Maura Conway

Department of Political Science
1, College Green
Trinity College
Dublin 2
Ireland

conwaym@tcd.ie

Reality Bytes:
Cyberterrorism and Terrorist 'Use' of the Internet

ABSTRACT
This paper examines the concept of cyberterrorism. Fringe activity on the Internet ranges from non-violent 'Use' at one end to 'Cyberterrorism' at the other. Rejecting the idea that cyberterrorism is widespread, the focus here is on terrorist groups' 'use' of the Internet, in particular the content of their websites, and their 'misuse' of the medium, as in hacking wars, for example. Terrorist groups' use of the Internet for the purpose of inter-group communication is also surveyed, partly because of its importance for the inter-networked forms of organisation apparently being adopted by these groups, but also due to the part played by the Internet in the events of 9-11 and their aftermath.

Contents

Introduction

Analysts have been saying for some time now that the new terrorism depends on the information revolution and its technologies.

> Indeed, terrorism has long been about "information"—from the fact that trainees for suicide bombings are kept from listening to international media, through the ways that terrorists seek to create disasters that will consume the front pages, to the related debates about countermeasures that would limit freedom of the press, increase public surveillance and intelligence gathering, and heighten security over information and communications systems. Terrorist tactics focus attention on the importance of information and communications for the functioning of democratic institutions; debates about how terrorist threats undermine

> democratic practices may revolve around freedom of information issues (Arquilla, Ronfeldt & Zanini 1999, 72; see also Arquilla & Ronfeldt 2001).

Of course, the increase in information, communication, and communication technologies is not simply impacting terrorist groups. Information is the new lifeblood of the international system. World politics today transcends simple inter-national relations, and much of the change has taken place as a result of the spread of information infrastructures (Luke 2001, 113). The information revolution is driving dramatic changes in political, diplomatic, military, economic, social, and cultural affairs. In the second half of the twentieth century, economically advanced countries made the shift into what has been termed the 'information society' or the 'information age.' The futurist Alvin Toffler has labelled this transition the 'Third Wave' (1980), suggesting that it will ultimately be as consequential as the two previous waves in human history: from hunter gatherer to agricultural societies, and from agricultural to industrial ones. The rapid expansion and diffusion of new International Communications Technologies (ICTs), particularly evident in the growth of the Internet, contribute to the set of phenomena collectively labelled globalisation and cut across traditional temporal and spatial boundaries.

In particular, both sub-state and non-state actors are said to be harnessing- or preparing to harness- the power of the Internet to harass and attack their foes. In newspapers and magazines, in film and on television, 'cyberterrorism' is in the zeitgeist. As early as 1996 John Deutch, former director of the Central Intelligence Agency (CIA), testified:

> International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means. Since the possibilities for attacks are not difficult to imagine, I am concerned about the potential for such attacks in the future. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb -- directed in this instance against, say, a telephone switching centre or other communications node -- to electronic means of attack. The latter methods could rely on paid hackers. The ability to launch an attack, however, are likely to be within the capabilities of a number of terrorist groups, which themselves have increasingly used the Internet and other modern means for their own communications. The groups concerned include such well-known, long-established organizations as the Lebanese Hizballah, as well as nameless and less well-known cells of international terrorists such as those who attacked the World Trade Center (Deutch 1996).

The Internet is neither simply a potential vehicle for carrying out attacks nor a potential target, however. The Internet is also the instrument of a political power shift. It is the first many-to-many communication system. The ability to communicate words, images, and sounds, which underlies the power to persuade, inform, witness, debate, and discuss (not to mention the power to slander, propagandise, disseminate bad or misleading information, engage in misinformation and/or disinformation, etc.) is no longer the sole province of those who own or control printing presses, radio stations, or television networks. Every machine connected to the Internet is potentially a printing press, a broadcasting station, or a place of assembly. And in the twenty first century, terrorists are availing of the opportunity to connect. The Internet is an ideal propaganda tool for terrorists: in the past they had to communicate through acts of violence and hope that those acts garnered sufficient attention to publicise the perpetrators cause or explain their ideological justification. With the advent of the Internet, however, the same groups can disseminate their information undiluted by the media and untouched by government sensors. In 1999 it was reported that 12 of the 30 terrorist groups deemed Foreign Terrorist Organisations (FTOs) by the United States Department of State had their own websites (McGirk 1999). Today, a majority of the 33 groups on the same list have an online presence (see Table 1).[1]

On Wednesday morning, 12 September 2001, you could still visit a Web site that integrated three of the wonders of modern technology: the Internet, live digital video, and New York City's World Trade Center. The site allowed Internet users worldwide to appreciate what millions of tourists have thrilled to since Minoru Yamasaki's architectural wonder was completed in 1973: the stunning 45-mile view from the top of the Trade Center towers. According to journalists, the caption on the site still read 'Real-Time Hudson River View from World Trade Center.' In the square above was a deep black nothingness. The terrorists had taken down the Towers; they had not taken down the Net. "[W]hereas hacktivism is real and widespread, cyberterrorism exists only in theory. Terrorist groups are using the Internet, but they still prefer bombs to bytes as a means of inciting terror," wrote Dorothy Denning (2001b) just weeks before the September attacks. Terrorist 'use' of the Internet has been largely ignored, however, in favour of the more headline-grabbing 'cyberterrorism.' The purpose of this paper is to help remedy that deficiency.

To that end, this paper examines the concept of cyberterrorism. It posits a four-tiered representation of fringe activity on the Internet ranging from 'Use' at one end to 'Cyberterrorism' at the other. Rejecting the idea that cyberterrorism is widespread, the focus here is on terrorist groups' 'use' of the Internet, in particular the content of the groups' websites, and their 'misuse' of the medium, as in hacking wars, for example. Terrorist groups' use of the Internet for the purpose of inter-group communication is also investigated. In this context, there is a brief exploration of the inter-networked forms of organisation apparently being adopted by these groups, followed by an analysis of the part played by the Internet in the events of 9-11 and their aftermath.

What is Cyberterrorism?

Cyberterrorism remains a term that lacks a clear, widely-accepted definition. The pejorative connotations of the terms 'terrorism' and 'terrorist' have resulted in some acts of computer abuse being labelled 'cyberterrorism'. In June 2001, for example, a headline in the *Boston Herald* read 'Cyberterrorist Must Serve Year in Jail' (Richardson 2001). The story continued: "Despite a Missouri cyberterrorists plea for leniency, a Middlesex Superior Court judge yesterday told the wheelchair-bound man 'you must be punished for what you've done' to Massachusetts schoolchildren and ordered him to serve a year in jail." Christian Hunold, 21, pleaded guilty to "launching a campaign of terror via the Internet" from his Missouri home, including directing Middle School students to child pornography Web sites he posted, telephoning threats to the school and to the homes of some

Table 1. **United States Foreign Terrorist Organisations 2002: Websites***

Organisation	**URL****	**Language(s)**
1. Abu Nidal Organisation (ANO)	N/A	N/A
2. Abu Sayyaf Group (ASG)	N/A	N/A
3. Al-Aqsa Martyrs Brigade	N/A	N/A
4. Armed Islamic Group (GIA)	N/A	N/A
5. Asbat al-Ansar	N/A	N/A
6. Aum Supreme Truth (Aum)	http://www.aleph.to/index_e.html http://www.aleph.to	English Japanese
7. Basque Homeland and Liberty (ETA)	http://www.contrast.org/mirrors/ehj/index.html http://www.batasuna.org/	English Basque
8. Al-Gama'a al-Islamiyya (Islamic Group)	http://www.azzam.com	English
9. Hamas	http://www.palestine-info.com/hamas	Arabic, English
10. Harakat ul-Mujahidin (HUM)	http://www.ummah.net.pk/harkat/	Arabic, English
11. Hizbollah	http://www.hizbollah.org	Arabic, English
12. Islamic Movement of Uzbekistan	N/A	N/A
13. Jaish-e-Mohammed	N/A	N/A
14. Al-Jihad (Egyptian Islamic Jihad)	N/A	N/A
15. Kahane Chai (Kach)	http://www.kahane.org	English
16. Kurdistan Workers Party (PKK)	http://www.pkk.org/index.html	Kurdish
17. Lashkar-e-Tayyiba	http://www.markazdawa.org.pk/	Arabic, English
18. Liberation Tigers of Tamil Eelam	http://www.eelamweb.com/	English
19. Mujahedin-e Khalq Organization	http://www.iran-e-azad.org/english/index.html	English
20. National Liberation Army (ELN), Colombia	http://www.eln-voces.com/	Spanish
21. Palestine Islamic Jihad (PIJ)	http://www.entifada.net/	Arabic
22. Palestine Liberation Front (PLF)	N/A	N/A
23. Popular Front for the Liberation of Palestine (PFLP)	http://www.pflp-pal.org/main.html	English
24. Popular Front for the Liberation of Palestine- General Command (PFLP-GC)	N/A	N/A
25. al-Qaida	http://www.alneda.com	Arabic
26. Real IRA	N/A	N/A
27. Revolutionary Armed Forces of Colombia (FARC)	http://www.farc-ep.org/	English, Spanish, Portuguese, Italian, German, Russian
28. Revolutinary Nuclei (formerly ELA)	N/A	N/A
29. Revolutionary Organization 17 November (17 November)	N/A	N/A
30. Revolutionary People's Liberation Party/Front (DHKP/C, Dev Sol)	http://www.ozgurluk.org	English
31. Salafist Group for Call and Combat	N/A	N/A
32. Sendero Luminoso (Shining Path)	http://www.csrp.org/	Spanish, English
33. United Self-Defense Forces of Colombia (AUC)	http://colombia-libre.org/colombialibre/pp.asp	Spanish

* Lists the 33 groups that were designated by the United States Secretary of State as Foreign Terrorist Organisations (FTOs) as of April 30, 2002, pursuant to section 219 of the Immigration and Nationality Act, as amended by the Effective Death Penalty Act of 1996.

** Some groups maintain more than one website; the URLs listed here are the group's official pages as far as is practicable.

children, and posting a picture of the school’s principal with bullet holes in his head and chest on the Net. But is this cyberterrorism? And if not, why not?

Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term ‘cyberterrorism’ in the 1980s. The concept is composed of two elements: cyberspace and terrorism. Cyberspace may be conceived of as “that place in which computer programs function and data moves” (Collin 1996). Terrorism is a less easily defined term. In fact, most scholarly texts devoted to the study of terrorism contain a section, chapter, or chapters devoted to a discussion of how difficult it is to define the term (see Gearty 1991; Guelke 1998; Hoffman 1998; Holms 1994; Schmid & Jongman 1988; Wardlaw 1982). In this paper I will employ the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d).[2] That statute contains the following definition:

> The term ‘terrorism’ means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.

Combining these definitions results in the construction of a narrowly drawn working definition of cyberterrorism as follows:

> cyberterrorism refers to premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against non-combatant targets (Denning 1999, 2 & 27; Pollitt n.d.).

A similar definition of cyberterrorism has been put forward by Professor Dorothy Denning in numerous articles and interviews, and in her testimony on the subject before the United States Congress’s House Armed Services Committee (Denning 2001, 2000a, 2000b, 1999). According to Denning:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

When it comes to discussion of cyberterrorism, there are two basic areas in which clarification is needed. One has to do with the confusion between cyberterrorism and cybercrime. Such confusion is partly caused by the lack of clear definitions of the two phenomena. A UN manual on IT-related crime recognises that, even after several years of debate among experts on just what constitutes cybercrime and what cyberterrorism, “there is no internationally recognised definition of those terms” (Mates 2001). The second has to do with making clear distinctions between two different facets of terrorist usage of information technology: terrorist use of computers as a facilitator of their activities, and terrorism involving computer technology as a weapon or target. Utilising the definitions outlined above, it is possible to resolve both difficulties. Cybercrime and cyberterrorism are not coterminous. Cyberspace attacks must have a 'terrorist' component in order to be labelled cyberterrorism. The attacks must instil terror as commonly understood (that is, result in death and/or large-scale destruction), and they must have a political motivation. As regards the distinction between terrorist use of information technology and terrorism involving computer technology as a weapon/target, only the latter may be defined as cyberterrorism. Terrorist 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that: 'use.'

Kent Anderson, senior vice-president of IT security and Investigations for information security firm Control Risks Group, has devised a three-tiered schema for categorising fringe activity on the Internet, utilising the terms 'Use,' 'Misuse,' and 'Offensive Use.' Anderson explains:

> Use is simply using the Internet/WWW to facilitate communications via e-mails and mailing lists, newsgroups and websites. In almost every case, this activity is simply free speech…Misuse is when the line is crossed from expression of ideas to acts that disrupt or otherwise compromise other sites. An example of misuse is Denial-of-Service (DoS) attacks against websites. In the physical world, most protests are allowed, however, [even] if the protests disrupt other functions of society such as train service or access to private property…The same should be true for online activity. Offensive use is the next level of activity where actual damage or theft occurs. The physical world analogy would be a riot where property is damaged or people are injured. An example of this type of activity online is the recent attack on systems belonging to the world economic forum, where personal information of high profile individuals was stolen (Weisenburger 2001, 2).

Combining Anderson's schema with the definition of cyberterrorism outlined above it is possible to construct a four-level scale of the uses of the Internet for political activism by unconventional actors, ranging from 'Use' at one end of the spectrum to 'Cyberterrorism' at the other. Unfortunately, such a schema has not generally been employed in the literature nor in the field of public policy. This is particularly disquieting given that the vast majority of terrorist activity on the Internet is limited to 'Use.'

'Use' and 'Misuse': Some Empirical Observations

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 (Arquilla, Ronfeldt & Zanini 1999, 66; Piller 2001). The most popular terrorist sites draw tens of thousands of visitors each month.

Hizbollah,[5] a Lebanese-based Shi'ite Islamic group, established their collection of websites in 1995. They currently manage three such sites: one for the Central Press Office, another to describe its attacks on Israeli targets,[6] and the last Al Manar TV for news and information.[7] All three may be viewed in either English or Arabic.[8] The Central Press Office site contains an introduction to the group, press cuttings and statements, political declarations, and speeches of the group's Secretary General. One may also access a photo gallery, video and audio clips. The information contained in these pages is updated regularly. In the event that one would like to find out more, contact information, in the form of an e-mail address, is provided. In a similar vein, Hamas' Web site presents political cartoons, streaming video clips and photomontages depicting the violent deaths of Palestinian children.[9] It has been claimed that the Armed Islamic Group (GIA), a fundamentalist sect warring with the Algerian government, posted a detailed bomb-making manual on their site.[10] The online home of the Tamil Tigers (LTTE), a liberation army in Sri Lanka best known for the 1991 assassination of former Indian Prime Minister Rajiv Ghandi, offers position papers, daily news, an online store- for sale are books and pamphlets, videos, audio tapes, CDs, a 2002 calendar, and the Tamil Eelam flag- and free e-mail services. Other terrorist sites host electronic bulletin boards, post tips on smuggling money to finance their operations, and provide automated registration for e-mail alerts.

Many terrorist group sites are hosted in the United States. For example, a Connecticut-based ISP was providing co-location and virtual hosting services for the Hamas site in data centers located in Connecticut and Chicago (Lyman 2002). While sites such as that maintained by Hamas are likely to be subject to more intense scrutiny following the September attacks, similar websites were the subject of debate in the United States previous to the events of 9-11. In 1997 controversy erupted when it was revealed that the State University of New York (SUNY) at Binghampton was hosting the website of the Revolutionary Armed Forces of Colombia (FARC) and a Tupac Amaru (MRTA) solidarity site was operating out of the University of California at San Diego (UCSD). SUNY officials promptly shut down the FARC site. In San Diego it was decided to err on the side of free speech and the Tupac Amaru site remains in operation (Collier 1997).[11] Interestingly, the FARC site now also operates out of UCSD. It is not illegal to host such a site, even if a group is deemed an FTO by the United States Department of State, as long as a site is not seeking financial contributions nor providing financial support to the group. Other content is generally considered to be protected speech under the First Amendment of the Constitution of the United States.

It's not all plain sailing for these 'netizens', however. Their homepages have been subject to intermittent DoS and other hack attacks and there have also been strikes against their Internet Service Providers (ISPs) that have resulted in more permanent difficulties. In 1997, for example, an e-mail bombing was conducted against the Institute for Global Communications (IGC),[12] a San Francisco-based ISP, hosting the Web pages of the Euskal Herria or Basque Country Journal, a publication edited by supporters of the Basque group Homeland and Liberty (ETA). The attacks against IGC commenced following the assassination by ETA of a popular town councillor in northern Spain. The protestors wanted the site pulled from the Internet. To accomplish this they bombarded IGC with thousands of spurious e-mails routed through hundreds of different mail relays, spammed IGC staff and customer accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against other organisations using IGC services. IGC pulled the Euskal Herria site on July 18, but not before archiving a copy of the site enabling others to put up mirrors. Shortly thereafter, mirror sites appeared on half a dozen servers on three continents. Despite this, the protestors e-mail action raised fears of a new era of censorship imposed by direct action from anonymous hacktivists. Furthermore, approximately one month after IGC pulled the controversial site off its servers, Scotland Yard's Anti-Terrorist Squad shut down Internet Freedom's UK Web site for hosting the journal. Scotland Yard claimed to be acting against terrorism (Denning 1999, 20-21).[13]

The so-called 'cyberwar' that raged between Israelis and Palestinians and their supporters in 2000 was a mere nuisance in comparison with such targeted and sustained campaigns. The Mideast 'cyberwar' began on November- about three weeks after Hizbollah seized three Israeli soldiers on patrol in the Sheba'a Farms area of south Lebanon and held them for ransom- when pro-Israeli hackers created a website to host FloodNet attacks. Within days, Hizbollah's site was flooded by millions of 'pings'- the cyber-equivalent of knocks on the door- and crashed. Hezbollah then tried reviving the site under slightly different spellings, but they too came under sustained attack. In all, six different Hizbollah sites, the Hamas site, and other Palestinian informational sites were victims of the FloodNet device (Gentile 2000a, 2000b; Hockstader 2000). Hizbollah's Central Press Office site came under attack once again when the group posted video clips of Israeli ground attacks on Palestinians in Gaza. Hizbollah then increased their server capacity in order to ward off further attacks (Gentile 2000a). These efforts notwithstanding, pro-Israeli hackers successfully hacked into the Hizbollah Web site a further time on December 26. They posted pictures of the 3 Israeli soldiers who were abducted in early October and the slogan "Free Our Soldiers Now" on a screen full of blue and white Star of David flags (Hosein 2001).[14] In addition, a group called Hackers of Israel Unite allegedly crashed the Almanar TV site using one computer with a 56K modem, an ADSL line, and a popular tool called WinSmurf that enables one to conduct a mass pinging (Gentile 2000b).

According to Hizbollah's then-Webmaster, Ali Ayoub, "Our counterattack is just to remain on the Net" (Hosein 2001). The Palestinians and their supporters were not long in striking back, however. In a coordinated counterattack, the Web sites of the Israeli army, Foreign Ministry, prime minister and parliament, among others were hit (Hockstader 2000). On a single day, December 29, 80 Israel-related sites were hacked and defaced by pro-Palestinian hackers. It is estimated that, in all, more than 246 Israeli-related sites were attacked between October 2000 and 1 January 2001 as compared with approximately 34 Palestinian-related sites that were hit in the same period (Hosein 2001). The success of the Palestinian counterattack-variously dubbed the 'e-jihad,' 'cyber-jihad,' or 'inter-fada'- may be explained by the way in which the pro-Palestinian hackers systematically worked their way through sites with dot-il domain names. Palestinian-related sites are generally harder to find because, although in March 2000 dot-ps was delegated the country code Top Level Domain (ccTLD) for the Occupied Palestinian Territories, only one such domain is currently operational (gov.ps) (see Cisneros 2001),[15] and not many groups have such easily identifiable URLs as Hezbollah. In addition, there are approximately 2 million Internet hookups in

Israel, which is considerably more than any other Middle Eastern country (see Table 1). The upshot of this is that the Israeli's have a far greater online presence than the Palestinians and their supporters in the Arab world and are therefore more easily targeted.

(Inter)Networking and 9-11

In their recent work Rand's John Arquilla, David Ronfeldt, and Michele Zanini point to the emergence of new forms of terrorist organisation attuned to the information age. 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, Ronfeldt & Zanini 1999, 41). This type of organisational structure is qualitatively different from traditional hierarchical designs. In the future, terrorists are likely to be organised to act in a more fully networked, decentralised, "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 realise its potential, such a network must utilise the latest information and communications technologies. The Internet is becoming an integral component of such organisations, according to the Rand analysts (Arquilla, Ronfeldt & Zanini 1999, 48-53; Arquilla & Ronfeldt 2001).

The militias or patriot movement in the United States are known to have adopted inter-networked forms of organisation similar to those outlined above. While the anonymity of the Internet is seen as fuelling the conspiracies of the militias, for the groups themselves access to such new technologies is seen as a vital tool for recruitment and funding (in a similar way to terrorist organisations). The Internet has enabled the militias to spread their ideas worldwide. There are militias in Australia and Canada, and it has been suggested that the Far Right in Europe has adopted the idea of 'leaderless resistance' via the Internet (Mulloy 1999, 16; see also Hoffman 1998, 105-120 and Levin 2002, 964-966). Activists within the patriot movement have repeatedly urged their compatriots, not only to organise themselves along networked lines, however, but also to opt out of other more pervasive networks that are viewed as dangerously perceptible to attack: "We need to set up our own cashless societies, our own barter networks, and unhook from the grid, to become self-sufficient, away from the power company, the gas company, and the water company" (Mulloy 1999, 324; see also Arquilla & Ronfeldt 2001). At the same time that the militias are unhooking from the grid, however, it is asserted that terrorist groups are more networked than ever before.

The adoption of such inter-networked forms of organisation by terrorist groups has not been sufficiently researched. However, since the events of 9-11 a clearer picture has begun to emerge of the way in which the Internet might be used to support such organisational structures. The abilities of intelligence officials to eavesdrop on e-mail and phone calls, was supposed to help prevent attacks such as those that occurred in New York and Washington from ever coming to successful fruition, but they did not and, as a result, assumptions about the role the Internet can play in fighting terrorism are being revised. Investigators are now turning to Internet tools in their investigation as never before (Schwartz 2001). What role has the Internet played in the investigation of the attacks thus far? Importantly, what can be done online to track the group depends in large part on what the group did online. In a briefing given in late September, FBI Assistant Director Ronald Dick, head of the United States National Infrastructure Protection Center (NIPC),[16] told reporters that the hijackers had used the Net, and "used it well."

In the immediate aftermath of the attacks federal agents issued subpoenas and search warrants to just about every major Internet company, including America Online, Microsoft, Yahoo, Google, and many smaller providers. It is known that the hijackers booked at least nine of their airline tickets for the four doomed flights online at least two to three weeks prior to the attacks. They also used the Internet to find information about the aerial application of pesticides. Investigators are said to have in their possession hundreds of e-mails linked to the terrorists in English, Arabic and Urdu. The messages were sent within the United States and internationally. According to the FBI, a number of these messages include operational details of the attacks. Some of the hijackers used e-mail services that are largely anonymous- Hotmail, for example- and created multiple temporary accounts. A number of them are known to have used public terminals, in libraries and elsewhere, to gain access to the Net, whereas others used privately owned personal or laptop computers to do so (Cohen 2001; Fallis & Cha 2001, A24).

In two successive briefings, senior FBI officials stated that the agency had found no evidence that the hijackers used electronic encryption methods to communicate on the Internet. This has not prevented politicians and journalists repeating lurid rumours that the coded orders for the attacks were secretly hidden inside pornographic Web images (Cohen 2001; Gibson 2001; Lyman 2001), or from making claims that the attacks could have been prevented had Western governments been given the power to prevent Internet users from employing encryption in their communications[17] (Cha 2001b). Although many e-mail messages sent to and from key members of the hijack teams were uncovered and studied, none of them, according to the FBI, used encryption. Nor did they use steganography, a technique which allows an encrypted file to be hidden inside a larger file (such as a '.jpeg' or '.gif' image, or an '.mp3' music file). Evidence from questioning terrorists involved in previous attacks, both in America and on American interests abroad, and monitoring their messages reveals that they simply used code words to make their communications appear innocuous to eavesdroppers.

Arquilla, Ronfeldt, and Zanini have also pointed to the way in which difficulties coping with terrorism will increase if terrorists move beyond isolated attacks towards new approaches that emphasise campaigns based on swarming. They point out that while little analytic attention has been paid to swarming, it is likely to be a key mode of conflict in the information age (1999, 41). In their *Countering the New Terrorism*, Arquilla *et al* describe this new technique thus:

> Swarming occurs when the dispersed nodes of a network of small (and perhaps some large) forces converge on a target from multiple directions. The overall aim is the *sustainable pulsing* of force or fire. Once in motion, swarm networks must be able to coalesce rapidly and stealthily on a target, then dissever and redisperse, immediately ready to recombine for a new

> pulse. In other words, information age attacks may come in ‘swarms’ rather than the more traditional ‘waves’ (1999, 53-54).

This device points to the adaptable, flexible, and versatile nature of offensive networks with regard to opportunities and challenges. The fact that the 9-11 hijackers employed a technique similar to the one described above has given the Rand analysts’ work a far higher profile than might otherwise have been expected. Far from being innovative or under-utilised, however, swarming has been employed by hacktivists- including those acting in support of terrorist organisations- for some time. As Dorothy Denning has pointed out, cases such as that involving the *Euskal Herria Journal* and other similar incidents illustrate the power of such tools. Despite the ISPs willingness to host the site, IGC simply could not sustain the attack and remain in business. On the other hand, such cases also illustrate the power of the Internet as an organ of free speech: because venues for publication on the Internet are so rich and diverse and dispersed throughout the world, it is extremely difficult for hacktivists and governments alike to banish from the Net content they deem offensive using swarming or any other techniques (Denning 1999, 21).

The Internet and 9-11: The Aftermath

Authorities have been keeping a watchful eye on Web sites perceived as extremist for a number of years. In February 1998, Dale Watson, chief of the International Terrorism section of the FBI, informed a United States Senate committee that major terrorist groups used the Internet to spread propaganda and recruit new members (Gruner & Naik 2001; Liu 2001). Previous to 9-11, however, the authorities were not entitled to interfere with such sites for legal reasons. Since that time, the FBI have been involved in the official closure of what appears to be hundreds- if not thousands- of sites. Several radical Internet radio shows, including IRA radio, Al Lewis Live and Our Americas, were pulled by an Indiana ISP in late September 2001 after they were contacted by the FBI and advised that their assets could be seized for promoting terrorism. The New York-based IRA Radio was accused of supporting the Real IRA. The site contained an archive of weekly radio programmes said to back the dissident Irish republicans. The archive of political interviews from the programme Al Lewis Live, hosted by iconoclastic actor/activist Lewis,[18] drew some 15,000 hits a day. Our Americas was a Spanish-language programme about rebels in Latin America (Kornblum 2001; Scheeres 2001).[19] Yahoo! has pulled dozens of sites in the *Jihad* Web Ring, a coalition of 55 *jihad*-related sites, while Lycos Europe established a 20-person team to monitor its websites for illegal activity and to remove terrorist-related content (Gruner & Naik 2001; Scheeres 2001).

In August 2001, the Taliban outlawed the use of the Internet in Afghanistan, except at the fundamentalist group’s headquarters. The Taliban, nevertheless, maintained a prominent home on the Internet despite United Nations sanctions, retaliatory hack attacks, and the vagaries of the United States bombing campaign. The unofficial Web site of Dharb-i-Mumin, an organisation named by the United States on a list of terrorist groups, is still operational.[20] Another site, entitled ‘Taliban Online,’ contained information including instructions on how to make financial donations, or donations of food and clothing, to the Afghan militia, but is no longer operational. In addition, a United States-based Web site operated by the group was shut down in late

September 2001 following a request from the United States Treasury Department to the group’s Kansas City-based ISP (NIPC 2001c, 1).

One of the larger *jihad*-related sites still in operation is Azzam.com.[21] The site is run by Azzam Publications a London-based publisher. The Azzam site is available in more than a dozen languages and offers primers including ‘How Can I Train Myself for *Jihad*.’ A number of Azzam’s affiliates were shut down after people complained to the ISPs hosting the sites (at least one, following a request from the FBI). The British company Swift Internet, which was the technical and billing contact for an Azzam site, is said to have received threatening e-mails accusing it of supporting a terrorist website. Swift has since distanced itself from the site by removing its name as a contact on public Internet records. Meanwhile, as often as the site is shut down, it is replaced by a substitute/mirror site under a different URL. Said the Azzam spokesperson: “One cannot shut down the Internet” (Gruner & Naik 2001).

At the present time American officials are said to be searching the Internet for the reappearance of an Arabic language website that they believe has been used by al-Qaida. Statements ostensibly made by al-Qaida and Taliban members have appeared on the site Alneda.com.[22] The site, which is registered in Singapore, appeared on Web servers in Malaysia and Texas in early June 2002, before it was shut down by American officials. The site is thought to have first appeared on the Net in early February 2002. It is expected to reappear under a numerical address in an effort to make it harder for American officials to track down. According to media accounts, the site contained audio and video clips of Osama bin Laden; pictures of al-Qaida suspects currently detained in Pakistan; a message claiming to be from al-Qaida spokesman Sualaiman Abu Ghaith, in which he warned of new attacks upon the United States; and a series of articles claiming that suicide bombings aimed at Americans are justifiable under Islamic law (Iqbal 2002; Kelley 2002). There has been media speculation that the site is being used to direct al-Qaida operational cells. According to one report the site has carried low-level operational information: in February it published the names and home phone numbers of al-Qaida fighters captured by Pakistan following their escape from fighting in Afghanistan with the aim that sympathisers would contact their families and let them know they were alive (Eedle 2002). Click on Alneda.com today and the following appears: Hacked, Tracked, and NOW Owned by the USA. The site is described as “a mostly unmoderated discussion board relating to current world affairs surrounding Islamic Jihad [*sic*] and the US led war on terrorism (plus other conflicts around the globe).” Not only does the domain name Alneda.com point to this site, but the URL Nukeafghanisatn.com also points to this discussion board.

Conclusion

In conclusion, the bulk of the evidence to date shows that terrorist groups are making widespread use if the Internet, but so far they have not resorted to cyberterrorism, or shown the inclination to move heavily in this direction. In keeping with this reality, Richard Clarke, White House special adviser for Cyberspace Security, has said that he prefers not to use the term ‘cyberterrorism,’ instead, he favours the term ‘information security’ or ‘cyberspace security,’ since at this stage terrorists have only used the Internet for propaganda, communications, and fundraising (Wynne 2002). In a similar vein, Michael Vatis, former head of the United States National Infrastructure Protection Center (NIPC), has stated that "Terrorists are already using technology for sophisticated communications and fund-raising activities. As yet we haven't seen computers being used by these groups as weapons to any significant degree, but he, like others, warns that this will probably happen in the future" (Veltman 2001). Indeed, According to a recent study, 75% of Internet users worldwide believe that 'cyberterrorists' may "soon inflict massive casualties on innocent lives by attacking corporate and governmental computer networks." The survey, conducted in 19 major cities around the world, found that 45% of respondents agreed completely that "computer terrorism will be a growing problem," and another 35% agreed somewhat with the same statement (Poulsen 2001). The problem certainly can't shrink much, hovering as it does at zero cyberterrorism incidents per year. That's not to say that cyberterrorism cannot happen or will not happen, but that, contrary to popular perception, it has not happened yet.

About the Author

Maura Conway is a PhD student in the Department of Political Science at Trinity College Dublin (TCD), Ireland. Her thesis research deals with terrorism and the Internet, and is facilitated by a Government of Ireland Scholarship. This article is based upon a paper presented at the 2002 Annual Meeting of the American Political Science Association entitled *Terrorism and Telecommunications: An Analysis of Terrorist 'Use' of the Internet*.

Notes

1. The European Union (EU) has recently updated its list of prohibited organisations (see http://ue.eu.int/pressData/en/misc/70413.pdf). Canada is the latest country to establish such a list (see http://www.sgc.gc.ca/national_security/counter-terrorism/AntiTerrorism_e.asp).

2. Title 22 of the United States Code, Section 2656f(d) may be viewed online at http://www.lii.warwick.ac.uk/uscode/22/2656f.html. This is the definition employed in the United States Department of State's annual report entitled *Patterns of Global Terrorism*. These are available online at http://www.state.gov/s/ct/rls/pgtrpt/.

3. Furthermore, ISPs in the UK may be legally required to monitor some customers' surfing habits if requested to do so by the police under the Regulation of Investigatory Powers Act 2000.

4. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was signed into law by American President George Bush in October 2001. The law gives government investigators broad powers to track wireless phone calls, listen to voicemail, intercept e-mail messages and monitor computer use, among others. I cannot enter into a discussion of the Act here due to limitations of space. However, the full text of the

Act is available at http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf (Section 1016 pertains to critical infrastructure protection). See also Johnson 2001; Matthews 2001.

5. Also Hizballah, Hezbollah, Hezbullah, Hezbollah, etc., a.k.a Islamic Jihad, Revolutionary Justice Organisation, Organisation of the Oppressed on Earth, and Islamic Jihad for the Liberation of Palestine.

6. Accessible at http://www.moqawama.tv/.

7. Online at http://www.manartv.com.

8. In addition, see http://www.nasrollah.org the home page of Sayed Hassan Nasrallah, the General Secretary of Hizbollah, in Arabic, English and French.

9. The Hamas site if off-line at time of writing.

10. I have not, as yet, been able to locate the GIA site.

11. The Tupac Amaru Solidarity Page hosted by UCSD is at http://burn.ucsd.edu/~ats/mrta.htm. The official homepage of the MRTA (in Europe) may be accessed at http://www.voz-rebelde.de. The latter page is available in English, Spanish, Italian, Japanese, Turkish, and Serbo-Croat translations. The Tupac Amaru were on the United States list of FTOs until 2001 when they were removed.

12. Online at http://www.igc.org/igc/gateway/index.html.

13. For more information on the e-mail bombing and IGC's response to it see http://www.igc.apc.org/ehj/. Also the press release issued by Internet Freedom UK in response to the shutting of their operations by Scotland Yard: http://www.fitug.de/debate/9709/msg00018.html. The group's website is located at http://www.netfreedom.org.

14. In October 2000, a number of media outlets in the United States and Europe were contacted by a group claiming that hackers had defaced a Hizbollah site. When journalists accessed the site they were greeted by the Israeli flag, Hebrew text and a tinny piano recording of Hatikva, the Israeli national anthem. This prompted several news organisations to report that Hizbollah's Central Press Office site had been defaced by pro-Israeli hackers (see Hockstader 2000; Piller 2001). Only later did it become apparent that the site at hizbolla.org (which is no longer operational) was a fraud that had been established by an unidentified individual or group using an address in Lebanon (Garrison & Grand 2001, 7).

15. The official website of the Palestinian National Authority at http://www.pna.gov.ps/ is accessible at time of writing. I have experienced difficulties accessing this site in the past.

16. The Clinton administration spearheaded the first major American effort to upgrade computer security in government and business against cybercrime. President Bill Clinton issued an order in May 1998 establishing the National Infrastructure

Protection Center, a collaboration between law enforcement, military and intelligence organisations to increase defences against computer crime. The centre also developed an information-sharing network with major industrial sectors (Schwartz 2001).

17. In Britain, Foreign Secretary Jack Straw provoked a storm of protest by suggesting on the BBC that the media and civil liberties campaigners had paved the way for the terror attacks on America by advocating free speech and favouring publicly available encryption.

18. Formerly Grandpa on the 1960s hit TV show 'The Munsters'!

19. Al Lewis Live, can still be heard on Pacifica Radio. The IRA Radio site is back online since March 2002 at http://www.iraradio.com. The other sites remain offline.

20. Online at http://dharb-i-mumin.cjb.net/.

21. The site http://www.azzam.com is accessible intermittently. Qoqaz.net (http://www.qoqaz.net) is an Azzam mirror, as is http://www.azzam.co.uk. In the event that none of these sites are online, there may be information on Azzam's new location on the site http://www.maktabah.net/home.asp.

22. The site has also appeared at the URL http://www.drasat.com.

References

Arquilla, John and David Ronfledt. 2001. 'Networks, Netwars, and the Fight for the Future,' *First Monday* Vol. 6, No. 10. http://www.firstmonday.org/issues/issue6_10/ronfeldt/index.html.

Arquilla, John, David Ronfeldt and Michele Zanini. 1999. 'Networks, Netwar and Information-Age Terrorism.' In *Countering the New Terrorism*, ed. Ian O. Lesser *et al*. California: Rand.

Collin, Barry C. 1996. 'The Future of Cyberterrorism.' Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago. http://afgen.com/terrorism1.html.

Cisneros, Oscar S. 'Dot-PS: Domain Without a Country,' *Wired*, 12 January 2001. http://www.wired.com/news/politics/0,1283,41135,00.html.

Collier, Robert. 'Terrorists Get Web Sites Courtesy of US Universities,' *San Francisco Chronicle*, 9 May 1997. http://burn.ucsd.edu/archives/ats-1/1997.May/0042.html.

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

Denning, Dorothy. 2000a. *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, May 23. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Denning, Dorothy. 2000b. 'Cyberterrorism.' *Global Dialogue*, Autumn. http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc

Denning, Dorothy. 1999. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Washington DC: Nautilus. http://www.nautilus.org/info-policy/workshop/papers/denning.html.

Deutch, John. 1996. *Statement Before the US Senate Governmental Affairs Committee (Permanent Subcommittee on Investigations)*, 25 June. http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html.

Di Maio, Paola. 2001. 'Hacktivism, Cyberterrorism or Online Democracy?' *The Information Warfare Site (IWS)*. http://www.iwar.org.uk/hackers/resources/hacktivism-europe/internet-europe.htm.

Eedle, Paul. 'Terrorism.Com,' *The Guardian* (UK), 17 July 2002. http://www.guardian.co.uk/Print/0,3858,4462872,00.html.

Garrison, Linda & Martin Grand. Ed.s. 2001. *National Infrastructure Protection Center: Highlights*, Issue 2-01. http://www.nipc.gov/publications/highlights/2001/highlight-01-02.htm.

Gearty, Conor. 1998. *Terror*. London: Faber & Faber.

Gentile, Carmen J. 'Hacker War Rages in Holy Land,' *Wired*, 8 November 2000a. http://www.wired.com/news/politics/0,1283,40030,00.html.

Gentile, Carmen J. 'Palestinian Crackers Share Bugs,' *Wired*, 2 December 2000b. http://www.wired.com/news/politics/0%2C1283%2C40449%2C00.html.

Guelke, Adrian. 1998. *The Age of Terrorism and the International Political System*. London & New York: IB Tauris Publishers.

Hockstader, Lee. 'Pings and E-Arrows Fly in Mideast Cyber-War,' *Washington Post*, 27 October 2000: A01.

Hoffman, Bruce. 1998. *Inside Terrorism*. London: Indigo.

Holms, John Pynchon. 1994. *Terrorism*. New York: Windsor Publishing Corps.

Hosein, Hanson. 'Bytes Without the Blood in Mideast,' *MSNBC*, 4 January 2001.

Iqbal, Anwar. 'Site Claims bin Laden's Message,' *United Press International* (UPI), 20 February 2002. http://www.upi.com/view.cfm?StoryID=20022002-075528-9498r.

Johnson, Bobbie. 'Farewell Web Freedom?' *The Guardian* (UK), 22 October 2001.

Kelley, Jack. 'Agents Pursue Terrorists Online,' *USA Today*, 20 June 2002. http://www.usatoday.com/life/cyber/tech/2002/06/21/terrorweb.htm.

Levin, Brian. 2002. 'A Legal and Historical Analysis of Extremists' Use of Computer Networks in America.' *American Behavioural Scientist* Vol. 45, No. 6: 958- 988.

Luke, Timothy W. 2001. 'Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism.' *Alternatives* 26(2): 113-142.

Lyman, Jay. 'Terrorist Web Site Hosted by US Firm,' *NewsFactor Network*, 3 April 2002. http://www.newsfactor.com/perl/story/17079.html.

Mates, Michael (Rapporteur). 2001. *Technology and Terrorism*. Brussels: NATO. http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm.

Matthews, William. 'Anti-Terror Law Expands Powers,' *Federal Computer Week*, 29 October 2001. http://www.fcw.com/fcw/articles/2001/1022/web-terror-10-26-01.asp.

McGirk, Tim. 'Wired for Warfare,' *Time (International)*, 11 October 1999.

Middleton, James 'US Hackers Could Face Life Sentences,' *Vnunet.com*, 28 February 2002. http://vnunet.com/News/1129590.

Mulloy, D.J. 1999. *Homegrown Revolutionaries: An American Militia Reader*. Norwich UK: Arthur Miller.

National Infrastructure Protection Center (NIPC). *NIPC Daily Report*, 11 December 2001.

Piller, Charles. 'Terrorists Taking Up Cyberspace,' *LA Times*, 8 February 2001

Pollitt, Mark. N.d. *Cyberterrorism: Fact or Fancy?* http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Poulsen, Kevin. 'Cyber Terror in the Air,' *SecurityFocus.com*, 30 June 2001

Richardson, Francis. 'Cyberterrorist Must Serve Year in Jail,' *Boston Herald*, 6 June 2001

Schmid, Alex P., and Albert J. Jongman. 1998. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*. Amsterdam: North-Holland Publishing Company.

Schwartz, John. 'When Point and Shoot Becomes Point and Click,' *The New York Times*, 12 November 2000.

Shachtman, Noah. 'Israel Blocks Palestinian ISP,' *Wired*, 16 July 2002. http://www.wired.com/news/politics/0,1283,53873,00.html.

Toffler, Alvin. 1980. *The Third Wave*. London: Pan Books.

Veltman, C. 'Beating Cyber Crime,' *The Daily Telegraph*, 1 March 2001: 12E.

Wardlaw, Grant. 1982. *Political Terrorism: Theory, Tactics, and Countermeasures*. Cambridge: Cambridge University Press.

Wynne, Jeff 'White House Advisor Richard Clarke Briefs Senate Panel on Cybersecurity,' *Washington File*, 14 February 2002. http://usinfo.state.gov/topical/global/ecom/02021401.htm.