Cyberterrorism: The Story So Far

Maura Conway

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

conwaym@tcd.ie

Abstract
This paper is concerned with the origins and development of the concept of cyberterrorism. It seeks to excavate the story of the concept through an analysis of both popular/media renditions of the term and scholarly attempts to define the borders of same. The contention here is not that cyberterrorism cannot happen or will not happen, but that, contrary to popular perception, it has not happened yet.

Keywords: Cyberterrorism, Terrorism, Internet, Information, Definition

Introduction

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).

What is clear from Deutch's statement is that the Internet is 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 printing presses, radio stations, or television networks. Every machine connected to the Internet is potentially a printing press, a broadcasting station, 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 1998 it was reported that 12 of the 30 terrorist organisations identified by the US State Department had their own websites. Today, a majority of the 33 groups on the same list are said to have an online presence. The question that then arises is this: Are terrorist groups who use the Internet in such a manner 'cyberterrorists'? The answer hinges on what constitutes cyberterrorism.

This paper is concerned with the origins and development of the concept of cyberterrorism. It seeks to excavate the story of the concept through an analysis of both popular/media renditions of the term and scholarly attempts to define the borders of same. Let me say at the outset that, in both realms, confusion abounds. This is startling, particularly given that since the events of 9-11, the question on everybody's lips appears to be 'Is Cyberterrorism Next?' (Denning 2001a; Swartz 2001). In academic circles the answer is generally 'not yet.' The media are less circumspect, however, and policy makers appear increasingly to be seduced by the latter's version of events. It seems to me that both question and answer(s) are hampered by the lack of certainty surrounding the central term. Let me begin by putting forward some concrete illustrations of this definitional void culled from newspaper accounts.

Cyberterrorists Abound

In June 2001 a headline in the *Boston Herald* read 'Cyberterrorist Must Serve Year in Jail' (Richardson 2001). The story continued: 'Despite a Missouri cyberterrorist's 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 children, and posting a picture of the school's principal with bullet holes in his head and chest on the Net.

In December 2001 a headline in the *Bristol Herald Courier*, Wise County, Virginia, USA read 'Wise County Circuit Court's Webcam "Cracked" by Cyberterrorists' (Still 2001). The webcam, which allows surfers to log on and watch the Wise County Circuit Courts in action, was taken offline for two weeks for repairs. '(Expletive Deleted) the United States Government' was posted on a web page, it was reported, but the defaced page could only be seen by the Court's IT contractors. Internet surfers who logged on could only see a blank screen. The 'attack' is though to have originated in Pakistan or Egypt, according to the report. 'This is the first cyberterrorism on the court's Internet technology, and it clearly demonstrates the need for constant vigilance,' according to Court Clerk Jack Kennedy. 'The damage in this case amounted to a $400 hard drive relating to the Internet video server. The crack attack has now resulted in better software and enhanced security to avoid a [*sic*] further cyberterrorism.' According to Kennedy, cracking can escalate to terrorism when a person cracks into a government- or military-maintained Web site; he said cyberterrorism has increased across the United States since the events of 9-11 and law enforcement has traced many of the attacks to Pakistan and Egypt.

The scare mongering is not confined to the US, however. In March of this year British IT security specialists Digilog published what has been described as ‘the most comprehensive study of the insecurity of wireless networks in London’ (Leyden 2002). The survey discovered that over 90 per cent of those networks are open to drive-by hacking, also known as war driving. Unfortunately, this potentially worthwhile survey is undermined by the emphasis placed on the supposed link between drive-by hackers and international terrorism: ‘And networks are not only at risk from attacks at close quarters. University research in Hawaii has shown that signals can be intercepted from a distance of over 25 miles, raising fears of large-scale cyber-terrorism. Computer-controlled power grids, telephone networks and water-treatment plants are at risk’ (as quoted in Leyden 2002).

Also in March linkLINE Communications, described as ‘a small, but determined Internet service provider’ located in Mira Loma, California received telephone and e-mail threats from an unnamed individual who claimed to have accessed- or be able to access- the credit card numbers of linkLINE’s customers. He said that he would sell the information and notify linkLINE’s customers if $50,000 was not transferred to a bank account number that he supplied. The ISP refused to concede to the cracker’s demands: ‘We’re not going to let our customers, or our reputation, be the victims of cyber-terrorism,’ said one of the company’s founders. linkLINE contacted the authorities and learned that the cracker and his accomplices may have extorted as much as $4 billion from other companies. The account was subsequently traced through Russia to Yemen (linkLINE Communications Inc. 2002).

A similar incident had taken place in November 2000. An attack, originating in Pakistan, was carried out against the American Israel Public Affairs Committee, a lobbying group. 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. The Pakistani hacker who took credit for the crack, the self-styled Dr. Nuker, 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’ (Schwartz 2000).

In May 2001 ‘cyberterrorism’ was on the agenda once again when supporters of the group Laskar Jihad (Holy War Warriors) hacked into the websites of the Australian embassy and the Indonesian national police in Jakarta to protest against the arrest of their leader. The hackers intercepted users logging on to the Web sites and redirected them to a site containing a warning to the Indonesian police to release Ja’far Umar Thalib, the group’s leader. Thalib was arrested in connection with inciting hatred against a religious group and ordering the murder of one of his followers. According to police, the hackers, the self-styled Indonesian Muslim Hackers Movement, did not affect police operations. The Australian embassy said the hackers did not sabotage its Web site, but only directed users to the other site (Anonymous 2001).

It is clear that the pejorative connotations of the terms ‘terrorism’ and ‘terrorist’ have resulted in some unlikely acts of computer abuse being labelled ‘cyberterrorism’. According to the above, sending pornographic e-mails to minors, posting offensive content on the Internet, defacing Web pages, using a computer to cause $400 worth of damage, stealing credit card information, posting credit card numbers on the Internet, and clandestinely redirecting Internet traffic from one site to another all constitute instances of cyberterrorism. And yet none of it could be described as terrorism- some of it not even criminal- had it taken place without the aid of computers. Admittedly, terrorism is a notoriously difficult activity to define. However, the addition of computers to plain old criminality it is not.

What is Cyberterrorism?

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). The definition of terrorism employed in this paper is that 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.”

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 (Pollitt n.d.).

The above definition is similar to the conceptualisation of cyberterrorism 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 2002, 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.

Utilising the above definitions, the ‘attack’ on the webcam of the Wise County Circuit Court does not qualify as cyberterrorism, nor do any of the other ‘cyberterrorist attacks’ outlined above. This is hardly surprising; the inflation of the concept of cyberterrorism may increase newspaper circulation, but is ultimately not in the public interest. Despite this, many have suggested adopting broader definitions of the term.

In an article, which appeared in *Terrorism and Political Violence* in 1997, Devost, Houghton and 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 it might incite fear- to be characterised as terrorist. This is problematic because, although there is no single accepted definition of so-called political terrorism, more than 80% of scholars agree that the latter has two integral components: the use of force or violence and a political motivation (Guelke 1998, 19; Schmid & Jongman 1988, 5). To this end, most country’s domestic laws conceive of terrorism as requiring violence and/or the threatening or taking of human life in pursuit of political or ideological goals. Devost, Houghton and Pollard are aware of this, but wish to allow for the inclusion of pure information system abuse (i.e. that does not employ nor result in physical violence) as a possible new facet of terrorism nonetheless (1996, 10). Others have followed suit.

Israel's former science minister, Michael Eitan, has deemed 'sabotage over the Internet' as cyberterrorism (Sher 2000). 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 (Mates 2001, 6). Yael Shahar, Web master at the International Policy Institute for Counter-Terrorism (ICT), located in Herzliya, Israel, differentiates between a number of 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 the way in which a group of Palestinian hackers and sympathisers set up a Web site that provides one-stop access to hacking tool and viruses, and tips on how to use the tools to mount attacks on Israeli targets. They are, he says, using the techniques of cyberterrorism (Leyden 2000). Leyden and others wish to conflate politically motivated hacking- so-called hacktivism- and terrorism. 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).

Noble's comment highlights 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.' Such a taxonomy is uncalled for: even had Dr. Nuker broken into the headquarters of the American Israel Public Affairs Committee 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 would be considered terrorist. Noble contends, furthermore, that "disinformation is easily spread; rumours 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? In fact, Ingles-le Noble (1999) himself recognises 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.

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). Indeed, it will be up to police investigators to decide whether an action is to be regarded as terrorism. Online groups, human rights organisations, 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). Notwithstanding, in the wake of the events of 9-11, US legislators followed suit. Previous to the 11th of September, if one successfully infiltrated a federal computer network, one was considered a hacker. However, following the passage of the USA Act, which authorised 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 labelled cyberterrorists and, if convicted, to face up to 20 years in prison (NIPC 2001; see also Middleton 2002). Clearly, policymakers believe that actions taken in cyberspace are qualitatively different from those taken in the 'real' world.

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 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). Second, it is useful to distinguish two different facets of terrorist use of information technology:

(1) Terrorist use of computers as a facilitator of their activities, and
(2) Terrorism involving computer technology as a weapon or target.

Utilising 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 labelled cyberterrorism. That is:

- Attacks must instil terror as commonly understood (i.e. result in death and/or large-scale destruction),
- Attacks 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 I 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 or 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' (see Conway 2002).

Conclusion

According to journalists, 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. 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 not taken down the Net, they had taken down the towers. '[W]heras 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.'

Richard Clarke, White House special adviser for Cyberspace Security, has said that he prefers not to use the term 'cyberterrorism,' but instead favours use of the term 'information security' or 'cyberspace security.' This is because, Clarke has stated, most terrorist groups have not engaged in information warfare (read 'cyberterrorism'). Instead, he admits, terrorist groups have at this stage 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 recent 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 cannot 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

Anonymous (2001) Hackers Divert Indonesian Hits. *The Age*, May 10. Available on the Internet at http://www.theage.com.au/news/2001/05/10/FFXTYW2ZHMC.html <5/9/2002>.

Collin, B. (1996) The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago. Available on the Internet at: http://www.afgen.com/terrorism1.html <5/9/2002>.

Conway, Maura (2002) Terrorism and Telecommunications: An Analysis of Terrorist 'Use' of the Internet. Paper presented at the 98th American Political Science Association (APSA) Annual Conference, Hynes Convention Centre, Boston. Available on the Internet at http://apsaproceedings.cup.org/Site/papers/040/040002ConwayMaur.pdf <5/9/2002>.

Daukantas, P. (2001) Professors Hash Out Emergency Response, Cyberterrorism Strategies. *Government Computer News*, December 14. Available on the Internet at http://www.gcn.com/vol1_no1/daily-updates/17642-1.html <5/9/2002>.

Denning, D. (2001a). *Is Cyber Terror Next?*, US Social Science Research Council, New York. Available on the Internet at http://www.ssrc.org/sept11/essays/denning.htm <5/9/2002>.

Denning, D. (2001b) Hacker Warriors: Rebels, Freedom Fighters, and Terrorists Turn to Cyberspace. *Harvard International Review*, Summer. Available on the Internet at: http://www.hir.harvard.edu/archive/articles/pdf/denning.html <5/9/2002>.

Denning, D. (2000a) *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, May 23. Available on the Internet at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html <5/9/2002>.

Denning, D. (2000b) Cyberterrorism. *Global Dialogue*, Autumn. Available on the Internet at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc <5/9/2002>.

Denning, D. (1999) *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Available on the Internet at: http://www.nautilus.org/info-policy/workshop/papers/denning.html <5/9/2002>.

Deutch, J. (1996) *Statement Before the US Senate Governmental Affairs Committee* (Permanent Subcommittee on Investigations), 25 June. Available on the Internet at http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html <5/9/2002>.

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

Devost, M., B. Houghton & N. Pollard (1996) Information Terrorism: Can You Trust Your Toaster? *The Terrorism Research Centre.* Available on the Internet at: http://www.terrorism.com/terrorism/itpaper.html <5/9/2002>.

Di Maio, P. (2001) Hacktivism, Cyberterrorism or Online Democracy?. *The Information Warfare Site (IWS)*, March 19. Available on the Internet at http://www.iwar.org.uk/hackers/resources/hacktivism-europe/internet-europe.htm <5/9/2002>.

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

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

Gearty, C. (1991) *Terror*, Faber & Faber, London.

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

Havely, J. (2000) When States go to Cyber-War. *BBC News Online*, February 16. Available on the Internet at http://news.bbc.co.uk/hi/english/sci/tech/newsid_642000/642867.stm <5/9/2002>.

Hershman, T. (2000) Cyberterrorism is Real Threat, Say Experts at Conference. *Israel.internet.com*, December 11.

Hoffman, B. (1998) *Inside Terrorism*, Indigo, London.

Holms, J. (1994) *Terrorism*, Windsor Publishing Corps, New York.

Ingles-le Noble, J. (1999) Cyberterrorism Hype. *Jane's Intelligence Review*. Available on the Internet at http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm <5/9/2002>.

Leyden, J. (2002) Drive-By Hacking Linked to Cyberterror. *The Register*, March 27. Available on the Internet at http://www.theregister.co.uk/content/55/24611.html <5/9/2002>.

Leyden, J. (2000) Palestinian Crackers Give Out Tools to Attack Israelis. *The Register*, December 4. Available on the Internet at http://www.theregister.co.uk/content/6/15199.html <5/9/2002>.

linkLINE Communications, Inc. (2002) linkLINE Communications Thwarts Cyber-Terrorist. *Yahoo!Finance*, March 19.

Mates, M. (Rapporteur) (2001) *Technology and Terrorism*, NATO, Brussels. Available on the Internet at http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm <5/9/2002>.

Middleton, J. (2002) US Hackers Could Face Life Sentences. *Vnunet.com*, February 28. Available on the Internet at http://vnunet.com/News/1129590 <5/9/2002>.

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

Pollitt, M. (n.d.) *Cyberterrorism: Fact or Fancy?*, Washington DC, FBI Laboratory. Available:http://www.cs.georgetown.edu/~denning/infosec/pollitt.html <5/9/2002>.

Poulsen, K. (2001) Cyber Terror in the Air. *SecurityFocus.com*, June 30. Available on the Internet at http://www.businessweek.com/technology/content/jul2001/tc20010726_694.htm <5/9/2002>.

Richardson, F. (2001) Cyberterrorist Must Serve Year in Jail. *Boston Herald*, June 6.

Schmid, A. & A. Jongman (1988) *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*, North-Holland Publishing Company, Amsterdam.

Schwartz, J. (2000) When Point and Shoot Becomes Point and Click. *The New York Times*, November 12.

Swartz, J. (2001) Experts: Cyberspace Could Be Next Target. *USA Today*, October 16.

Sher, H. (2000) Cyberterror Should be International Crime- Israeli Minister. *Newsbytes*, November 10.

Still, K. (2001) Wise County Circuit Court's Webcam 'Cracked' by Cyberterrorists.*Bristol Herald Courier*, December 20.

Veltman, C. (2001) Beating Cyber Crime. *The Daily Telegraph*, March 1, p.12E.

Wardlaw, G. (1982) *Political Terrorism: Theory, Tactics, and Countermeasures*, Cambridge University Press, Cambridge.

Weisenberger, K. (2001) Hacktivists of the World, Divide. *SecurityWatch.com* April 23. Available on the Internet at: http://www.securitywatch.com/TRE/042301.html <5/9/2002>.

Wynne, J. (2002) White House Advisor Richard Clarke Briefs Senate Panel on Cybersecurity. *Washington File*, February 14. Available on the Internet at http://usinfo.state.gov/topical/global/ecom/02021401.htm <5/9/2002>.