Terrorism and IT:
Cyberterrorism and Terrorist Organisations Online[1]

Paper prepared for presentation at the International Studies Association (ISA) Annual International Convention, Portland, Oregon, USA, 25 February to 1 March, 2003.

Maura Conway

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

conwaym@tcd.ie

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 *et al*. 1999, 72; see also Arquilla and 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 international 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

[1] This paper is a reworking of two previously published articles (see Conway 2002a and 2002b). The research on which the paper is based was supported by a grant from the Irish Research Council for the Humanities and Social Sciences (IRCHSS).

termed the 'information society' or the 'information age.' The futurist Alvin Toffler (1980) has labeled this transition the 'Third Wave', 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 labeled globalization and cut across traditional temporal and spatial boundaries.

Every machine connected to the Internet is potentially a printing press, a broadcasting station, or a place of assembly. 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, propagandize, 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. And in the twenty-first century, terrorists are availing of the opportunity to connect.

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. 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 publicize 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 Organizations (FTOs) by the United States Department of State had their own Web sites (McGirk, 1999).[2] Today, a majority of the 33 groups on the same list have an online presence (see Conway 2002a, Table 1).[3] But are terrorists who operate in cyberspace 'cyberterrorists'? The answer hinges on what constitutes cyberterrorism.

Defining and Redefining Cyberterrorism

There are a number of stumbling blocks to constructing a clear and concise definition of cyberterrorism. First, a majority of the discussion of cyberterrorism has been conducted in the popular media, where the focus is on ratings and readership figures rather than establishing good operational definitions of new terms. Second, the term is subject to chronic misuse and overuse and since 9/11, in particular, has become a buzzword that can mean radically different things to different people. In addition, it has become common when dealing with computers and the Internet to create new words by placing the handle *cyber*, *computer*, or *information* before another word. This may appear to denote a

[2] On May 3, 2002, the European Union updated its list of prohibited organizations. See http://ue.eu.int/pressData/en/misc/70413.pdf. The latest country to devise such a list is Canada. See http://www.sgc.gc.ca/publications/news/20020723_e.asp.

[3] A comprehensive list of all terrorist Web sites is available on Barry Cromwell's 'Separatist, Para-Military, Military, Intelligence, and Political Organizations' site at http://www.cromwell-intl.com/security/netusers.html.

completely new phenomenon, but often it does not and confusion ensues. Finally, a major obstacle to creating a definition of cyberterrorism is the lack of an agreed-upon definition of terrorism (Embar-Seddon 2002, 1034). This does not mean that no acceptable definitions of cyberterrorism have been put forward. On the contrary, there are a number of well thought out definitions of the term available, and these are discussed below.[4] However, no single definition of cyberterrorism is agreed upon by all, in the same way that no single, globally accepted definition of classical political terrorism exists.

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; Schmid and Jongman, 1988; Wardlaw, 1982). This paper will employ the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d). 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."[5]

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.). By this definition, sending pornographic e-mails to minors, posting offensive content on the Internet, defacing Web pages, stealing credit card information, posting credit card numbers on the Internet, and clandestinely redirecting Internet traffic from one site to another do not constitute instances of cyberterrorism, contrary to what local government authorities and the press have stated (see Conway 2002c). Admittedly, terrorism is a notoriously difficult concept to define; however, the addition of computers to old-fashioned criminality it is not.

The inflation of the concept of terrorism may increase newspaper circulation, but is ultimately not in the public interest. Despite this, many have suggested adopting broader definitions of the term. In a 1997 article in the journal *Terrorism and Political Violence*, Matthew Devost, Brian Houghton and Neal Pollard defined 'information terrorism' as "the intentional abuse of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action" (1997, 75). They conceive of information terrorism as "the nexus between criminal information system fraud or abuse, and the physical violence of terrorism" (1996, 10; 1997, 76). This allows for attacks that would not necessarily result in violence against humans-- although they might incite fear-- to be characterized as terrorist. But while there is no single accepted definition of terrorism, a majority of scholars agree that it has two

[4] One of the most accessible sound bites on what defines cyberterrorism is that it is 'hacking with a body count' (Collin, quoted in Ballard *et al* 2002, 992).

[5] This is also the definition employed in the US State Department's annual report *Patterns of Global Terrorism.*

integral components: the use of force or violence and a political motivation (Guelke 1998, 19; Schmid & Jongman 1988, 5). Indeed, most domestic laws define classical or political terrorism as requiring violence or the threat to or the taking of human life for political or ideological ends. Devost, Houghton and Pollard are aware of this, but wish to allow for the inclusion of pure information system abuse (that does not employ nor result in physical violence) as a possible new facet of terrorism nonetheless (1996, 10). Others have followed their lead.

Israel's former science minister, Michael Eitan, has deemed "sabotage over the Internet" as cyberterrorism (Sher 2000). And according to the Japanese government, cyberterrorism aims at "seriously affecting information systems of private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying data" (FBIS 2002b). A report by the Moscow-based ITAR-TASS news agency states that in Russia cyberterrorism is perceived as "the use of computer technologies for terrorist purposes" (FBIS 2002a). In 1999, a report by the Center for the Study of Terrorism and Irregular Warfare (CSTIW) at the Naval Postgraduate School in Monterey, California defined cyberterrorism as the "unlawful destruction or disruption of digital property to intimidate or coerce people" (Daukantas 2001). "We shall define cyberterrorism as any act of terrorism…that uses information systems or computer technology either as a *weapon* or a *target*," stated a recent NATO brief, *Technology and Terrorism* (Mates 2001, 6). Yael Shahar, Web master at the International Policy Institute for Counter-Terrorism (ICT), located in Herzliya, Israel, differentiates between many different types of what he prefers to call 'information terrorism': 'electronic warfare' occurs when hardware is the target, 'psychological warfare' is the goal of inflammatory content, and it is only 'hacker warfare', according to Shahar, that degenerates into cyberterrorism (Hershman 2000).

John Leyden, writing in *The Register*, describes how a group of Palestinian hackers and sympathizers set up a Web site that provides one-stop access to hacking tools and viruses, and tips on how to use the tools to mount attacks on Israeli targets. According to Leyden, these hackers are using the techniques of cyberterrorism (Leyden 2000). It is clear that Leyden and others wish to conflate politically motivated hacking--so-called hacktivism-- and terrorism. Such unwarranted expansion of the concept of cyberterrorism runs contrary to the definitions outlined earlier. Advancing one step further, Johan J. Ingles-le Noble, writing in *Jane's Intelligence Review*, had this to say:

> Cyberterrorism is not only about damaging systems but also about intelligence gathering. The intense focus on 'shut-down-the-power-grid' scenarios and tight analogies with physically violent techniques ignore other more potentially effective uses of IT in terrorist warfare: intelligence-gathering, counter-intelligence and disinformation (1999, 6).

Ingles-le Noble's comments highlight the more potentially realistic and effective uses of the Internet by terrorist groups (i.e. intelligence-gathering, counter-intelligence, disinformation, etc.). However, he mistakenly labels these alternative uses 'cyberterrorism.' Consider the November 2000 electronic attack carried out from Pakistan against the American Israel Public Affairs Committee (AIPAC), a pro-Israeli lobbying group based in Washington, DC. The group's site was defaced with anti-Israeli commentary. The attacker also stole some 3,500 e-mail addresses and 700 credit card numbers, sent anti-Israeli diatribes to the addresses, and published the credit card data on

the Internet. Dr. Nuker, the Pakistani hacker who claimed responsibility for the incident, said he was a founder of the Pakistani Hackerz Club, the aim of which was to "hack for the injustice going around the globe, especially with [*sic*] Muslims." But even had Dr. Nuker broken into AIPAC's headquarters and physically stolen the credit card information and e-mail addresses, this would not be considered an act of terrorism, but a criminal undertaking. It is only acting on the information obtained to perpetrate an attack in furtherance of some political aim that could be considered terrorist.

Ingles-le Noble further contends that "disinformation is easily spread; rumors get picked up by the media, aided by the occasional anonymous e-mail." That may be so, but spreading false information whether via word-of-mouth, the print or broadcast media, or some other medium, is oftentimes not even criminal, never mind terrorist. Why should things be any different in cyberspace? Ingles-le Noble (1999) himself recognizes that:

> There is undoubtedly a lot of exaggeration in this field. If your system goes down, it is a lot more interesting to say it was the work of a foreign government rather than admit it was due to an American teenage 'script-kiddy' tinkering with a badly written CGI script. If the power goes out, people light a candle and wait for it to return, but do not feel terrified. If their mobile phones switch off, society does not instantly feel under attack. If someone cracks a web site and changes the content, terror does not stalk the streets.

Nonetheless, there is widespread concern that a catastrophic cyberterrorist attack is imminent, particularly in the wake of the events of 9/11. However, the bulk of the evidence to date shows that while terrorist groups are making widespread use of the Internet, so far they have not resorted to cyberterrorism, or shown the inclination to move heavily in that direction. Dramatic predictions to the contrary certainly make good copy, generate high ratings and sell many books and journals, but do not contribute to an intelligent, well-informed analysis of the threat of cyberterrorism.

Distinguishing Characteristics

When it comes to discussion of cyberterrorism, there are two basic areas in which clarification is needed. First, 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 recognizes that, even after several years of debate among experts on just what constitutes cybercrime and what cyberterrorism, "there is no internationally recognized definition of those terms" (Mates 2001). Second, it is useful to distinguish two different facets of terrorist use of information technology: terrorist use of computers as a facilitator of their activities, and terrorism involving computer technology as a weapon or target. Utilizing the definitions outlined above, it is possible to clarify both difficulties. Cybercrime and cyberterrorism are not coterminous. Cyberspace attacks must have a 'terrorist' component in order to be labeled cyberterrorism. The attacks must instill 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 (i.e. for the purposes of inter-group communication, propaganda, etc.) 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[6] has devised a three-tiered schema for categorizing fringe activity on the Internet, utilizing 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 (see Table 1). Unfortunately, such a schema has not generally been employed in the literature or in the legislative arena. This is particularly disquieting given that the vast majority of terrorist activity on the Internet is limited to 'Use.'

Table 1. Typology of Cyber Activism and Cyber Attacks

Action	*Definition*	*Source*	*Example*
Use	Using the Internet to facilitate the expression of ideas and communication(s)	Internet users	Emails, mailing lists, newsgroups, websites
Misuse	Using the Internet to disrupt or compromise Web sites or infrastructure	Hackers, Hacktivists	Denial-of-Service (DoS) attacks
Offensive Use	Using the Internet to cause damage or engage in theft	Crackers	Stealing data (e.g. credit card details)
Cyberterrorism	An attack carried out by terrorists either via the Internet or targeting the Internet that results in violence against persons or severe economic damage	Terrorists	A terrorist group using the Internet to carry out a major assault on the New York Stock Exchange

[6] Anderson was formerly senior vice-president of IT Security and Investigations for information security firm Control Risks Group.

'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 et al., 1999, p. 66; Piller, 2001). The most popular terrorist sites draw tens of thousands of visitors each month.

Hizbollah,[7] a Lebanese-based Shi'ite Islamic group, established their collection of Web sites in 1995. They currently manage three such sites: one for the Central Press Office,[8] another to describe its attacks on Israeli targets,[9] and the last Al Manar TV for news and information.[10] All three may be viewed in either English or Arabic.[11] 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.[12] 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.[13] 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 Gandhi, 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 Web sites were the subject of debate in the United States previous to the events of 11 September. In 1997 controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the Web site 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

---

[7] 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.
[8] Online at http://www.hizbollah.org.
[9] Accessible at http://www.moqawama.tv/.
[10] Online at http://www.manartv.com.
[11] In addition, see http://www.nasrollah.org the home page of Sayed Hassan Nasrallah, the General Secretary of Hizbollah, in Arabic, English, and French.
[12] Accessible at http://www.palestine-info.co.uk/hamas/index.htm.
[13] I have not, as yet, been able to locate the GIA site.

operation (Collier, 1997).[14] 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 (see also McCullagh 2002a & 2002b).

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),[15] 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 councilor 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 organizations using IGC services. IGC pulled the *Euskal Herria* site on 18 July 1997, 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 U.K. Web site for hosting the journal. Scotland Yard claimed to be acting against terrorism (Denning 1999, 20-21).[16]

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 Web site 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

[14] 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.

[15] Online at http://www.igc.org/igc/gateway/index.html.

[16] 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 Web site is located at http://www.netfreedom.org.

notwithstanding, pro-Israeli hackers successfully hacked into the Hizbollah Web site a further time on 26 December. They posted pictures of the three 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).[17] 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).

Also in October 2000, a number of media outlets in the US 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 (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).

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, 29 December 2000, 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),[18] and not many groups have such easily identifiable URLs as Hezbollah. In addition, there are approximately two million Internet hookups in Israel, which is considerably more than any other Middle Eastern country (see Table 2). 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.

[17] In October 2000, a group claiming that hackers had defaced a Hizbollah site contacted a number of media outlets in the United States and Europe. When journalists accessed the site the Israeli flag, Hebrew text and a tinny piano recording of Hatikva, the Israeli national anthem, greeted them. This prompted several news organizations 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 (see Garrison and Grand 2001, 7).

[18] The official Web site of the Palestinian National Authority at http://www.pna.gov.ps/ was accessible at time of writing. I have experienced difficulties accessing this site in the past.

(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 organization 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 *et al* 1999, 41). This type of organizational structure is qualitatively different from traditional hierarchical designs. In

Table 2 . Internet Users in the Middle East, 2001

Country	*Number of Subscribers*	*% of Population*
Bahrain	140,200	21.36
Iran	420,000	0.63
Iraq	12,500	0.05
Israel	1,940,000	17.12
Jordan	212,000	3.99
Kuwait	200,000	9.47
Lebanon	300,000	8.38
Oman	120,000	4.42
Palestine	60,000	N/A
Qatar	75,000	9.75
Saudi Arabia	570,000	2.5
Syria	60,000	0.35
UAE	900,000	36.79
Yemen	17,000	0.09

Source: http://www.nua.ie

the future, terrorists are likely to be organized to act in a more fully networked, decentralized, "all-channel" manner. Ideally, there is no single, central leadership, command or headquarters. Within the network as a whole there is little or no hierarchy and there may be multiple leaders depending upon the size of the group. In other words, there is no specific heart or head that can be targeted. To realize its potential, such a network must utilize the latest information and communications technologies. The Internet is becoming an integral component of such organizations, according to the Rand analysts (Arquilla *et al* 1999, 48-53; Arquilla & Ronfeldt 2001). The militias or patriot movement in the United States are known to have adopted inter-networked forms of organization 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 organizations). 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). Activists within the patriot movement have repeatedly urged their compatriots, not only to organize 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 organization 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 organizational 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. 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 2001, FBI Assistant Director Ronald Dick, head of the United States National Infrastructure Protection Center (NIPC),[19] 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 rumors that the coded orders for the attacks were secretly hidden inside pornographic Web images (Cohen, 2001; Lyman, 2002), 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 (Cha 2001, E01).[20] 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

[19] He Clinton administration spearheaded the first major US 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 organizations to increase defenses against computer crime. The center also developed an information-sharing network with major industrial sectors.

[20] 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 favoring publicly available encryption.

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 emphasize 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 (Arquilla *et al* 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' (Arquilla *et al* 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-utilized, however, swarming has been employed by hacktivists -- including those acting in support of terrorist organizations -- 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 and 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. An Indiana ISP pulled several radical Internet radio shows, including IRA radio, Al Lewis Live and Our Americas, in late September 2001 after the FBI contacted them 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 (Cobain 2001). The archive of political interviews from the programme Al Lewis Live, hosted by iconoclastic actor/activist Lewis,[21] drew some 15,000 hits a day. Our Americas was a Spanish-language programme about rebels in Latin America (Kornblum, 2001; Scheeres, 2001).[22] 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 Web sites for illegal activity and to remove terrorist-related content (Gruner and Naik, 2001; Scheeres, 2001).[23]

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 organization named by the United States on a list of terrorist groups, is still operational.[24] 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 2001, 1).

One of the larger jihad-related sites that remained in operation in the wake of 9-11 was Azzam.com. The site was run by Azzam Publications a London-based publisher. The Azzam site was available in more than a dozen languages and offered 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 Web site. 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 and Naik, 2001).

At the present time American officials are said to be searching the Internet for the reappearance of an Arabic language Web site 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.[25] The site, which is registered in Singapore, appeared on Web servers in Malaysia and Texas in early June 2002, before American officials shut it down. 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

[21] Formerly Grandpa on the 1960s hit TV show 'The Munsters'!
[22] 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.
[23] The Electronic Frontier Foundation is keeping a tally of sites that have been shut down or restricted since 9/11. The list is available at http://www.eff.org/Censorship/Terrorism_militias/antiterrorism_chill.html.
[24] Online at http://dharb-i-mumin.cjb.net/.
[25] The site has also appeared at http://www.drasat.com.

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 (AFP 2002). 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 sympathizers 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 (see also McWilliams 2002).

New Legislative Measures

In February 2001, the UK updated its Terrorism Act to classify "the use of or threat of action that is designed to seriously interfere with or seriously disrupt an electronic system" as an act of terrorism (see Di Maio 2001; Mates 2001).[26] In fact, it will be up to police investigators to decide whether an action is to be regarded as terrorism. Online groups, human rights organizations, civil liberties campaigners, and others condemned this classification as absurd, pointing out that it placed hacktivism on a par with life-threatening acts of public intimidation (Weisenburger 2001, 9).[27] Notwithstanding, in the wake of the events of 9-11, US legislators followed suit. Previous to 9/11, if one successfully infiltrated a federal computer network, one was considered a hacker. However, following the passage of the USA Act,[28] which authorized the granting of significant powers to law enforcement agencies to investigate and prosecute potential threats to national security, there is the potential for hackers to be labeled cyberterrorists and, if convicted, to face up to 20 years in prison (NIPC 2001; see also Middleton 2002 & Levin 2002, 984-985). Clearly, policymakers believe that actions taken in cyberspace are qualitatively different from those taken in the 'real' world.

It is not the Patriot Act, however, but the massive 500-page law establishing the US Department of Homeland Security that has the most to say about terrorism and the Internet. The law establishing the new department envisions a far greater role for the

[26] The full text of the UK Terrorism Act 2001 is available online at http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm.

[27] 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.

[28] 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 US 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.

United States' government in the securing of operating systems, hardware, and the Internet in the future. In November 2002, US President Bush signed the bill creating the new department, setting in train a process that will result in the largest reshuffle of US bureaucracy since 1948. At the signing ceremony, Bush said that the "department will gather and focus all our efforts to face the challenge of cyberterrorism" (as quoted in McCullagh 2002c). The Department of Homeland Security will merge five agencies that currently share responsibility for critical infrastructure protection in the United States: the FBI's National Infrastructure Protection Center (NIPC), the Defense Department's National Communications System, the Commerce Department's Critical Infrastructure Office, the Department of Energy's analysis center, and the Federal Computer Incident Response Center. The new law also creates a Directorate for Information Analysis and Infrastructure Protection whose task it will be to analyze vulnerabilities in systems including the Internet, telephone networks and other critical infrastructures, and orders the establishment of a "comprehensive national plan for securing the key resources and critical infrastructure of the United States" including information technology, financial networks, and satellites. Further, the law dictates a maximum sentence of life-imprisonment without parole for those who deliberately transmit a program, information, code, or command that impairs the performance of a computer or modifies its data without authorization, "if the offender knowingly or recklessly causes or attempts to cause death." In addition, the law allocates $500 million for research into new technologies, is charged with funding the creation of tools to help state and local law enforcement agencies thwart computer crime, and classifies certain activities as new computer crimes (Krebs 2002; McCullagh 2002c; Poulsen 2002).

Conclusion

In the space of thirty years, the Internet has metamorphosed from a US Department of Defense command-and-control network consisting of less than one hundred computers to a network that criss-crosses the globe: today, the Internet is made up of tens of thousands of nodes (i.e. linkage points) with over 105 million hosts spanning more than 200 countries. With a current (February 2003) estimated population of regular users of over 605 million people, the Internet has become a near-ubiquitous presence in many world regions. That ubiquity is due in large part to the release in 1991 of the World Wide Web. In 1993 the Web consisted of a mere 130 sites, by century's end it boasted more than one billion. In the Western world, in particular, the Internet has been extensively integrated into the economy, the military, and society as a whole. As a result, many people now believe that it is possible for people to die as a direct result of a cyberterrorist attack and that such an attack is imminent.

On Wednesday morning, 12 September 2001, you could still visit a Web site that integrated three of the wonders of modern technology: the Internet, digital video, and the World Trade Center. The site allowed Internet users worldwide to appreciate what millions of tourists have delighted in since Minoru Yamasaki's architectural wonder was completed in 1973: the glorious 45-mile view from the top of the WTC towers. According to journalists, the caption on the site still read 'Real-Time Hudson River View from World Trade Center' (O'Toole 2001). In the square above was deep black

nothingness. The terrorists hadn't taken down the Net, they had taken down the towers. "Whereas 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 (2001) just weeks before the September attacks. Terrorist 'use' of the Internet has been largely ignored, however, in favor of the more headline-grabbing 'cyberterrorism.'

In conclusion, the bulk of the evidence to date shows that terrorist groups are making widespread use of 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, former White House special adviser for Cyberspace Security, has said that he prefers not to use the term 'cyberterrorism,' instead, he favors 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 US 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 this will probably happen in the future" (Veltman 2001). According to a 2001 study, 75% of Internet users worldwide agree, they believe that 'cyberterrorists' will "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.

References

Agence France Presse (AFP). 2002. 'Investigators Watching for Suspected al-Qaida Web Site.' *Agence France Presse* 23 June.

Arquilla, J. & D. Ronfledt. 2001. 'Networks, Netwars, and the Fight for the Future.' *First Monday* 6(10), at http://www.firstmonday.org/issues/issue6_10/ronfeldt/.

Arquilla, J., D. Ronfeldt & M. Zanini. 1999. 'Networks, Netwar and Information-Age Terrorism.' In Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini & Brian Michael Jenkins, *Countering the New Terrorism.* Santa Monica, Calif.: Rand.

Ballard, J.D., J.G. Hornik, & D. McKenzie. 2002. 'Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues.' *American Behavioral Scientist* 45(6): 989-1016.

Cha, A.E. 2001. 'To Attacks' Toll Add a Programmer's Grief.' *The Washington Post* 21 September: E01.

Cobain, I. 2001. 'FBI Closes Website Linked to Real IRA.' *The Times* (London) 8 October: 8.

Cohen, Adam. 2001. 'When Terror Hides Online.' *Time* 12 November.

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

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

Conway, M. 2002a. 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet.' *First Monday* 7(11), at http://www.firstmonday.org/issues/issue7_11/conway/index.html.

Conway, M. 2002b. 'What is Cyberterrorism?' *Current History* 101(659): 436-442.

Conway, M. 2002c. 'Cyberterrorism.' Paper presented at the conference on *War and Virtual War: The Challenge to Communities*, Mansfield College, Oxford, 16-18 July.

Daukantas, P. 2001. 'Professors Hash Out Emergency Response, Cyberterrorism Strategies.' *Government Computer News* 14 December, at http://www.gcn.com/vol1_no1/daily-updates/17642-1.html.

Denning, D. 2001. 'Hacker Warriors: Rebels, Freedom Fighters, and Terrorists Turn to Cyberspace.' *Harvard International Review* Summer, at: http://www.hir.harvard.edu/archive/articles/pdf/denning.html.

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

Devost, M., B. Houghton & N. Pollard. 1997. 'Information Terrorism: Political Violence in the Information Age.' *Terrorism and Political Violence* 9(1): 72-83.

Devost, M., B. Houghton & N. Pollard. 1996. 'Information Terrorism: Can You Trust Your Toaster?' *The Terrorism Research Center*, at http://www.terrorism.com/terrorism/itpaper.html.

Di Maio, P. 2001. 'Hacktivism, Cyberterrorism or Online Democracy?' *The Information Warfare Site (IWS)* 19 March, at http://www.iwar.org.uk/hackers/resources/hacktivism-europe/internet-europe.htm

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

Embar-Seddon, A. 2002. 'Cyberterrorism: Are We Under Siege?' *American Behavioral Scientist* 45(6): 1017-1043.

Fallis, D.S. & A.E. Cha. 2001. 'Agents Following Suspects' Lengthy Electronic Trail.' *The Washington Post* 4 October: A24.

Foreign Broadcast Information Service (FBIS). 2002a. 'Russia Cracks Down on 'Cyberterrorism.'' *ITAR-TASS*, FBIS-SOV-2002-0208, 8 February.

Foreign Broadcast Information Service (FBIS). 2002b. 'Government Sets Up Anti-Cyberterrorism Homepage.' *Sankei Shimbun*, FBIS-EAS-2002-0410, 10 April.

Garrison, L. & M. Grand (Ed.s). 2001. *National Infrastructure Protection Center: Highlights*, at http://www.nipc.gov/publications/highlights/2001/highlight-01-02.htm.

Gearty, C.A. 1991. *Terror*. London: Faber and Faber.

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

Gentile, C.J. 2000b. 'Palestinian Crackers Share Bugs.' *Wired* 2 December, at

http://www.wired.com/news/politics/0%2C1283%2C40449%2C00.html.
Gruner, S. & G. Naik. 2001. 'Extremist Sites Under Heightened Scrutiny.' *The Wall Street Journal Online* 8 October, at http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn.
Guelke, A. 1998. *The Age of Terrorism and the International Political System*. London: IB Tauris Publishers.
Hershman, T. 2000. 'Cyberterrorism is Real Threat, Say Experts at Conference.' *Israel.internet.com* 11 December.
Hockstader, L. 2000. 'Pings and E-Arrows Fly in Mideast Cyber-War.' *Washington Post* 27 October: A01.
Hoffman, B. 1998. *Inside Terrorism.* London: Indigo.
Hosein, H. 2001. 'Bytes Without the Blood in Mideast.' *MSNBC* 4 January.
Ingles-le Noble, J. 1999. 'Cyberterrorism Hype.' *Jane's Intelligence Review*, at http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm.
Iqbal, A. 2002. 'Site Claims bin Laden's Message.' United Press International 20 February, at http://www.upi.com/view.cfm?StoryID=20022002-075528-9498r.
Johnson, B. 2001. 'Farewell Web Freedom?' *The Guardian* (UK) 22 October.
Kelley, J. 2002. 'Agents Pursue Terrorists Online.' *USA Today* 20 June, at http://www.usatoday.com/life/cyber/tech/2002/06/21/terrorweb.htm.
Kornblum, J. 2001. 'Radical Radio Shows Forced from the Net.' *USA Today* 25 October: 3D.
Krebs, B. 2002. 'Homeland Security Bill Heralds IT Changes.' *The Washington Post* 25 November, at http://www.washingtonpost.com/wp-dyn/articles/A54872-2002Nov14.html.
Levin, B. 2002. 'Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America.' *American Behavioral Scientist* 45(6): 958-988.
Leyden, J. 2000. 'Palestinian Crackers Give Out Tools to Attack Israelis.' *The Register* (UK) December 4, at http://www.theregister.co.uk/content/6/15199.html.
Liu, M. 2001. 'Holy War on the Web.' *Newsweek* (International) 15 October: 62.
Luke, T.W. 2001. 'Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism.' *Alternatives* 26(2): 113-142.
Lyman, J. 2002. 'Terrorist Web Site Hosted by US Firm.' *NewsFactor Network* 3 April, at http://www.newsfactor.com/perl/story/17079.html.
Mates, M. (Rapporteur). 2001. *Technology and Terrorism*. Brussels: NATO, at http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm.
Matthews, W. 2001. 'Anti-Terror Law Expands Powers.' *Federal Computer Week*, 29 October 29, at http://www.fcw.com/fcw/articles/2001/1022/web-terror-10-26-01.asp.
McCullagh, D. 2002a. 'University Bans Controversial Links.' *C¦Net News* 25 September, at http://news.com.com/2100-1023-959544.html?tag=fd_top.
McCullagh, D. 2002b. 'University Backs Down on Link Ban.' *C¦Net News* 8 October, at http://news.com.com/2100-1023-961297.html?tag=mainstry.
McCullagh, D. 2002c. 'Bush Signs Homeland Security Bill.' *CNET News* 25 November, at http://news.com.com/2102-1023-975305.html.
McGirk, T. 1999. 'Wired for Warfare.' *Time* (International) 11 October.

McWilliams, B. 2002. 'One Man's Info War on al-Qaida.' *Wired* 18 December, at http://www.wired.com/news/infostructure/0,1377,56896,00.html.
Middleton, J. 2002. 'US Hackers Could Face Life Sentences.' *Vnunet.com* 28 February, at http://www.vnunet.com/News/1129590.
Mulloy, D.J. 1999. *Homegrown Revolutionaries: An American Militia Reader*. Norwich U.K.: Arthur Miller.
National Infrastructure Protection Center (NIPC). 2001. *NIPC Daily Report: 11 December*. Washington, DC: NIPC.
Piller, C. 2001. 'Terrorists Taking Up Cyberspace.' *Los Angeles Times* 8 February: A1.
O'Toole, F. 2001. 'Terrorists Hold Levers of Control of New Kind of War.' *The Irish Times* 16 September.
Pollitt, M. n.d. 'Cyberterrorism: Fact or Fancy?' at http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.
Poulsen, K. 2001. 'Cyber Terror in the Air.' *SecurityFocus.com* 30 June.
Scheeres, J. 2001. 'Suppression Stifles Some Sites.' *Wired* 25 October, at http://www.wired.com/news/business/0,1367,47835,00.html.
Schmid, A. P. & A.J. Jongman. 1988. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*. Amsterdam: North-Holland.
Schwartz, J. 2000. 'When Point and Shoot Becomes Point and Click.' *New York Times* 12 November.
Sher, H. 2000. 'Cyberterror Should be International Crime- Israeli Minister.' *Newsbytes* 10 November.
Toffler, A. 1980. *The Third Wave.* London: Pan Books.
Veltman, C. 2001. 'Beating Cyber Crime.' *Daily Telegraph* 1 March: 12E.
Wardlaw, G. 1982. *Political Terrorism: Theory, Tactics, and Countermeasures.* Cambridge: Cambridge University Press.
Weisenberger, K. 2001. 'Hacktivists of the World, Divide.' *SecurityWatch.com* 23 April, at: http://www.securitywatch.com/TRE/042301.html.
Wynne, J. 2002. 'White House Advisor Richard Clarke Briefs Senate Panel on Cybersecurity.' *Washington File* 14 February, at http://usinfo.state.gov/topical/global/ecom/02021401.htm.