View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by DCU Online Research Access Service

Cyberterrorism: Hype and Reality

Maura Conway
Dublin City University

Introduction

The term cyberterrorism unites two significant modern fears: fear of technology and fear of terrorism. Both of these fears are evidenced in this quote from Walter Laqueur, one of the most well known figures in terrorism studies: "The electronic age has now made cyberterrorism possible. A onetime mainstay of science fiction, the doomsday machine, looms as a real danger. The conjunction of technology and terrorism make for an uncertain and frightening future."[1] It is not only academics that are given to sensationalism. Cyberterrorism first became the focus of sustained analysis by government in the mid-1990s. In 1996 John Deutch, former director of the Central Intelligence Agency (CIA), testified before the Permanent Subcommittee on Investigations of the United States' Senate Governmental Affairs Committee:

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.[2]

Both the popularity and, to some extent, the credibility of such scenarios was given a boost by the entertainment industry. Hollywood, eager to capitalise on the cyberterrorist threat, released the James Bond film *Goldeneye* in 1995. Other sectors were quick to follow with the publishing industry introducing Tom Clancy and Steve R. Pieczenik's *Net Force* series in 1998. As Ralf Bendrath has pointed out:

> "Sometimes it is hard to tell what is science and what is fiction. Winn Schwartau, for example, the rock manager turned preacher of 'information warfare' who runs the famous website infowar.com, has testified several times as an IT security expert before Congress, and has written two novels on cyber-terror. Even renowned cyber-war theoreticians like John Arquilla have not hesitated to publish thrilling cyber-terror scenarios for the general audience. But these works are not only made for entertainment. They produce certain visions of the future and of the threats and risks looming there."[3]

In 1998 the Global Organized Crime Project of the Center for Strategic and International Studies in Washington DC published a report entitled *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. This was the first major academic contribution to the field. The document's authors view cyberterrorism as a sub-species of Information Warfare (IW). This is because information warfare is a form of asymmetric warfare and is therefore viewed as an eminently suitable terrorist strategy. Cyberterrorism has since come to be viewed as a component allied to offensive information warfare, but one that has a direct corollary in traditional, physical, non-information based 'warfare' (i.e. classical political terrorism). In other words, cyberterrorism is recognised as having links with traditional terrorist tactics,

but may be viewed as a new strategy employing new tools and exploiting new dependencies.

Although the author's of the CSIS report fail to provide a definition of what it is they mean by 'cyberterrorism,' they are at pains to illustrate its potentially disastrous consequences:

> A smoking keyboard does not convey the same drama as a smoking gun, but it has already proved just as destructive. Armed with the tools of Cyberwarfare, substate or nonstate or even individual actors are now powerful enough to destabilise and eventually destroy targeted states and societies… Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees. Such a strategic attack, mounted by a cyberterrorist group, either substate or nonstate actors, would shut down everything from electric power grids to air traffic control centers.[4]

A focus on such 'shut-down-the-power-grid' scenarios is increasingly a feature of analyses of the cyberterrorist threat.[5]

This chapter is concerned with explicating the origins and development of the concept of cyberterrorism with a view to separating the hype surrounding the issue from the more prosaic reality. This is more difficult than it may at first appear, however. Ralf Bendrath has identified three major stumbling blocks.[6] First, this debate is not simply about predicting the future, but is also about how to prepare for it (i.e. the future) in the present. The problem is that those involved in the debate cannot draw on either history or experience to bolster their positions, as a major cyberterrorist incident has never yet occurred. For this reason different scenarios or stories about the possible course of future events are providing the grounds on which decisions must be made. The upshot of this is that the various actors (i.e. government and opposition, the computer security industry, the media-entertainment complex, scholars, and others) with their various, and often times divergent, interests are competing with each other by means of their versions of the future, which are particularly subject to political exploitation and instrumentation.

A second, and related, problem is the nature of the space in which a cyberterrorist attack would occur:

> "In the physical landscape of the real world, any action has its constraints in the laws of nature…Cyberspace, in contrast, is a landscape where every action is possible only because the technical systems provide an artificial environment that is built to allow it. The means of attack therefore change from system to system, from network to network. This makes threat estimation and attack recognition much more difficult tasks."[7]

Bendrath's final point relates to the highly technical nature of the new threat and the constraints this places on social scientists and their ability to estimate the magnitude of that threat. Bendrath's solution is for social scientists to draw conclusions by looking at how the threat is perceived: "The way a problem is framed normally determines or at least limits the possible solutions for it."[8]

With this in mind, this paper seeks to excavate the story of the concept of cyberterrorism through an analysis of both popular/media renditions of the term and scholarly attempts to define its borders. It must be stated at the outset that, in both media and academic 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?'[9] 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.'[10] 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." The defendant, 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.'[11] 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. However, 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. It was predicted that an escalation in hack attacks would occur in the aftermath of 9-11.[12] However, the predicted escalation did not materialise. In the weeks following the attacks, Web page defacements were well publicised, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers- particularly those located in the US- were wary of being associated with the events of September 11th and curbed their activities as a result.

In March 2002, 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 wasn't 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.[13]

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."[14] In May 2001 'cyberterrorism' reared its head once again when supporters of the terrorist group Laskar Jihad (Holy War Warriors) hacked into the website of Australia's Indonesian 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.

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.

The Origins of Cyberterrorism

Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term 'cyberterrorism' in the mid-1980s.[15] The idea of terrorists utilising communications technologies to target critical infrastructure was first mooted more than two decades ago, however. In 1977, Robert Kupperman, then Chief Scientist of the US Arms Control and Disarmament Agency, stated:

> "Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest. Thirty years ago terrorists could not have obtained extraordinary leverage. Today, however, the foci of communications, production and distribution are relatively small in number and highly vulnerable."[16]

Such fears crystallised with the advent of the Internet. The opening chapter of *Computers at Risk* (1991), one of the foundation books in the US computer security field, which was commissioned and published by the US National Academy of Sciences, begins as follows:

> "We are at risk. America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable – to the effects of poor

> design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[17]

Nevertheless, cyberterrorism only became the object of sustained academic analysis and media attention in the mid-1990s. It was the advent of and then the increasing spread of the World Wide Web (WWW) along with the vocal protestations of John Deutch, then Director of the Central Intelligence Agency (CIA), as to the potentiality of the Web as a terrorist tool and/or target that kick-started research into the phenomenon of cyberterrorism in the United States.

From 'Real World' Terrorism to Cyberterrorism

It has been pointed out that if you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers.[18] This discrepancy bears more than a grain of truth, as there are a number of stumbling blocks to constructing a clear and concise definition of cyberterrorism. Chief among these are the following:

- 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.
- 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.
- 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 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 more generally.[19]

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. One of the most accessible sound bites on what defines cyberterrorism is that it is 'hacking with a body count.'[20] 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.

Mark M. Pollitt's article 'Cyberterrorism: Fact or Fancy?,' published in *Computer Fraud and Security* in 1998, made a significant contribution with regard to the definition of cyberterrorism. Pollitt points out, as many others fail to do, that the concept of cyberterrorism is composed of two elements: cyberspace and terrorism. Cyberspace may be conceived of as "that place in which computer programs function and data moves."[21] 'Cyberspace' as a term has its origins in science fiction writing. It first appeared in William Gibson's 1984 novel *Neuromancer*, which featured a world called cyberspace, after Cyber, the most powerful computer.[22] 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.[23] In his paper Pollitt employs 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."

Pollitt combines Collin's definition of cyberspace and the US Department of State's definition of terrorism which results in the construction of a narrowly drawn working definition of cyberterrorism as follows:

> "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents."[24]

A similar definition of cyberterrorism has been put forward by Dorothy Denning in numerous articles and interviews, and in her testimony on the subject before the United States Congress's House Armed Services Committee. 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."[25]

Pollitt and Denning are two of only a very small number of authors to recognise and make explicit the way in which the word 'cyberterrorism' is meaningless in and of itself and that it is only the relational elements of which the word is composed that imbue it with meaning.[26] A majority of authors appear to overlook this connection. In fact, numerous authors of articles dealing explicitly with cyberterrorism provide no definition of their object of study at all.[27]

Utilising the definitions provided by Denning and Pollitt, the 'attack' on the Web-cam of the Wise County Circuit Court does not qualify as cyberterrorism, nor do any of the other 'cyberterrorist attacks' outlined earlier. It's hardly surprising; the inflation of the concept of cyberterrorism may increase newspaper circulation, but is ultimately not in the public interest. Despite this, many scholars (and others) have suggested adopting broader definitions of the term. Many authors do this implicitly by falling into the trap of either conflating hacking and cyberterrorism or confusing cyber crime with cyberterrorism, while a number of authors fall into both of these traps. Such missteps are less arbitrary than they may first appear however, as two important academic contributions explicitly allow for such a broadening of the definition of cyberterrorism.

Virtual Violence

Traditional terrorism generally involves violence or threats of violence. However, despite the prevalent portrayal of traditional violence in virtual environments, 'cyber violence' is still very much an unknown quantity. It is accepted, for example, that the destruction of another's computer with a hammer is a violent act. But should destruction of the data contained in that machine, whether by the introduction of a virus or some other technological means, also be considered 'violence'?[28] This question goes right to the heart of the definition of cyberterrorism.

In a seminal article, published in the journal *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."[29] They conceive of

information terrorism as "the nexus between criminal information system fraud or abuse, and the physical violence of terrorism."[30] 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 terrorism, more than 80% of scholars agree that the latter has two integral components: the use of force or violence and a political motivation.[31] 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 (i.e. that does not employ nor result in physical violence) as a possible new facet of terrorism nonetheless.[32]

Nelson *et al*'s reasoning as to why disruption, as opposed to destruction, of information infrastructures ought to fall into the category of cyberterrorism is quite different:

> "Despite claims to the contrary, cyberterrorism has only a limited ability to produce the violent effects associated with traditional terrorist acts. Therefore, to consider malicious activity in cyberspace 'terrorism,' it is necessary to extend existing definitions of terrorism to include the destruction of digital property. The acceptance of property destruction as terrorism allows this malicious activity, when combined with the necessary motivations, to be defined as Cyberterror."[33]

As we have seen, Mark Pollitt employs the State Department's definition of terrorism to construct his definition of cyberterrorism. Neither the State Department definition, nor Pollitt's, specifically identifies actions taken against property as terrorism. According to Nelson *et al*, however, in practice the Title 22 definition "clearly includes the destruction of property as terrorism when the other conditions for terrorism are satisfied (premeditated, politically motivated, etc.)."[34] In addition, the FBI definition of terrorism explicitly includes acts against property. However, Nelson *et al* point out that both the State Department and FBI definitions are subsumed by the Department of Defense definition contained in regulation O-2000.12-H, which includes "malicious property destruction" as a type of terrorist attack. This regulation also addresses destruction at the level of binary code, which it specifically refers to under the use of special weapons

Use of sophisticated computer viruses introduced into computer-controlled systems for banking, information, communications, life support, and manufacturing could result in massive disruption of highly organised, technological societies. Depending on the scope, magnitude, and intensity of such disruptions, the populations of affected societies could demand governmental concessions to those responsible for unleashing viruses. Such a chain of events would be consistent with contemporary definitions of terrorist acts."[35] Taking the above into account, Nelson *et al* define cyberterrorism as follows: "Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological."[36] The problem is that this definition massively extends the terrorist remit by removing the requirement for violence resulting in death and/or serious destruction from the definition of terrorism and lowering the threshold to "disruption of digital property."

A related problem is that although Nelson *et al* are quite precise in their categorisations and repeatedly stress that the other conditions necessary for an act to be identified as terrorist must be satisfied (i.e. premeditation, political motivation, etc.) before disruptive cyber attacks may be classified as cyberterrorism, others are

less circumspect. Israel's former science minister, Michael Eitan, has deemed "sabotage over the Internet" as cyberterrorism.[37] 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."[38] 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."[39] 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.[40]

Hacking versus Cyberterrorism

'Hacking' is the term used to describe unauthorised access to or use of a computer system. The term 'hacktivism' is composed of the words 'hacking' and 'activism' and is the handle used to describe politically motivated hacking. 'Cracking' refers to hacking with a criminal intent; the term is composed of the words 'criminal' and 'hacking.' In a majority of both media reports and academic analyses of cyberterrorism, one or other of these terms – hacking, hacktivism, cracking - or the activities associated with them are equated with or identified as variants of cyberterrorism.

Hackers have many different motives. Many hackers work on gaining entry to systems for the challenge it poses. Others are seeking to educate themselves about systems. Some state that they search for security holes to notify system administrators while others perform intrusions to gain recognition from their peers. Hacktivists are politically motivated; they use their knowledge of computer systems to engage in disruptive activities on the Internet in the hopes of drawing attention to some political cause. These disruptions take many different forms, from 'denial of service' (DoS) attacks that tie up Web sites and other servers, to posting 'electronic graffiti' on the home pages of government and corporate Web sites, to the theft and publication of private information on the Internet. Crackers hack with the intent of stealing, altering data, or engaging in other malicious damage.[41] A significant amount of cracking is carried out against businesses by former employees.

The term 'hacker' was originally applied to those early pioneers in computer programming who continually reworked and refined programs. This progressed, as Sprague explains, to the "displaying of feats of ingenuity and cleverness, in a productive manner, involving the use of computer systems."[42] Gaining unauthorised access to computer networks was one way of displaying such expertise. This original generation of hackers developed a code of practice, which has come to be known as the Hacker Ethic. It was premised on two principles, namely the free sharing of information and a prohibition against harming, altering, or destroying any information that was discovered through this activity. Over the course of time, however, "a new generation appropriated the word 'hacker' and with help from the press, used it to define itself as password pirates and electronic burglars. With that the public perceptions of hackers changed. Hackers were no longer seen as benign explorers but malicious intruders."[43] As a result, the classical computer hacker – bright teenagers and young adults who spend long hours in front of their computer screens – is now the 'cyberpunk.'

Hackers as Terrorists

Much has been made of the similarities between profiles of terrorists and those of hackers. Both groups tend to be composed primarily of young, disaffected, males.[44] In the case of computer hackers, a distinct psychological discourse branding them the product of a pathological addiction to computers has emerged. In fact, a large number of hackers who have been tried before the criminal courts for their exploits have successfully used mental disturbance as a mitigating factor in their defence, and have thus received probation with counselling instead of jail time.[45]

Hackers are commonly depicted as socially isolated and lacking in communication skills. Their alleged anger at authority is said to reduce the likelihood of their dealing with these frustrations directly and constructively. In addition, the flexibility of their ethical systems; lack of loyalty to individuals, institutions, and countries; and lack of empathy for others are said to reduce inhibitions against potentially damaging acts. At the same time, their description as lonely, socially naïve, and egotistical appears to make them vulnerable to manipulation and exploitation.[46]

Some hackers have demonstrated a willingness to sell their skills to outsiders. The most famous example is the Hanover Hackers case. In 1986, a group of hackers in Hanover, Germany, began selling information they obtained through unlawfully accessing the computer systems of various Departments of Energy and Defence, a number of defence contractors, and the US Space Agency NASA, to the Soviet KGB. Their activities were discovered in 1988, but nearly two years elapsed before the group were finally identified and apprehended.[47] During the first Gulf War, between April 1990 and May 1991, a group of Dutch hackers succeeded in accessing US Army, Navy, and Air Force systems. They sought to sell their skills and sensitive information they had obtained via the intrusions to Iraq, but were apprehended by police in the Netherlands.[48]

According to Gregory Rattray, a majority of the analyses of hackers-for-hire - what he calls 'cybersurrogates' for terrorism - generally stress the ease[49] and advantages of such outsourcing. These analysts presume that terrorist groups will be able to easily contact hackers-for-hire, while keeping their direct involvement hidden through the use of cut-outs and proxies. The hackers could then be employed to reconnoitre enemy information systems to identify targets and methods of access. Furthermore, it is posited that if hacker groups could be employed to actually commit acts of cyberterrorism, terrorist groups would improve their ability to avoid culpability or blame altogether. Rattray does flag the important risks and disadvantages to such schemes, however. First, seeking to employ hackers to commit acts not just of disruption, but of significant destruction that may involve killing people would in all likelihood prove considerably more difficult than buying information for the purposes of intelligence gathering. Second, simply contacting, never mind employing, would-be hackers-for-hire would subject terrorists to significant operational security risks. Third, terrorist organisations run the risk of cybersurrogates being turned into double agents by hostile governments. All three scenarios, Rattray admits, weigh heavily against the employment of cybersurrogacy as a strategy.[50]

And these are not the only risks faced by terrorists planning to employ IT to carry out attacks. In their paper 'The IW Threat from Sub-State Groups: An Interdisciplinary Approach' (1997), Andrew Rathmell, Richard Overill, Lorenzo Valeri, and John Gearson point out that should the terrorists themselves lack sufficient computer expertise, there is the likelihood that they would recruit hackers who would prove insufficiently skilled to carry out the planned attacks. In addition, these authors

concur with Rattray that there is a strong case to be made for such hackers changing sides. This is because the primary motive of the hacker-for-hire is financial gain thus, given sufficient monetary inducement, such individuals are unlikely to object to reporting to other than their original 'employer.'[51]

David Tucker also has some interesting insights into the hacker-for-hire scenario. Based on a simulation in which he took part, which involved a hacker and members of a number of terrorist organizations. Of the terrorists who took part in the conference/simulation that Tucker attended, one was a member of the Palestinian Liberation Organisation (PLO), two were members of Basque Fatherland and Liberty (ETA), one from the Liberation Tigers of Tamil Eelam (LTTE), and one from the Revolutionary Armed Forces of Colombia (FARC). Tucker foresees potential organisational problems for any hacker-terrorist collaboration. He points out that on those occasions when hackers aren't acting alone, they operate in flat, open-ended associations. This is the opposite of many terrorist groups, which are closed hierarchical organisations. There is certainly the potential for clashes between these different organisational styles, developed in different operating environments and derived from different psychological needs. Tucker reports that a former member of ETA who was involved in the simulation repeatedly stressed the need to belong and the strength of attachment to the group as characteristic of members of clandestine organisations.[52] This is not a character trait typically associated with hackers. In fact, in the simulation in which Tucker took part, the hacker and the terrorists involved disagreed over tactics and had difficulty communicating. Eventually, these difficulties became so great that it resulted in a breakdown in the simulation group. The hacker and the terrorists were simply not able to work together. Tucker observes that if the breakdown can be generalised, it would have obvious consequences for hacker-terrorist collaboration.[53]

The only likely scenario, given the above, is cyber attacks carried out by terrorists with hacking skills.[54] This is not impossible. "The current trend towards easier-to-use hacking tools indicates that this hurdle will not be as high in the future as it is today, even as it is significantly lower today than it was two years ago."[55] According to William Church, a former US Army Intelligence Officer:

> "If you look at the Irish Republican Army, which was probably the closest before they made peace, they were on the verge of it. They had computer-oriented cells. They could have done it. They were already attacking the infrastructure by placing real or phoney bombs in electric plants, to see if they could turn off the lights in London. But they were still liking the feel of physical weapons, and trusting them."[56]

Terrorists are generally conservative in the adoption of new tools and tactics.[57] Factors influencing the adoption of some new tool or technology would include: the terrorist group's knowledge and understanding of the tool, and their trust in it. Terrorists generally only put their trust in those tools that they have designed and built themselves, have experimented with, and know from experience will work. It's for this reason that weapons and tools generally proliferate from states to terrorists.[58] O'Brien and Nusbaum suggest that intelligence agencies should utilise online chat forums, hacker Web sites, etc. to gather intelligence on contemporary asymmetric threats. They suggest that most hackers possess a large degree of hubris with regards to their hacking knowledge and abilities as a result of which such "threat-savvy users" could be coaxed into revealing vulnerabilities they had discovered on the Net, as well as boasting about their own abilities and exploits.[59] David Smith, the man responsible for transmitting the Melissa virus, helped the FBI bring down several major

international hackers. Smith used a fake online identity to communicate with and track other hackers from around the world. His intelligence gathering resulted in the arrest of both Jan DeWit, the author of the Anna Kournikova virus, and Simon Vallor, the author of the Gokar virus.[60] This position is endorsed by Soo Hoo, Goodman, and Greenberg:

> "Foreign Bases of operation might be useful for intelligence-gathering activities, but again, they are not required for IT-enabled terrorism…[I]nformation about various systems' vulnerabilities is often shared online between hackers on computer bulletin boards, Web sites, news groups and other forms of electronic association, and this information can be obtained without setting foot in the target country."[61]

It seems unlikely, however, that professional hackers or cyber mercenaries would engage in the cavalier behaviour described above:

> "While amateur hackers receive most publicity, the real threat are the professionals or 'cyber mercenaries.' This term refers to highly skilled and trained products of government agencies or corporate intelligence branches that work on the open market. The Colombian drug cartels hired cyber mercenaries to install and run a sophisticated secure communications system; Amsterdam-based gangs used professional hackers to monitor and disrupt the communications and information systems of police surveillance teams."[62]

There is no evidence of such mercenaries having carried out attacks under the auspices of known terrorist organisations, however.

The US Department of Justice labelled Kevin Mitnick, probably the world's most famous computer hacker, a "computer terrorist."[63] On his arraignment, Mitnick was denied access not only to computers, but also to a phone, "the judge believing that, with a phone and a whistle, Mitnick could set off a nuclear attack."[64] Before all-digital switches made it possible for telephone companies to move them out of band, one could actually hear the switching tones used to route long-distance calls. 'Phreaking' is the term used to describe the art and science of cracking the phone network. Early phreakers built devices called `blue boxes' that could reproduce these tones, which could be used to commandeer portions of the phone network. The reference above is to an early phreaker who acquired the sobriquet `Captain Crunch' after he proved that he could generate switching tones with a plastic whistle pulled out of a box of Captain Crunch cereal! But at no time did he seek to set off any nuclear device using this method. Incredulity aside, hackers are unlikely to become terrorists, because their motives are divergent. Despite the allegedly similar personality traits shared by both terrorists and present-day hackers, the fact remains that terrorism is an extreme and violent occupation, and far more aberrant than prankish hacking. Although hackers have demonstrated that they are willing to crash computer networks to cause functional paralysis and even significant financial loss, this propensity for expensive mischief is not sufficient evidence that they would be willing to jeopardise lives or even kill for a political cause.[65]

Hacktivism versus Cyberterrorism

Hacktivism grew out of hacker culture, although there was little evidence of sustained political engagement by hackers prior to the mid-1990s.[66] Nineteen ninety-eight is viewed by many as the year in which hacktivism really took off.[67] Probably the first incidence of hacktivism took place in 1989 when hackers with an anti-nuclear stance released a computer worm into NASA's SPAN network. The worm carried the message "Worms Against Nuclear Killers…Your System has Been Officially

WANKed…You talk of times of peace for all, and then prepare for war." At the time, anti-nuclear protesters were seeking to stop the launch of the shuttle that carried the plutonium-fuelled Galileo probe on the first leg of its voyage to Jupiter.[68] It was in '98 that the US-based Electronic Disturbance Theatre (EDT) first employed it's FloodNet software in an effort to crash various Mexican government Web sites to protest the treatment of indigenous peoples in Chiapas and support the actions of the Zapatista rebels. FloodNet is a Java applet that, once the launching page has been accessed, repeatedly loads pages from targeted networks. If enough people participate in a FloodNet attack (i.e. access the launching page at a given date and window of time), the targeted computer will be brought to a halt, bombarded by too many commands for it to process. The FloodNet software is available at http://www.thing.net/~rdom/ecd/floodnet.html. Over 8,000 people participated in this, one of the first digital sit-ins. Probably the very first such demonstration was carried out against the French government. On 21December 1995, a group called Strano Network launched a one-hour Net'Strike attack against Web sites operated by various French government agencies. It was reported that as least some of the sites were inaccessible during that time.[69] It was also in '98 that JF, a young British hacker, entered about 300 Web sites and replaced their home pages with anti-nuclear text and imagery. At that time, JF's hack was the biggest political hack of its kind. 'Hacktions' also took place in Australia, China, India, Portugal, Sweden, and elsewhere in the same year.[70] Michael Vatis, one-time Director of the FBI's National Infrastructure Protection Center (NIPC), has labelled such acts as cyberterrorism.[71] Tim Jordan identifies two different types of hacktivism: Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA). According to Jordan:

> "Mass Virtual Direct Action involves the simultaneous use, by many people, of the Internet to create electronic civil disobedience. It is named partly in homage to the dominant form of offline protest during the 1990s, non-violent direct action or NVDA."[72]

The FloodNet attack on the Mexican government Web sites described above was an example of MVDA as was the action against the 1999 World Trade Organisation (WTO) conference in Seattle. The organisers of the latter event, the UK-based Electrohippies, estimated that over 450,000 people participated in their sit-in on the WTO Web site. In contrast to MVDA, IVDA utilises classical hacker/cracker techniques and actions for attacking computer systems, but employs them for explicitly political purposes. Jordan makes the point that the name IVDA does not mean the actions are necessarily undertaken by those acting alone, but instead that the nature of such actions means that they must be taken by individuals (i.e. they in no way rely on mass action), although they may be taken by many individuals acting in concert.[73] JF's anti-nuclear protest described above was an example of IVDA, which generally consists of infiltration of targeted networks and semiotic attacks (i.e. Web site defacements). The major difference between MVDA and IVDA, apart from those already described, is that MVDA activists rarely seek to hide their identities – through the use of pseudonyms (handles), for example – or cover their tracks. Advocates of MVDA seek to gather together large groups of people to take part in hacktions and thus to inspire public debate and discussion, and maintain that they have a right to protest even if some of those protests are illegal or bordering on same. Many of those using IVDA, on the other hand, act alone and prefer to remain anonymous, which raises issues of representativeness, authenticity, etc.[74] Finally, there are also differences between those hacktivists who are devoted to the classical hacking ideal of free flow of information and therefore view DoS attacks as wrong in principle and

those who view MVDA as both direct non-violent action and important symbolic protest.[75]

It is the disruptive nature of hacktions that distinguishes this form of 'direct action Net politics' or 'electronic civil disobedience' from other forms of online political activism. E-mail petitions, political Web sites, discussion lists, and a vast array of other electronic tools have been widely adopted as recruitment, organising, lobbying, and communicating techniques by social movements and political organisations of all sorts. Stefan Wray has described this type of use of the Internet by political activists as 'Computerised Activism.'[76] The hacktivist movement is different, because it does not view the Internet simply as a channel for communication, but also crucially as a site for action. It is a movement united by its common method as opposed to its common purpose.[77] Those political causes that have attracted hacktivist activity range from campaigns against globalisation, restrictions on encryption technology, and political repression in Latin America to abortion, the spread of electronic surveillance techniques and environmental protection. Hacktivists are, therefore, arrayed across a far wider political spectrum than the techno-libertarian agenda with which committed 'netizens,' including the hacker fraternity, are often identified.

Hacktivists, although they use the Internet as a site for political action, are not cyberterrorists. They view themselves as heirs to those who employ the tactics of trespass and blockade in the realm of real-world protest. They are, for the most part, engaged in disruption not destruction. According to Carmin Karasic, the software engineer who designed the FloodNet program: "This isn't cyberterrorism. It's more like conceptual art."[78] Ronald Deibert is correct when he states that while Dorothy Denning's definition of cyberterrorism is accurate and illuminating, her portrayal of hacktivism in her article 'Activism, Hacktivism, Cyberterrorism' is misleading. It employs the typical practice of conflating hacking with criminal activity. This is an association that not only ignores the history of hacking, but what many view as the positive potential of hacking as a tool for legitimate citizen activism.[79] Denning appears to have adopted a more moderate position in her later work;[80] Michael Vatis, on the other hand, continues to view hacktivists as perpetrators of low-level cyberterrorism.

Cyber Crime versus Cyberterrorism

The issue of computer crime was first raised in the 1960s, when it was realised that computers could easily be employed to commit a variety of frauds. Cyber crime is a more recent phenomenon, which was enabled with the introduction of the modem and the ability to remotely access computer systems, the explosion of e-commerce, and the resultant increase in financial transactions taking place via the Internet. Attempts to conflate cyberterrorism and cyber crime were inevitable. A UN manual on IT-related crime recognises that, even after several years of debate among experts on just what constitutes cyber crime and what cyberterrorism, "there is no internationally recognised definition of those terms."[81] Nevertheless, it is clear that while cyberterrorism and cyber crime both employ information technology, their motives and goals do not coincide. Cyber criminals have financial gain as there primary motive.

> "[W]e have entered a new age of computer crime. With the rise of E-commerce, the development of the Net as a commercial entity, and unparalleled media attention, the profit motive for computer crime has entered the stratosphere. Recently, Janet Reno (former Attorney General of the United

States) dubbed it a 'huge growth industry.' She's probably not wrong. What Reno and other agents of law enforcement are talking about is not hacking, it is crime. It is the kind of crime where people are hurt, money is stolen, fraud is committed, and criminals make money. It is not the grey area of electronic trespass or rearranged Web pages. It is not the world of electronic civil disobedience and 'hacktivism'…In short, it [is] about money, and that makes it a different kind of crime."[82]

Areas in which individual criminals and criminal organisations have proven proficient in cyberspace include: the theft of electronic funds, the theft of credit card information, extortion, and fraud.[83] Secondary to financial gain is the acquisition of information that can underpin the operations associated with making money. It is for this reason that transnational crime syndicates are probably more interested in maintaining a functioning Internet than attacking Internet infrastructures. In other words, organised crime groups view the Net as a tool, not a target. This is because many such organisations employ the Internet – and the public telecommunications network generally – as a vehicle for intelligence gathering, fraud, extortion, and theft.[84] For example, as banks and other financial institutions increasingly rely on the Internet for their daily operations, they become more attractive targets for criminal activity. Having said that, criminal groups, such as drug traffickers, may seek to penetrate information systems to disrupt law enforcement operations or collect information on operations planned against them.[85]

This does not mean that the proceeds of cyber crime may not be used to support terrorism, but only that were this to occur it ought not to be classed as cyberterrorism *per se*.

Computer as Target versus Computer as Tool

In a probing article simply entitled 'Cyberterrorism?' (2002), Sarah Gordon and Richard Ford draw the reader's attention to the differences between what they call "traditional cyberterrorism" and "pure cyberterrorism." According to Gordon and Ford, traditional cyberterrorism features computers as the target or the tool of attack while pure cyberterrorism is more restricted as it is limited to attacks against computers, networks, etc.[86] The author's point out that both the media and the general public favour the definition encapsulated in the term "traditional cyberterrorism" while the focus in academia is on "pure cyberterrorism." So while conceding Denning's – and thence Pollitt's – definition is "solid," Gordon and Ford find the definition less than comprehensive:

> "First, [Denning] points out that this definition is usually limited to issues where the attack is against 'computers, networks, and the information stored therein,' which we would argue is 'pure cyberterrorism.' Indeed, we believe that the true impact of her opening statement ('the convergence of terrorism and cyberspace') is realised not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be. Thus, only one aspect of this convergence is generally considered in any discussion of cyberterrorism – an oversight that could be costly. Second, it is very different from the definition that appears to be operationally held by the media and the public at large."[87]

A number of authors agree with Gordon and Ford that cyberterrorism should encompass any act of terrorism that utilises "information systems or computer technology as either a *weapon* or a *target.*"[88] Nelson *et al* include physical attacks

upon information infrastructures in this category.[89] However, the same authors disagree with Gordon and Ford on the issue of leveraging the abilities of the virtual world to complete a terrorist mission. Gordon and Ford seek to place the latter activity squarely in the category of cyberterrorism. Nelson *et al* emphatically reject this approach. They identify two new categories into which this type of activity may be placed: 'cyberterror support' and terrorist 'use' of the Net. "Cyberterror support is the unlawful use of information systems by terrorists which is not intended, by itself, to have a coercive effect on a target audience. Cyberterror support augments or enhances other terrorist acts." On the other hand, "terrorist use of information technology in their support activities does not qualify as cyberterrorism."[90]

Distinguishing Characteristics

Kent Anderson suggests 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.[91]

Combining Anderson's schema with the definitions of cyberterrorism outlined by Pollitt and Denning, it is possible to construct a four-level scale of the uses (and abuses) 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 XX). 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.'[92]

Table XX - 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 via the Internet that results in violence against persons or severe economic	Terrorists	A terrorist group using the Internet to carry out a major assault on the New

	damage		York Stock Exchange

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.[93] In fact, 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.[94] 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. 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 PATRIOT 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.[95] 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. 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 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 which 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."[96] The Department of Homeland Security merges 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 analyse 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 authorisation, "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.[97]

Concluding Thoughts on Cyber-Terrorism

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 an estimated population of regular users of over 600 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.' 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 just weeks before the September attacks.[98] 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."[99] 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.[100] 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.

[1] Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), 254.
[2] John Deutch, statement before the US Senate Governmental Affairs Committee (Permanent Subcommittee on Investigations), June 25, 1996. Full text found at http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html (accessed May 25, 2006).
[3] Ralf Bendrath, "The American Cyber-Angst and the Real World: Any Link?" in Robert Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (New York: New Press, 2003), 49.
[4] Center for Strategic and International Studies (CSIS), *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: CSIS Press, 1998), xiii.
[5] Barry C. Collin, "The Future of Cyberterrorism," paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago, 1997, full text available at http://afgen.com/terrorism1.html (accessed May 25, 2006); Matthew G. Devost, Brian K. Houghton, & Neal Allen Pollard, "Information Terrorism: Political Violence in the Information Age," *Terrorism and Political Violence* 9:1 (1997): 72-83; Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?," *Computer Fraud and Security* (February 1998): 8-10.
[6] Ralf Bendrath, "The American Cyber-Angst and the Real World: Any Link?," 51-52.
[7] Ibid., 51.
[8] Ibid., 52.
[9] Dorothy Denning, "Is Cyber Terror Next?," in Craig Calhoun, Paul Price, and Ashley Timmer (Ed.s), *Understanding September 11* (New York: New Press, 2001); full text found at http://www.ssrc.org/sept11/essays/denning.htm (accessed May 25, 2006); Jon Swartz, "Experts: Cyberspace Could Be Next Target," *USA Today*, October 16, 2001.
[10] Francis Richardson, "Cyberterrorist Must Serve Year in Jail," *Boston Herald*, June 6, 2001.
[11] Still, Kathy Still, "Wise County Circuit Court's Webcam 'Cracked' by Cyberterrorists," *Bristol Herald Courier*, December 20, 2001.
[12] Institute for Security Technology Studies (ISTS), *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth College: Institute for Security Technology Studies, 2001). Full text available online at http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf (accessed May 25, 2006).
[13] linkLINE Communications, Inc., "linkLINE Communications Thwarts Cyber-Terrorist," *Yahoo!Finance*, March 19, 2002.
[14] John Schwartz, "When Point and Shoot Becomes Point and Click,' *The New York Times*, November 12, 2000.
[15] Collin, "The Future of Cyberterrorism."
[16] As quoted in Devost, Houghton, & Pollard, "Information Terrorism: Political Violence in the Information Age," 76.
[17] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington DC: National Academy Press, 1991), 7. Full text found at http://www.nap.edu/books/0309043883/html/index.html (accessed May 25, 2006).

[18] Sarah Gordon & Richard Ford, "Cyberterrorism?" *Computers and Security* 21:7 (2002): 636.
[19] Ayn Embar-Seddon, "Cyberterrorism: Are We Under Siege?" *American Behavioral Scientist* 45:6 (2002): 1034.
[20] Barry Collin, quoted in James D. Ballard, Joseph G. Hornik, & Douglas McKenzie, "Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues," *American Behavioral Scientist* 45:6 (2002): 992.
[21] Collin, "The Future of Cyberterrorism."
[22] William Gibson, *Neuromancer* (USA: Ace, 2004 [1984]).
[23] See, for example, Conor Gearty, *Terror* (London: Faber & Faber, 1998); Adrian Guelke, *The Age of Terrorism and the International Political System* (London & New York: IB Tauris Publishers, 1998); Bruce Hoffman, *Inside Terrorism* (London: Indigo, 1998); Alex P. Schmid & Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature* (Amsterdam: North-Holland Publishing Company, 1988); Grant Wardlaw, *Political Terrorism: Theory, Tactics, and Countermeasures* (Cambridge: Cambridge University Press, 1982).
[24] Pollitt, "Cyberterrorism: Fact or Fancy?," 9.
[25] Dorothy Denning, "Is Cyber Terror Next?"; also contained in Denning's testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, which is retrievable from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed May 25, 2006). Denning first put forward this definition in her 1999 paper "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," which is available online at http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf.
[26] Sarah Gordon & Richard Ford, "Cyberterrorism?," 637.
[27] See, among others, CSIS, *Cybercrime, Cyberterrorism, Cyberwarfare*; Christen, Denney & Maniscalco, "Weapons of Mass Effect: Cyber-Terrorism"; Mark Henych, Stephen Holmes & Charles Mesloh, "Cyber Terrorism: An Examination of the Critical Issues," *Journal of Information Warfare* 2:2 (2003); Rattray, "The Cyberterrorism Threat."
[28] Sarah Gordon & Richard Ford, "Cyberterrorism?," 640.
[29] Devost, Houghton, & Pollard, "Information Terrorism: Political Violence in the Information Age," 75.
[30] Ibid., 76.
[31] Guelke, *The Age of Terrorism and the International Political System*, 19; Michael Mates, *Technology and Terrorism* (Brussels: NATO, 2001), available online at http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm (accessed May 25, 2006); Schmid & Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*, 5.
[32] Devost, Houghton, & Pollard, "Information Terrorism: Political Violence in the Information Age," 10.
[33] Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, Greg Gagnon, *Cyberterror: Prospects and Implications* (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, 1999), 7. Full text available at http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf (accessed May 25, 2006).

[34] Ibid., 8.
[35] As quoted in Nelson *et al*, *Cyberterror: Prospects and Implications*, 9.
[36] Ibid., 9.
[37] H. Sher, "Cyberterror Should be International Crime- Israeli Minister," *Newsbytes* November 10, 2000.
[38] Foreign Broadcast Information Service (FBIS), "Government Sets Up Anti-Cyberterrorism Homepage," *Sankei Shimbun* (FBIS-EAS-2002-0410), 10 April, 2002.
[39] Foreign Broadcast Information Service (FBIS), "Russia Cracks Down on 'Cyberterrorism,'"*ITAR-TASS* (FBIS-SOV-2002-0208), 8 February, 2002.
[40] Tanya Hershman, "Cyberterrorism is Real Threat, Say Experts at Conference," *Israel.internet.com*, 11 December, 2000.
[41] See National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications: An Awareness Document* (Arlington, VA: Office of the Manager, National Communications Systems, 2000), 40. Full text retrievable from http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf (accessed May 25, 2006).
[42] As quoted in Liz Duff & Simon Gardiner, "Computer Crime in the Global Village: Strategies for Control and Regulation – In Defence of the Hacker," *International Journal of the Sociology of Law* 24:2 (1996): 215.
[43] As quoted in Amanda Chandler, "The Changing Definition and Image of Hackers in Popular Discourse," International Journal of the Sociology of Law 24:2 (1996): 232.
[44] Kevin Soo Hoo, Seymour Goodman, & Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival* 39:3 (1997): 144-145; Gregory J. Rattray, "The Cyberterrorism Threat,'" in James M. Smith & William C. Thomas (Ed.s), *The Terrorism Threat and US Government Response: Operational and Organizational Factors* (Colorado: US Air Force Institute for National Security Studies, 2001), 89. The full text of the latter is available at http://www.usafa.af.mil/df/inss/Ch%205.pdf (accessed May 25, 2006).
[45] See, for example, Chandler, "The Changing Definition and Image of Hackers in Popular Discourse," 242-246; Duff & Gardiner, "Computer Crime in the Global Village: Strategies for Control and Regulation – In Defence of the Hacker," 223; Reid Skibell, "The Myth of the Computer Hacker," *Information, Communication & Society* 5:3 (2002): 342; Paul A. Taylor, *Hackers: Crime in the Digital Sublime* (London: Routledge, 1999), 44-50.
[46] CSIS, *Cybercrime, Cyberterrorism, Cyberwarfare*, 15.
[47] See Clifford Stoll, *The Cuckoo's Egg* (London: Pan Books, 1991).
[48] See Jack L. Brock, *Computer Security: Hackers Penetrate DOD Computer Systems*. (Washington DC: General Accounting Office, 1991). Full text available online at http://www.globalsecurity.org/security/library/report/gao/145327.pdf (accessed May 25, 2006).
[49] See Andrew Rathmell, Richard Overill, Lorenzo Valeri, John Gearson, "The IW Threat from Sub-State Groups: An Interdisciplinary Approach," paper presented at the Third International Symposium on Command and Control Research and Technology, Institute for National Strategic Studies, National Defense University, Washington DC, 17-20 June, 1997, 4. Paper retrievable from http://www.kcl.ac.uk/orgs/icsa/Old/terrori.html (accessed May 25, 2006).
[50] Rattray, "The Cyberterrorism Threat,'" 87-88.

[51] Rathmell *et al*, "The IW Threat from Sub-State Groups: An Interdisciplinary Approach," 5.
[52] David Tucker, *The Future of Armed Resistance: Cyberterror? Mass Destruction?* (Conference Report) (Monterey, CA: The Center on Terrorism and Irregular Warfare, 2000), 16. Full text available online at http://www.nps.navy.mil/ctiw/files/substate_conflict_dynamics.pdf (accessed May 25, 2006).
[53] Ibid., 14-16.
[54] Embar-Seddon, "Cyberterrorism: Are We Under Siege?" 1037.
[55] Soo Hoo, Goodman, & Greenberg, "Information Technology and the Terrorist Threat," 141.
[56] John Borland, "Analyzing the Threat of Cyberterrorism," *TechWeb: The Business Technology Network*, September 25, 1998, available online at http://www.techweb.com/wire/story/TWB19980923S0016 (accessed May 25, 2006). See also Andrew Rathmell, "Cyber-Terrorism: The Shape of Future Conflict?" *RUSI Journal* October (1997): 43-44, available online at http://www.kcl.ac.uk/orgs/icsa/Old/rusi.html (accessed May 25, 2006); Rathmell *et al*, "The IW Threat from Sub-State Groups: An Interdisciplinary Approach," 7-8.
[57] Rattray, "The Cyberterrorism Threat,'" 89; Jessica Stern, *The Ultimate Terrorists*. (Cambridge, MA: Harvard University Press, 1999), 74; Lorenzo Valeri & Michael Knights, "Affecting Trust: Terrorism, Internet and Offensive information Warfare," *Terrorism and Political Violence* 12:1 (2000): 20.
[58] John Borland, "Analyzing the Threat of Cyberterrorism."
[59] Kevin O'Brien & Joseph Nusbaum, "Intelligence Gathering on Asymmetric Threats: Part 2," *Jane's Intelligence Review* 15:11 (2000): 53.
[60] See Martha Mendoza, "Virus Sender Helped FBI Bust Hackers, Court Records Say," *USA Today*, September 18, 2003. Retrievable from http://www.usatoday.com/tech/news/computersecurity/2003-09-18-reformed-hacker_x.htm (accessed May 25, 2006).
[61] Soo Hoo, Goodman, & Greenberg, "Information Technology and the Terrorist Threat," 143.
[62] Kevin O'Brien & Joseph Nusbaum, "Intelligence Gathering on Asymmetric Threats: Part 1," *Jane's Intelligence Review* 15:10 (2000): 53.
[63] Hank T. Christen, James P. Denney & Paul M. Maniscalco, "Weapons of Mass Effect: Cyber-Terrorism," in Paul M. Maniscalco & Hank T. Christen (Ed.s), *Understanding Terrorism and Managing the Consequences* (New Jersey: Prentice Hall, 2002), 194.
[64] As quoted in Skibell, "The Myth of the Computer Hacker," 342.
[65] Soo Hoo, Goodman, & Greenberg, "Information Technology and the Terrorist Threat," 145.
[66] See Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," *The New York Times*, October 31, 1998, available online at http://www.cs.du.edu/~lavita/hacktivists.pdf (accessed May 25, 2006); Niall McKay, "The Golden Age of Hacktivism," *Wired*, September 22, 1998, full text online at http://www.wirednews.com/news/politics/0,1283,15129,00.html (accessed May 25, 2006). See also Douglas Thomas, "Finding a New Term: From 'Hacking' to 'Cybercrime,'" *Online Journalism Review*, February 22, 2000, available online at http://www.ojr.org/ojr/ethics/1017965933.php (accessed May 25, 2006).

[67] McKay, "The Golden Age of Hacktivism"; Alexandra Samuel, "Digital Disobedience: Hacktivism in Political Context," paper presented at the American Political Science Association (APSA) Annual Conference, San Francisco, California, USA, September 29 – August 2, 2001; Stefan Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics," paper presented at The World Wide Web and Contemporary Cultural Theory Conference, Drake University, November 1998, full text retrievable from http://switch.sjsu.edu/web/v4n2/stefan/.
[68] Dorothy Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review* 23:2 (2001), full text available online at http://www.hir.harvard.edu/articles/index.html?id=905 (accessed May 25, 2006); Denning, "Activism, Hacktivism, and Cyberterrorism," 25-26.
[69] Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace."
[70] See Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web" and McKay, "The Golden Age of Hacktivism."
[71] Michael Vatis, "What is Cyber-Terrorism?" in Yonah Alexander & Michael S. Swetnam (Ed.s), *Cyber Terrorism and Information Warfare: Threats and Responses* (New York: Transnational Publishers, 2001), 4.
[72] Tim Jordan, "Mapping Hacktivism: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) and Cyberwars," *Computer Fraud & Security* Iss. 4 (2001): 8.
[73] Ibid., 9.
[74] Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism," 7.
[75] See Jordan, "Mapping Hacktivism," 11 and Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism," 11.
[76] Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism," 3. See also Denning, "Activism, Hacktivism, and Cyberterrorism" and Jordan, "Mapping Hacktivism," 10.
[77] Samuel, "Digital Disobedience," 4.
[78] As quoted in Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web."
[79] Ronald Deibert, *Black Code: Censorship, Surveillance, and the Militarization of Cyberspace* (New York: Social Science Research Council, 2003), 19 fn.64, full text available online at http://www.ssrc.org/programs/itic/publications/ITST_materials/blackcode.pdf (accessed May 25, 2006); Denning, "Activism, Hacktivism, and Cyberterrorism."
[80] See Denning's Denning's testimony before the Special Oversight Panel on Terrorism.
[81] Mates, *Technology and Terrorism.*
[82] Thomas, "Finding a New Term."
[83] See National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications*, 36-39.
[84] CSIS, *Cybercrime, Cyberterrorism, Cyberwarfare*, 3.
[85] National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications*, 35.
[86] Sarah Gordon & Richard Ford, "Cyberterrorism?," 636-637 & 641.
[87] Ibid., 637.
[88] Mates, *Technology and Terrorism*, 6.
[89] Nelson *et al*, *Cyberterror: Prospects and Implications*, 9-10.

[90] Nelson *et al*, *Cyberterror: Prospects and Implications*, 10. See also Linda Garrison & Martin Grand, "Cyberterrorism: An Evolving Concept," *National Infrastructure Protection Center: Highlights* 6:01 (2001): 3, which is available online at http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-06.pdf (accessed May 25, 2006).
[91] Kirsten Weisenberger, "Hacktivists of the World, Divide," *SecurityWatch.com*, April 23, 2001.
[92] See, for example, Maura Conway, "Terrorism and the Internet: New Media, New Threat?" *Parliamentary Affairs* 59:2 (2006); Maura Conway, "Cybercortical Warfare: Hizbollah's Internet Strategy," in Sarah Oates, Diana Owen and Rachel Gibson (Eds), *The Internet and Politics: Citizens, Voters and Activists* (London: Routledge, 2005); Maura Conway, "Terrorist Web Sites: Their Contents, Functioning, and Effectiveness," in Philip Seib (Ed.), *Media and Conflict in the Twenty-First Century* (New York: Palgrave, 2005); Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* 7:11 (2002), which is available online at http://www.firstmonday.org/issues/issue7_11/conway/index.html (accessed May 25, 2006); Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges (Washington DC: United States Institute of Peace Press, 2006); Gabriel Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet* (Washington DC: United States Institute of Peace, 2004), which may be retrieved from http://www.usip.org/pubs/specialreports/sr116.pdf (accessed May 25, 2006).
[93] See Paola Di Maio, "Hacktivism, Cyberterrorism or Online Democracy?' (2001) on *The Information Warfare Site (IWS)* at http://www.iwar.org.uk/hackers/resources/hacktivism-europe/internet-europe.htm (accessed May 25, 2006); also Mates, *Technology and Terrorism*.
[94] Kirsten Weisenberger, "Hacktivists of the World, Divide," 9.
[95] (NIPC 2001; see also Middleton 2002 & Levin 2002, 984-985)
[96] As quoted in Declan McCullagh, "Bush Signs Homeland Security Bill," *ZDNet*, November 25, 2002. Available online at http://news.zdnet.com/2100-1009_22-975305.html (accessed May 25, 2006).
[97] Kevin Poulsen, "Lawyers Fear Misuse of Cyber Murder Law," *SecurityFocus Online*, November 21, 2001. Retrievable from http://online.securityfocus.com/news/1702 (accessed May 25, 2006); McCullagh, "Bush Signs Homeland Security Bill."
[98] Denning, "Cyberwarriors."
[99] Carole Veltman, "Beating Cyber Crime," *Daily Telegraph* (UK), 1 March, 2001: 12E.
[100] Poulsen, "Lawyers Fear Misuse of Cyber Murder Law."