7]—which nonetheless shares sufficient similarities with the use approach as to be almost indistinguishable from it. Finally, in a recent report for the United States Institute of Peace entitled *WWW.terror.net: How Modern Terrorism Uses the Internet*, Gabriel Weimann identifies eight different 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.[8]

There is considerable overlap amongst the terrorist uses of the Net identified by the different authors in Table 1.[9] While twenty-two different categories of use are mentioned, often authors are simply using different terms to refer to the same issues. This is clearest in terms of the identity shared by the concepts 'fundraising' and 'finance,' but also relates to the concepts 'information gathering' and 'data mining,' for example. Given such overlaps, the analysis below relies on what have been determined to be the five core terrorist uses of the Internet: information provision, financing, networking, recruitment, and information gathering. Each of the uses identified in Table 1 fits into one of these categories or its sub-categories. All four authors mentioned identify resource generation along with information provision, particularly propaganda, as primary terrorist uses of the Internet. I have subsumed a number of other issues, including secure communication and planning, under the heading 'Networking.'

Table 1: Core Terrorist Uses of the Internet.

| **Author(s)** | *Furnell & Warren* [10] | *Cohen* [11] | *Thomas* [12] | *Weimann* [13] |
|---|---|---|---|---|
| **Uses** | Propaganda & Publicity<br>Fundraising<br>Information Dissemination<br>Secure Communications | Planning<br>Finance<br>Coordination & Operations<br>Political Action<br>Propaganda | Profiling<br>Propaganda<br>Anonymous/ Covert Communication<br>Generating "Cyberfear"<br>Finance<br>Command & Control<br>Mobilisation & Recruitment<br>Information Gathering<br>Mitigation of Risk<br>Theft/ Manipulation of Data<br>Offensive Use<br>Misinformation | Psychological Warfare<br>Publicity & Propaganda<br>Data Mining<br>Fundraising<br>Recruitment & Mobilisation<br>Networking<br>Sharing Information<br>Planning & Coordination |

Finally, although recruitment is mentioned by just two of the authors discussed here,[14] there is evidence to support the view that the Internet has been utilized to promote participation in terrorist activity. Each of the five core terrorist uses of the Internet is explained and analyzed in more detail below.

## Five Terrorist Uses of the Net

### *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, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist

Daniel Pearl in Pakistan via their Web sites.[15] These functions are clearly improved by the Web's enhanced volume, increased speed of data transmission, low-cost, relatively uncontrolled nature, and global reach.

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. As Weimann points out, "these traditional media have 'selection thresholds' (multistage processes of editorial selection) that terrorists often cannot reach." [16] 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.

### *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." [17] 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. For example, the IRA's main Web site contains a page on which visitors can make credit card donations.[18] 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. A second, and related, fundraising method is to profile site visitors by employing user demographics (yielded, for example, from identifying information entered in online questionnaires or order forms) and to contact those whose profiles indicate they are potential financial supporters, a function which may be carried out by proxies, ac-

cording to Tibbetts.[19] A third 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.

*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.[20] 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.' [21]

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.[22] 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.[23]

*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.

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. 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.

As the LVF and InfoCom examples show, the support sought by and provided to terrorist organizations may not always be in the form of cash. Terrorist groups use the Internet to solicit other fungible goods, to accumulate supplies, and to recruit foot soldiers. In this paper, however, the term 'financing' has been used in its narrow sense to mean the remittance of money. Nonetheless, it may also be used as shorthand for the accumulation of any of the material resources necessary for terrorists to maintain their organizations and carry out operations.

***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 subgroups and external organizations around the globe from their central Web site.

*Transforming Organizational Structures* [24]

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." [25] 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.[26]

*Planning and Coordination*

"Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the Internet." [27] 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.[28]

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." [29] 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." [30] 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.[31,32]

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.[33]

*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." [34] 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." [35]

### *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.[36]

Online recruitment by terrorist organizations is said to be widespread. Fritz, Harris, Kolb, Larich, and Stocker 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.[37] 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.[38]

### *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.[39] 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 'in-

formation sharing,' which refers to more general online information collection by terrorists.

*Data Mining*

In January 2003, U.S. 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." [40]

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." According to Zimmerman, "it is currently unlikely that the information on our Web site would provide significant advantage to assist a terrorist." [41]

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[42] since 9/11 thousands of documents and tremendous amounts of data have been removed from U.S. government sites. The difficulty, however, is that much of the same information remains available on private sector Web sites.[43] 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,[44] 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.[45,46]

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.[47] The Australian press 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.[48]

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.[49]

*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 U.S. Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts.[50]

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.[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.[52] 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.[53]

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.[54]

*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.[55] As a result, many have called for laws restricting the publication of bomb-making instructions on the Internet, while others have pointed out that this material is already easily accessible in bookstores and libraries.[56] 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." [57] 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.[58] According to a U.S. 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.[59,60] Ken Shirriff sums up this point well:

> Note that *The Anarchist Cookbook* is available from nearly any bookstore in the U.S. These dangerous institutions will also sell you Nazi and hate literature, pornography, instructions on growing drugs, and so forth. For some reason, getting this stuff from a bookstore is not news, but getting it over the Internet is.[61]

Despite assertions to the contrary,[62] the infamous *Anarchist Cookbook* [63] is not available online, although it is easily purchased from bookstores or from Amazon.com. 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 both the domain and tool of hackers. In testimony before the U.S. 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.[64] 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 U.S. 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.[65]

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 U.S. legislation, rendering any attempt to halt their spread outside the reach of American law enforcement.[66]

## Fighting Back

Use of the Internet is a double-edged sword for terrorists. They are not the only groups 'operating' the Net,[67] 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 various groups of hacktivists.

### *The Role of Law Enforcement and Intelligence Agencies*

*Intelligence Gathering*

The bulk of this paper 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.[68] 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." [69] 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 non-profit organization's Project on Government Secrecy.[70] "They are a greater value as an intelligence source than if they were to disappear" (as quoted by Lasker).[71] 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.[72]

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.[73] These guidelines have since been modified and terrorist Web sites are thought to be under increased surveillance since 9/11, especially by Western intelligence agencies.[74] 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. And still intelligence agencies simply cannot monitor the entire Internet all of the time.

*Technological Fixes*

Given the above, it is unsurprising that many U.S. 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." [75] 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.[76] Numerous other technological fixes are also in the works.

*Other Innovations*

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. On this side of the Atlantic, 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.[77] 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.

***Other Agencies: Sanitising Government Sites***

U.S. 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).[78]

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 U.S. 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.[79]

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 Ter-*

*rorism* that described industry's shortcomings in preparing for a possible terrorist attack.[80] 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 (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.[81]

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" (as quoted by Hauss and Samuel).[82] 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.[83] In any event, the predicted escalation in hack attacks [84] did not materialize. In the weeks following the attacks, Web page defacements were well 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 U.S.—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,[85] self-described as "an internet counterinsurgency." Also prominent is the Washington

DC-based Search for International Terrorist Entities (SITE) Institute [86] 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 by Lasker).[87] 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" (as quoted by Lasker).[88]

## Conclusion

Researchers are still unclear whether the ability to communicate online worldwide has resulted in an increase or a decrease in terrorist acts. 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.[89] 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. 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.

## Notes:

[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.

[2] David Resnick, "Politics on the Internet: The Normalization of Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York & London: Routledge, 1999), 55-56.

[3] Wayne Rash, *Politics on the Nets: Wiring the Political Process* (New York: W.H. Freeman, 1997), 176-177.

[4] Steve Furnell and Matthew Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers and Security* 18, no. 1 (1999): 30-32.

[5] Fred Cohen, "Terrorism and Cyberspace," *Network Security* 5 (2002): 18-19.

[6] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters* (Spring 2003): 114-122, <http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm> (12 Dec. 2005).

[7] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 113.

[8] Gabriel Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet* (Washington DC: United States Institute of Peace, 2004), <http://www.usip.org/pubs/specialreports/sr116.pdf> (12 Dec. 2005), 5-11.

[9] Such overlaps are not just evident amongst those who adopt a use paradigm, but are shared with those who adopt an Information Operations (IO) approach (see Dorothy Denning, "Information Operations and Terrorism," 2004 (Pre-Print); N.E. Emery, R. S. Earl, and R. Buettner, "Terrorist Use of Information Operations," *Journal of Information Warfare* 3, no. 2 (2004); Kevin O'Brien and Izhar Lev, "Information Operations and Counterterrorism," *Jane's Intelligence Review* 14, no. 9 (2002).

[10] Furnell and Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium."

[11] Cohen, "Terrorism and Cyberspace."

[12] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning.'"

[13] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*.

[14] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning;'" Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*.

[15] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 5.

[16] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 6.

[17] Loretta Napoleoni, "Money and Terrorism," *Strategic Insights* 3, no. 4 (2004): 1, <http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf> (12 Dec. 2005).

[18] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 7.

[19] 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), 20, <http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf> (15 May 2005).

[20] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 117.

[21] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," *Washington Post*, 14 December 2004, A19, <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html> (12 Dec. 2005).

[22] Jan Libbenga, "Terrorists Grow Fat on E-Mail Scams," *The Register*, 28 September 2004, <http://www.theregister.co.uk/2004/09/28/terrorist_email_scams/> (12 Dec. 2005).

[23] Todd M. Hinnen, "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet," *Columbia Science and Technology Law Review* 5 (2004): 18, <http://www.stlr.org/html/volume5/hinnenintro.html> (12 Dec. 2005); see also Steven Emerson, "Fund-Raising Methods and Procedures for International T`errorist

Organizations," Testimony before the House Committee on Financial Services, 12 February 2002, 11-12, 16, <http://financialservices.house.gov/media/pdf/021202se.pdf> (12 Dec. 2005).

[24] For a brief introduction to organizational network analysis, see John Arquilla and David Ronfeldt, "Networks, Netwars and the Fight for the Future," *First Monday* 6, no. 10 (2001), <http://www.firstmonday.org/issues/issue6_10/ronfeldt/index.html> (12 Dec. 2005); John Arquilla and David Ronfeldt, "What Next for Networks and Netwars?" in *Networks and Netwars*, ed. John Arquilla and David Ronfledt (California: Rand, 2001), 319-323, <http://www.rand.org/publications/MR/MR1382/MR1382.ch10.pdf> (12 Dec. 2005).

[25] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism*, ed. Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini, and Brian Michael Jenkins (Santa Monica, Calif.: Rand, 1999), 41, <www.rand.org/publications/MR/MR989/MR989.chap3.pdf> (12 Dec. 2005).

[26] Arquilla, Ronfeldt, and Zanini, "Networks, Netwar and Information-Age Terrorism," 48-53; John Arquilla, and David Ronfeldt, "Emergence and Influence of the Zapatista Social Netwar," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt (California: Rand, 2001), <http://www.rand.org/publications/MR/MR1382/MR1382.ch6.pdf> (12 Dec. 2005).

[27] Peter Margulies, "The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment," *UCLA Journal of Law and Technology* 8, no. 2 (2004): 2, <http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf> (12 Dec. 2005).

[28] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[29] Michele Zanini, "Middle Eastern Terrorism and Netwar," *Studies in Conflict and Terrorism* 22, no. 3 (1999): 251.

[30] 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> (12 Dec. 2005).

[31] Hinnen, "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet," 38.

[32] 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> (12 Dec. 2005).

[33] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[34] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 5.

[35] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 119.

[36] 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, no. 3 (2000): 305-306; Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival* 39, no. 3 (1997): 140; Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 8.

[37] Kathryn Fritz, Lindsay Harris, Daniel Kolb, Paula Larich, and Kathleen Stocker, "Terrorist Use of the Internet and National Response," Unpublished Paper (College Park: University of Maryland, 2004), 9, <http://www.wam.umd.edu/~larich/735/index.html> (12 Dec. 2005)

[38] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 8.

[39] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 6.

[40] Declan McCullagh, "Military Worried about Web Leaks," *C|Net News*, 16 January 2003, <http://news.com.com/2100-1023-981057.html> (12 Dec. 2005).

[41] Mike M. Ahlers, "Blueprints for Terrorists?" *CNN.com*, 19 November 2004, <http://www.cnn.com/2004/US/10/19/terror.nrc/> (12 Dec. 2005).

[42] OMB Watch is a watchdog group based in Washington DC. Their home page is at <http://www.ombwatch.org> (12 Dec. 2005).

[43] McCullagh, "Military Worried about Web Leaks;" 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), <http://www.ombwatch.org/rtk/secrecy.pdf> (12 Dec. 2005).

[44] See <http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm>.

[45] See <http://www.nucleartourist.com/>.

[46] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 15.

[47] 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, <http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html> (12 Dec. 2005).

[48] Australian Broadcasting Corporation (ABC), "NSW Considers Limits on Government Website," *ABC Online*, 28 April 2004.

[49] Gabriel Weimann, "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 2004), 15.

[50] 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), 15-16, <http://cryptome.org/abi.htm> (12 Dec. 2005).

[51] Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), 51.

[52] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 115; Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[53] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[54] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 10.

[55] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 17.

[56] Anti-Defamation League, "Terrorist Activities on the Internet," *Terrorism Update* (Winter 1998), <http://www.adl.org/Terror/focus/16_focus_a.asp> (12 Dec. 2005).

[57] Stern, *The Ultimate Terrorists*, 50.

[58] Stern, *The Ultimate Terrorists*, 51.

[59] The same report mentions that one Kansas bomber got his bomb instructions from the August 1993 *Reader's Digest* (1997), 6-7.

[60] US Department of Justice, *Report on the Availability of Bombmaking Information*, 5.

[61] Ken Shirriff, *The Anarchist Cookbook FAQ* (2001), <http://www.righto.com/anarchist-cookbook-faq.html> (12 Dec. 2005).

[62] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[63] William Powell, *The Anarchist Cookbook* (Ozark PR LLC, 2003 (1971)).

[64] Eugene Spafford, *Testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities*, 24 July 2003, 31, <http://commdocs.house.gov/committees/security/has205260.000/has205260_0f.htm> (12 Dec. 2005).

[65] Niall McKay, "Do Terrorists Troll the Net?" *Wired*, 4 November 1998, <www.wired.com/news/politics/0,1283,15812,00.html> (12 Dec. 2005).

[66] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 17.

[67] Richard Rogers, "Operating Issue Networks on the Web," *Science as Culture* 11, no. 2 (2002): 191.

[68] Soo Hoo, Goodman, and Greenberg, "Information Technology and the Terrorist Threat," 140.

[69] *Staff Statement No. 11, The Performance of the Intelligence Community* (Washington DC: 9/11 Commission, 2004), 9, <http://www.9-11commission.gov/staff_statements/staff_statement_11.pdf> (12 Dec. 2005).

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

[71] John Lasker, "Watchdogs Sniff Out Terror Sites," *Wired News*, 25 February 2005, <http://www.wired.com/news/privacy/0,1848,66708,00.html> (12 Dec. 2005).

[72] John R. Bradley, "Website Postings Give Away Terror Activities," *The Straits Times*, 5 May 2004, <http://www.asiamedia.ucla.edu/article.asp?parentid=10916> (12 Dec. 2005).

[73] *Staff Statement No. 9. Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11* (Washington DC: 9/11 Commission, 2004), 8, <http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf> (12 Dec. 2005).

[74] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill Osborne, 2003), 220.

[75] *Staff Statement No. 11, The Performance of the Intelligence Community*, 10.

[76] Bernhard Warner, "Experts Comb Web for Terror Clues," *The Washington Post*, 12 November 2003, <http://cryptome.org/web-panic.htm> (12 Dec. 2005); see also Associated Press, "Man Hijacks Al-Qaeda Site for FBI Use," *USA Today*, 30 July 2002, <http://www.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm> (12 Dec. 2005).

[77] Stephanie Gruner and Gautam Naik, "Extremist Sites under Heightened Scrutiny," *The Wall Street Journal Online*, 8 October 2001, <http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn> (12 Dec. 2005); Richard Norton-Taylor, "MI5 Posts Terror Appeal on Arab Websites," *The Guardian*, 26 October 2001.

[78] Pew Internet and American Life Project, *One Year Later: September 11 and the Internet* (Washington DC: Pew Internet and American Life Project, 2002), 33-37, <http://www.pewinternet.org/pdfs/PIP_9-11_Report.pdf> (12 Dec. 2005).

[79] Lucy A. Dalglish, Gregg P. Leslie, and Phillip Taylor, eds., *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know* (Arlington, VA: The Reporters Committee for Freedom of the Press, 2002), 25, <http://www.rcfp.org/news/documents/Homefront_Confidential.pdf> (12 Dec. 2005); Pew Internet and American Life Project, *One Year Later: September 11 and the Internet*, 8-9; see also John C. Baker, 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), <http://www.rand.org/publications/MG/MG142/>.

[80] Dalglish, Leslie, and Taylor, *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know*, 2; Guy Gugliotta, "Agencies Scrub Web Sites of Sensitive Chemical Data," *Washington Post*, 4 October 2001, A29, <//www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A2738-2001Oct3>(12 Dec. 2005); Pew Internet and American Life Project, *One Year Later: September 11 and the Internet*, 8-9; Julia Scheeres, "Suppression Stifles Some Sites," *Wired*, 25 October 2001, <http://www.wired.com/news/business/0,1367,47835,00.html>(12 Dec. 2005).

[81] Dorothy Denning, *Is Cyber Terror Next?* (New York: US Social Science Research Council, 2001), 1, <http://www.ssrc.org/sept11/essays/denning.htm> (12 Dec. 2005); National Infrastructure Protection Center, *NIPC Daily Report*, 18 October 2001.

[82] Charles Hauss and 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).

[83] Hauss and Samuel, "What's the Internet Got to Do with It? Online Responses to 9/11;" National Infrastructure Protection Center, *Cyber Protests Related to the War on Terrorism: The Current Threat* (Washington DC: National Infrastructure Protection Center, 2001), <http://www.iwar.org.uk/cip/resources/nipc/cyberprotestupdate.htm> (12 Dec. 2005).

[84] Institute for Security Technology Studies (ISTS), *Cyber Attacks during the War on Terrorism: A Predictive Analysis* (Dartmouth College: Institute for Security Technology Studies, 2001), <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm> (12 Dec. 2005).

[85] In Hebrew, 'Haganah' means defense. Internet Haganah is online at <www.haganah.org.il/haganah/index.html> (12 Dec. 2005).

[86] The SITE Web site is at <http://www.siteinstitute.org/> (12 Dec. 2005).

[87] Lasker, "Watchdogs Sniff Out Terror Sites."

[88] Lasker, "Watchdogs Sniff Out Terror Sites."

[89] Arquilla, Ronfeldt, and Zanini, "Networks, Netwar and Information-Age Terrorism," 66; Charles Piller, "Terrorists Taking Up Cyberspace," *Los Angeles Times*, 8 February 2001, A1.

**MAURA CONWAY** is a Lecturer in the School of Law & Government at Dublin City University and a PhD candidate in the Department of Political Science at Trinity College Dublin, Ireland. Her research interests are in the area of terrorism and the Internet. She is particularly interested in cyberterrorism and its portrayal in the media, and the functioning and effectiveness of terrorist Web sites. Along with a number of book chapters, Maura has also published in *First Monday*, *Current History*, the *Journal of Information Warfare*, and elsewhere. *Address for Correspondence*: Department of Law & Government, Dublin City University, Glasnevin, Dublin 9, Ireland; *E-mail*: maura.conway@dcu.ie.