THE MEDIA AND CYBERTERRORISM:
A STUDY IN THE CONSTRUCTION OF 'REALITY'

Maura Conway
School of International Relations
University of St. Andrews
Fife KY16 9AL
Scotland
Mc52@st-andrews.ac.uk

Paper presented at the First International Conference on the Information Revolution and the Changing Face of International Relations and Security

Lucerne, Switzerland
23-25 May 2005

"[Cyberterrorism] isn't so much a threat to national security as a threat to civilisation"
- Paul Vixie, *Newsweek* (2003)[1]

"More cyberterroristic than the cyberterrorists themselves, the cyberterror-inducing media have the information world at their mercy"
- François Debrix (2001)

INTRODUCTION

Why is it that some threats take on huge political salience and others do not? Cyberterrorism is thus far noticeable by its absence. Nonetheless, a central element of the post 9/11 'War on Terror' and related efforts to beef-up US 'homeland security' has been an almost paranoid emphasis on the potentially catastrophic threats posed by cyberterrorism. A vast array of political, military, business, academic, and media commentators have appeared on television and been quoted in newspapers predicting

[1] Vixie was, at that time, president of the Internet Software Consortium (an industry group). See Adams & Guterl, 2003.

deadly attacks by terrorists on the computerised infrastructures that now constitute the structures of everyday American urban life. This depiction of computerised systems as the Achilles heel of advanced industrial societies was further fuelled by the use of everyday urban infrastructures as weapons of mass murder on 9/11 itself (Graham 2004).

Following the decline of the USSR, a number of events occurred that highlighted the growing influence of information technology in the realms of both national and international security. Examples include the high level of IT capability manifested by US troops in the first Gulf War (1990-1991), the increasingly global nature of media coverage as demonstrated in the Somali (1993) and Balkan conflicts (1992-1998), and increased systems failures resulting from the activities of hackers. These and other events highlighted states', particularly the United States', growing dependence on information technology thus ushering in fears of a radically new security threat: the possibility of information systems serving as both a weapon and a tool of attack. This cyber threat became the object of increased attention from the US federal government in the 1990s. A particular concern was that enemy's of the United States, unable to emerge successfully from an encounter with American forces on the conventional battlefield, would pursue alternative approaches to inflicting damage on the sole remaining superpower (Pollard 2004, 43). The events of 9/11 were therefore doubly shocking for many US government officials: not only were the attacks appalling in themselves, but the conventional nature of the attacks was also completely unexpected.

Far from reducing the fear of cyber attack however, for many the 9/11 attacks only served to increase the credibility of the cyber threat.

According to a study released in June 2001, seventy-five percent of Internet users worldwide now believe in cyberterrorism. The survey conducted in nineteen major cities around the world found that forty-five percent of respondents agreed completely that "computer terrorism will be a growing problem," while thirty-five percent of respondents agreed somewhat with the same statement (Poulsen 2001). In a July 2002 survey conducted by the American Business Software Alliance, eighty-two percent of information technology professionals were said to believe that US businesses were ill equipped to deal with cyberterrorism (King 2002). A more recent survey carried out by *Federal Computer Week* and the Pew Internet and American Life Project in 2003 found that about half of Americans fear terrorists will launch cyberattacks on those critical infrastructures that operate the banking, electrical, transportation, and water systems, disrupting everyday life and crippling economic activity (Pew Internet and American Life Project 2003).[2] What these statistics show is that cyberterror is in the zeitgeist. What this paper seeks to do is to show how it took root there.

THREAT POLITICS

Traditional security studies views threat images as relatively unproblematic and assumes that real threats--out in the world--are directly reflected in security policy. In the last decade or so, practitioners of so-called 'new security' approaches have argued, on the contrary, that there exists no natural or self-evident conformity between the substance of a threat image and whether it has an impact on the political

[2] This survey was conducted before the blackout across the northern United States and eastern Canada on 14 August, 2003.

agenda (see Buzan 1991, Buzan *et al* 1998). The analytical approach adopted here is informed by the framework laid out by Barry Buzan, Ole Wæver and others, who are collectively known as the Copenhagen School,[3] which is closely identified with 'new' security studies.

The Copenhagen School approach to security may be described as broadly constructivist. One of the major issues addressed by Buzan *et al* in their seminal text *Security: A New Framework for Analysis* (1998) is "what quality makes something a security issue in international relations?" (Buzan, Wæver, & de Wilde 1998, 21). The answer, they say, can be found in the traditional military-political understanding of security. According to Buzan *et al*, things are generally designated as security issues because it can be argued that these things are more important than others and should therefore be given absolute priority. The evidence for such prioritising often takes the form of a statement such as "If we do not tackle this problem, everything else will be irrelevant (because we will not be here or we will not be free to deal with it in our own way)" (Buzan *et al* 1998, 24 & 36). In this way, the securitizing actor claims the right to break the normal political rules of the game. It is for this reason that constructivists view 'security' as a self-referential practice, because it is in this practice that issues become 'security issues' (i.e. not necessarily because a real existential threat exists, but because X issue is presented as such a threat). "Thus the exact *definition* and *criteria* of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" [italics in original] (Buzan *et al* 1998, 25). Cyberterrorism, it is

[3] Many of the figures associated with this approach were employed at the Copenhagen Peace Research Institute (COPRI) before it was closed on 31 December 2002.

argued here, has taken on such saliency. As a terrorism subset, it sits atop the US political agenda.[4]

The formation of agendas depends, unsurprisingly, on power and politics. But while this may appear obvious, it is actually perceived as controversial by many in the community of traditional security studies researchers. Olav Knudsen has even suggested that research that investigates how the security policy agenda is set diverts attention away from 'real' problems (2001, 359-61). Security policy researchers rarely have a problem identifying the 'real' threats, but oftentimes these threat images receive very little substantive political attention. The inability of these researchers to get environmental problems taken seriously as a security issue is a case in point. There is thus a very real need for research and analysis which explores why different actors often perceive the same issue in radically different ways, as well as why certain threat images take on political salience and others do not (Eriksson & Noreen 2002, 1).

According to researchers working at the Scandinavian Threat Politics project,[5] to understand the politics of threat one must be concerned with how threat images are created and become part of the political agenda. In the opinion of the Scandinavian researchers two types of studies need to be undertaken in order to understand the politics of threat:

1. Studies that focus on specific substantive issues that, at different times, are either included or dropped from the agenda as threat images.

[4] A number of authors have recently suggested adopting a constructivist approach to analysing the cyberterror threat, see Dunn 2004; Eriksson & Giacomello 2004. For a brief (but friendly) critique of this approach see Deibert 2002, 116-117.

[5] The Threat Politics project is a research project funded by the Swedish Emergency Management Agency in conjunction with the Swedish Institute of International Affairs, Uppsala University, and Södertörns University College. The project Web site is available in English and Swedish and may be accessed online at http://www.threat-politics.net/.

2. Studies that take as their starting point specific political arenas and how threat images are emphasised or downplayed within them.

The present paper seeks to combine both types of study. The Copenhagen approach to security distinguishes among three types of units: referent objects, securitizing actors, and functional actors. ‘Referent objects’ are those things that are seen to be existentially threatened and that have a legitimate claim to survival. Those actors who securitize issues by declaring something (the referent object) existentially threatened are known as ‘securitizing actors,’ while those actors who affect the dynamics of a sector without being the referent object or the actor calling for security on behalf of the referent object, but who nonetheless significantly influence decisions in the field of security are designated ‘functional actors’ (Buzan et al 1998, 36). In the present analysis, the American state--conceived of as the nexus between US territory, government and society--is the referent object: the thing that is claimed to be threatened by cyberterrorism.[6] The US government is the securitizing actor and the American media establishment is the major functional actor. The goal of this paper is to present a unified analysis of the politics of the cyberterrorist threat by focusing on cyberterrorism as a specific substantive threat image and tracing how it has been portrayed in the specific political arena occupied by the American media.

THREAT FRAMING

The process of formulating problems, finding scapegoats, and coming up with solutions has been identified in different contexts as ‘speech acts,’ ‘problem

[6] For a thorough analysis of ‘National security and the nature of the state,’ see Buzan 1991, Ch. 2; Buzan 1995.

definition,' and 'framing.' The problem is to depict an issue--something that is perceived as threatening, for example--in such a way that others listen and are convinced (or are at least persuaded to pay attention to the issue). The term framing is employed here; for Robert Entman,

> [t]o frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described (1993, 52).

Framing is a verbal expression of thought. Individuals perceive and interpret events; events are never simply given. Perception and interpretation are most often followed by verbalisation: that is to say, actors give verbal form to their conceptions of threats and risks. The movement is thus from thought to speech and from the individual to the collective level of analysis. Generally, the choice of "speech costume" has a major impact on whether an issue makes it onto the political agenda (Eriksson & Noreen 2002, 10).

One of the most significant forms of 'threat framing' or 'costuming' is to identify something as a 'security' threat. In the literature, this behaviour has come to be called 'securitization.' Security policy is often regarded as having precedence over all other politics, while national security policy is invariably viewed as the foundation of all security policy: no other societal goals may be achieved unless society's existence may be guaranteed (Wæver 1995, 49). The upshot of this is that security policy and associated threat images are extremely loaded issues (Deibert 2002, 115). Exploitation of the politically loaded concepts of security and threat may, therefore, make it easier to insert an issue onto the political agenda. Threats and vulnerabilities that are securitized in this manner must meet certain criteria that distinguish them from the normal run of the merely political. What are these criteria?

> [S]ecurity is about survival. It is when an issue is presented as posing an existential threat to a designated referent object…The special nature of security threats justifies the use of extraordinary measures to handle them. The invocation of security has been the key to legitimising the use of force, but more generally it has opened the way for the state to mobilise, or to take special powers, to handle existential threats. Traditionally by saying 'security,' a state representative declares an emergency condition, thus claiming a right to use whatever means are necessary to block a threatening development (Buzan, Wæver, & de Wilde 1998, 21; see also Wæver 1995).

This is what, in language theory, is called a speech act. It is the utterance itself that is the act; by saying the words, something is done. A successful speech act is a combination of language and society: that is of both intrinsic features of speech and the collectivity that authorises and recognises that speech.

A speech act has both internal and external conditions. The most important internal conditions are to follow the security form, the grammar of security, and construct a plot that includes existential threat, point of no return, and a possible way out. There are two main conditions attaching to the external conditions of a speech act. The first is the social capital of the speaker (i.e. the securitizing or functional actor) who must hold a position of authority. The second condition has to do with threat: it is more likely that one can conjure a security threat if certain objects can be referred to that are generally held to be threatening. These objects do not, in themselves, necessarily result in securitization, but instead act as facilitating conditions (Buzan *et al* 1998, 33). Importantly, an issue is securitized only if and when the target audience accepts it as such.[7]

Agenda Setting

In terms of agenda setting, there are two main approaches: one that focuses on elites and the other pluralist-based. The elite approach focuses on formal political power and highly-placed decision-makers, while the second approach broadens the concept of the 'political agenda' to include such factors as the agenda(s) of the media. As already indicated, it is the role of the latter that is explored here, although it must be emphasised that issues that receive attention in the media, but not the attention of decision-makers will not appear on the political agenda. Nevertheless, the media remains a central player because it is able, among other things, to influence public opinion: an issue that achieves salience in societal debate may be expected to make its mark on the political agenda (Eriksson & Noreen 2002, 4). The contention here is that the American news media act as the main source of political information for mass publics--both within the United States, but increasingly, due to the spread of satellite television and the Internet, also abroad--and as the primary 'transmission belt' communicating public fears and desires to political elites and government actors. The "media establishment" has been described as a "major power broker" which exerts

[7] A discourse that seeks to present something as an existential threat, but without evidence of audience acceptance is known as a 'securitizing move' (Buzan *et al* 1998, 25). For details of failed securitization projects (undertaken on behalf of the state), see Marsh 1995.

"unprecedented power over the dissemination of news" (West 2001, viii). In fact, Timothy Cook identifies the news media as a political institution in itself because it "engages, along with other political institutions, in the authoritative allocation of values in American society" (1998, 85-86). Not only does it act as an intermediary between the mass public and the government, but also within and among branches of government. Gronke and Cook go even further when they posit that "in a system of declining rates of affiliation with political parties and falling levels of participation in community, civic, and other political organisations, it is not unreasonable to suggest that the news media is *the* dominant intermediary organisation in American democracy" (2002, 1). As a functional actor, therefore, the media is unparalleled.

Methodology

Buzan *et al* advise that the way to study securitization is to study discourse and political constellations (1998):

> [A] threat image first appears in the mind, whether it is a reaction to something real or merely a work of the imagination. Human cognitive and memory functions play a role in this context. One's conception of a threat may, of course, stop with the thought. In such case, the threat image becomes neither an object for framing nor political action. In other words, it is impossible for a threat image to gain salience if it has not been given some sort of form for decision-makers. It is not sufficient merely to think about threats. They must also be talked about or written about in order to draw attention to them. The way in which this is done

> has an impact on their success; that is, their effects on the agenda" (Eriksson & Noreen 2002, 18).

Threat is first constructed in the individual conscious; individuals view something as a threat. The next step is for actors in the threatened society to give form to the threat by talking or writing about it in public fora. That is, the threat assumes the trappings of language and is transformed into a topic of public debate through the dissemination of newspaper stories, magazine articles, television documentaries, and eventually mass-market books and movies. Opinion polls are an important source for determining public responses to the threat image as amplified in the latter.[8] Should public debate reach a high enough level of saliency, the threat will become part of the political agenda and an object of political consideration and action. Once the threat becomes the object of government reports and legislation, the threat has effectively been securitized.

FEAR OF TECHNOLOGY, FEAR OF TERRORISM

Frequently, it is our basic perceptions that determine how we conceive of an issue, which is filtered through our prism of preconceived notions. A large amount of social psychological research has found that the uncertain and the unknown generally produce fear and anxiety. This is the psychological basis of the classic ghost story: the fear is greatest when you suspect something, but you're not certain what it is (Eriksson & Noreen 2002, 8). The term cyberterrorism unites two significant modern

[8] However, for some of the pitfalls in relying on opinion polls, see Bennett & Entman 2001, 5-6; Entman 2000, 19-23.

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” (Laqueur 1999, 254). As significant uncertainties or unknowns, both technology and terrorism are perceived as more ominous than known threats (Embar-Seddon 2002, 1034).

Fear of terrorism,[9] conceived of as random, incomprehensible, and uncontrollable violence, may strike one as relatively ‘normal,’ fear of technology as perhaps less so. However, as Mark Pollitt points out, for those unfamiliar with high technology, it is arcane, complex, abstract and indirect in its impact on individuals. And “because computers do things that used to be done by humans, there is a natural fear related to a loss of control. People believe that technology has the ability to become the master, and humanity the servant.” Couple this relatively new fear with the age-old fears associated with apparently random violence and the result is a truly heightened state of alarm. Pollitt contends that the media have further upped the ante by hyping the concept of convergence:[10]

> According to the press, one is led to believe that all of the functions controlled by individual computers will all converge into a singular system. Further support for this scenario is the increase in ‘connectivity.’

[9] See Homer-Dixon (2002, 57-58) for an interesting take on the fears exploited by the 9/11 attackers and how the “neural network” compounded these.

[10] The Oxford English Dictionary (2003) defines convergence as “The process by which originally distinct technologies may become more compatible or integrated as they develop, so that an increasing number of devices (esp. in electronics, computing, and telecommunications) are multifunctional and interoperable.”

> Many people conclude that the entire world will soon be controlled by a single computer system (1991, 8).

The convergence represented by the reliance on uninterrupted systems of electrically powered computer networks to support all other infrastructures makes attacks on the electrical power grid particularly fearful. The result is that many people now feel themselves "hostages to electricity" (as quoted in Graham 2004, 8). These feelings are reinforced by the prevalence of so-called 'shut-down-the-power-grid scenarios' in the mass media.[11] Two of the most well known scenarios[12] are those designed by John Arquilla of the Naval Postgraduate School in Monterey, California[13] and technology journalist Dan Verton.

Shut-Down-the-Power-Grid Scenarios

John Arquilla's 'The Great Cyberwar of 2002' first appeared in *Wired* magazine in February 1998. In the scenario "Liddy Dole faces the biggest crisis of her presidency: the first global cyberwar, where the enemy is invisible, the battles virtual, and the casualties all too real" (Arquilla 1998). The electric grid is one of the first infrastructures to be targeted by the attackers:

[11] A number of academic analyses of cyberterrorism also include such scenarios, see Collin 1998; Devost, Houghton, and Pollard 1996 & 1997. Thomas Homer-Dixon, writing in *Foreign Policy*, introduces his comments with a brief shut-down-the-power-grid scenario, although his is not cyber-based, but involves only physical attacks (2002, 52-53).

[12] Postmodernists prefer the term 'simulations' (see Baudrillard 1983).

[13] Together with his collaborator David Ronfeldt of Rand, Arquilla is a prominent analyst of information warfare. Arquilla and Ronfeldt are perhaps best known for their development of the concepts of Netwar and cyberwar. Many of their publications are available for download from the Rand Web site at http://www.rand.org.

> Power outage!….The latest TV news reports indicate that three 500-kilovolt transmission lines extending from hydroelectric dams along the West Coast [*sic*] were knocked out, interrupting electricity and phone service throughout California and Oregon. The executive director of the Western Systems Coordinating Council reported that the problem has cascaded throughout the grid, knocking power plants offline in Rock Springs, Wyoming, in Hells Canyon, Idaho, and in Brush, Colorado, causing outages in several western US states. Reports by noon or so also indicate that no signs of sabotage have been detected. That means no physical destruction of the system (Arquilla 1998).

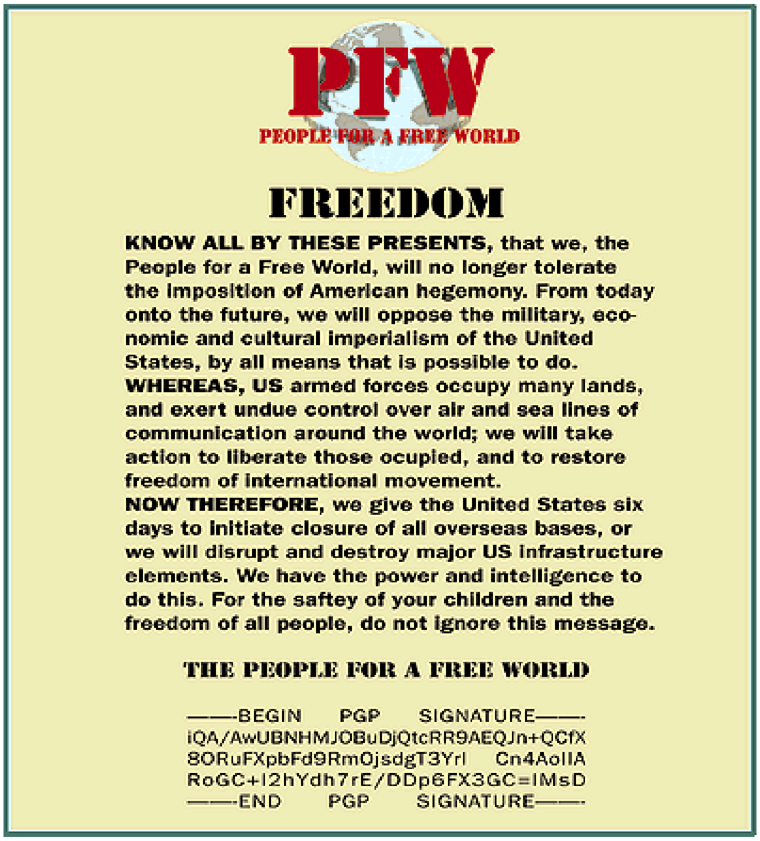
The body count escalates rapidly caused by everything from traffic accidents to the explosion of a chemical plant. Who are the perpetrators of this mayhem, according to Arquilla's scenario? A group known as the Dove of Jihad claim responsibility, but this is quickly dismissed; China and Russia are then held responsible, followed by a shadowy figure operating out of Afghanistan(!). Eventually, however, the perpetrators are identified as a coalition of states including North Korea, Vietnam, Iraq, and Libya, aided by the Cali cartel in Colombia and various Asian triads.

Arquilla's scenario is somewhat tongue-in-cheek, and he eventually--the scenario runs to over twenty printed pages--identifies a coalition of states, and not terrorists, as those responsible. This outcome is foreshadowed by the scenario's title: 'The Great Cyberwar.' Arquilla, and his collaborator David Ronfeldt, distinguish in their work between cyberwar and Netwar; cyberwar is the domain of states, while cyberterrorism may be viewed as a category of Netwar, which is the domain of non-/sub-state actors (Arquilla & Ronfeldt 1993, 1996). Nonetheless, there is a cyberterror component to the scenario in that a number of real and fictional terrorist groups are mentioned, and the coalition of states that are eventually found to be behind the attacks seek to conceal themselves by dubbing their group People For a Free World (see Figure 1), which is reminiscent of the names of a number of terrorist organisations, including the Weather People and the New People's Army, amongst others.

François Debrix's choice of Fox TV documentary *Dangers on the Internet Highway: Cyberterror* (broadcast in the US in Autumn 1999) to illustrate his argument regarding the hype surrounding the subject of cyberterrorism is interesting from our perspective because the programme is developed around the scenario of "the world's first cyber or Netwar." The programme-makers argue that America's reliance on ICTs is the country's "Achille's Heel," insisting that "the cyber frontier is the next venue for war" and that "cyberwarfare is taking the Internet to its most lethal level" (2001, 154). Various info-war specialists, including John Arquilla, sketch the impacts of a supposed series of escalating cyber attacks: the collapse of air traffic control systems resulting in multiple airplane crashes, overloaded digital networks resulting in collapsed finance and e-commerce networks, collapsed power grids, non-functioning telephone networks, widespread car and train crashes, and nuclear meltdowns. In the television scenario, even the US's ability to fight a conventional war is wiped out due to the coordinated hacker attacks. "Meanwhile, the perpetrators of the war remain undetected behind their distant, encrypted terminals, free to bring the world's mightiest nation to its knees with a few keystrokes in total impunity" (Graham 2004, 18).

Fox TV's scenario bears some striking resemblances to Arquilla's contribution to *Wired* just a few months earlier, but there are also some striking differences. On the

Figure 1 Graphic Accompanying ‘The Great Cyberwar of 2002’
***Wired* 6(2), 1998**



PFW
PEOPLE FOR A FREE WORLD

FREEDOM

KNOW ALL BY THESE PRESENTS, that we, the People for a Free World, will no longer tolerate the imposition of American hegemony. From today onto the future, we will oppose the military, economic and cultural imperialism of the United States, by all means that is possible to do.
WHEREAS, US armed forces occupy many lands, and exert undue control over air and sea lines of communication around the world; we will take action to liberate those ocupied, and to restore freedom of international movement.
NOW THEREFORE, we give the United States six days to initiate closure of all overseas bases, or we will disrupt and destroy major US infrastructure elements. We have the power and intelligence to do this. For the saftey of your children and the freedom of all people, do not ignore this message.

THE PEOPLE FOR A FREE WORLD

```
———-BEGIN    PGP    SIGNATURE———-
iQA/AwUBNHMJOBuDjQtcRR9AEQJn+QCfX
8ORuFXpbFd9RmOjsdgT3Yrl    Cn4AoIlA
RoGC+I2hYdh7rE/DDp6FX3GC=IMsD
———-END    PGP    SIGNATURE———-
```

one hand, the described outcomes of the cyber attack(s) are strangely similar. On the other, while cyberterrorism is explicitly referred to in the programme’s title, the perpetrator of the attacks is unveiled as a little-known country previously thought to have little IT capacity. This does not square with Arquilla’s academic analyses of potential cyber threats, which make an explicit distinction between the activities of hostile states (cyberwar) and those of sub-state organisations (Netwar, a subset of which is cyberterrorism).

Over the course of the next few years, the emphasis in terms of the cyber threat image shifts from states to terrorists and back again.[14] Nobody's quite sure whom they ought to be more afraid of: states or terrorists? Many journalists mix their message and warn that both types of actors are equally threatening.[15] In May 2001, no less august a publication than the *New Yorker* assured its readers that "sophisticated terrorists (or hostile governments) now have the ability to crash satellite systems, to wage economic warfare by unplugging the Federal Reserve system from Wall Street, even to disrupt the movements of ships at sea" (Specter 2001). While in June an article in *USA Today* entitled 'Cyberspace: The Next Battlefield,' asserted "an adversary could use…viruses to launch a digital blitzkrieg against the United States. It might send a worm to shut down the electric grid in Chicago and air traffic control operations in Atlanta, a logic bomb to open the floodgates of the Hoover Dam and a sniffer to gain access to the funds-transfer networks of the Federal Reserve" (Stone 2001). Post 9/11, however, the spectre of cyberterror took on a new urgency.

In 2003, Dan Verton, a technology journalist,[16] contributed *Black Ice: The Invisible Threat of Cyberterrorism*, an analysis of the cyberterrorist threat aimed at the mass-market. The first chapter of Verton's book describes a coordinated series of cyber and physical attacks on critical infrastructures in the US's Pacific Northwest

[14] In his article 'The American Cyber-Angst and the Real World' (2003), Ralf Bendrath traces the course of the cyber threat image between c. 2000 and 2003 from cyberterrorists to states, back to cyberterrorists and, perhaps, back to states again.

[15] In June 2001, Lawrence K. Gershwin, a top CIA official, took a similar stance in a statement to the Joint Economic Committee of the US Congress. Gershwin told the Committee that foreign governments, rather than terrorists, were the most significant threat to US computers for the next five to ten years. "Terrorists really like to make sure that what they do works….They do very nicely with explosions, so we think largely that they're working on that." Nonetheless, Gershwin warned that a terrorist organisation could surprise intelligence officers and mount a cyber attack within the following six months (see Associated Press 2001; Joint Economic Committee 2001, 6-10).

[16] This is not to suggest that all journalists, without exception, are guilty of hyping the cyberterrorist threat. It is possible to point to the efforts of some journalists--technology journalists, in particular--to desecuritize cyberterrorism. See, for example, Declan McCullagh's contributions to *Wired* and *C¦Net News*; Thomas C. Greene and others in *The Register*; Bruce Schneier in his books, articles, and *Cryptogram* newsletter (http://www.schneier.com/crypto-gram.html); and a goodly amount of the commentary on cyberterrorism produced by *ZDnet* ('Information Resources for IT Professionals').

(2003, 1-16). The attackers carry out a series of suicide bombings using conventional explosives and anthrax-laced powder, they unleash malicious software code which targets Internet root servers and mobile phones, they deface the Web pages of a number of major news organisations, and they set off an electromagnetic pulse (EMP) bomb. Verton is clear as to the perpetrators; a collection of sub-state actors comprising a core group of al-Qaeda members, aided by Russian hackers and a number of disgruntled energy company employees with rightwing sympathies. The effects of the attacks are described thus:

> The power outages last for weeks, in some areas, for months. System failures begin to cascade out of control and are felt as far south as California….Medical facilities quickly enter crisis mode as they are forced to rely on back-up power generators for critical care systems….[T]he lack of telecommunications makes coordinating medical emergencies and sharing data on the possible biological or chemical cases nearly impossible. Businesses, banks, government offices, industrial plants, and manufacturing firms are also starved of connectivity. Some will be forced to close their doors for good…Failures and disruptions ripple through potable water control systems, the computers that manage sewage treatment plants, and chemical and oil refineries (Verton 2003, 14-15).

One sceptical reader describes Verton’s contribution as “paranoid speculation,” and lambastes Verton for his contention that “we can safely discard the opinions of those who argue that cyberterrorism….is impossible" (Greene 2004; Verton 2003, 96).[17] However, such contentions are accepted/acceptable because events in our media-saturated world are allowed to be at one true and false, real and fictional. Verton concludes his scenario with the following observation:

> This is the face of the new terrorism. It is a thinking man's game that applies the violent tactics of the old world to the realities and vulnerabilities of the new high-tech world. Gone are the days when the only victims are those who are unfortunate enough to be standing within striking distance of the blast. Terrorism is now about smart, well-planned indirect targeting of the electronic sinews of a nation (Verton 2003, 15-16).

He thus transforms his imaginings from prediction to reality. In a similar fashion, the narrator of Fox TV's *Dangers on the Internet Highway* assures viewers that the information contained therein "is not science fiction" (Debrix 2001, 154), intimating that it is thus 'science fact.' Jean Baudrillard, has labelled this condition of undecidability of the event and uncertainty of meaning "hyperreal" modernity. Hyperreality occurs when the media uses its technological capabilities to paint something as more true to life than the object it is purporting to represent (Baudrillard 1983;see also Der Derian 1995, 37-41).

François Debrix suggests that Verton's and Arquilla's musings along with other, similar scenarios give the impression that:

[17] For an article which takes many of the incidents outlined in the scenarios above, interrogates the likelihood of their successful occurrence, and finds them wanting, see Cohen 2003.

> [T]he next Pearl Harbor will be both everywhere and nowhere at the same time. It's targets will not be the US military or defence system but, instead, the US public and its post-industrial and highly informatized lifestyle. What is now a tool for comfort, an object of leisure, or a necessary support for work….will become the world's deadliest weapon (2001, 156).

Debrix notes that popular fears have taken on a new gravity and emergency responses have become everyday realities in media-saturated societies. This is perhaps especially true in post-9/11 America. Debrix suggests that:

> In a generalised context of uncertainty, common anxiety and more or less planned strategies of emergency give rise to social epiphenomena like cyberterror, its at once real and imagined dangers, and its often paranoid responses. In a context where information becomes knowledge, there is no way of distinguishing cyberterrorism from its representations (on TV, in security literatures, as hypertext on the Web) (Debrix 2001, 153).

The exaggerated nature of the scenarios imagined by Verton, Arquilla, and others is further highlighted when one considers that blackout, failure, and accident are part of the normal operating environment of networked computer and infrastructure systems. It is worth keeping in mind that "water system failures, power outages, air traffic disruptions, and other cyberterror scenarios are routine events that do not always affect national security. System failure is a routine occurrence" (as quoted in Graham 2004, 21). In a relatively sober analysis that appeared in *Jane's Intelligence Review* in 1999, it was observed 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 (Ingles-le Noble 1999).

Thus far, cyber-error has proved more frequent and more debilitating than cyberterror. In terms of electrical power, most outages occur due to natural phenomena such as severe weather. In August 2004, Hurricane Charlie ravaged parts of the American state of Florida and it was reported that "it will be weeks rather than days before the most storm-ravaged parts of [Florida] have electricity." This is because the damage was so severe that parts of the power system had to be rebuilt. When Hurricane Andrew devastated the Miami Area in August 1992, it was fully five weeks before power was restored to all the local supplier's customers (Mayk 2004; Wald 2004).

REASONING BY ANALOGY

The importance of basic conceptions is illustrated, within cognitive research, by explanation by analogy, which is a problem-solving method in which knowledge of previous problems with allegedly similar structures is used to find the best way to solve current problems. Within the cyberterror threat discourse the most prevalent analogy is the possibility of an ‘electronic Pearl Harbour.’ The comparison of so-called ‘weapons of mass disruption’ with ‘weapons of mass destruction’ (WMD) is another popular play on words.

Electronic Pearl Harbour

Winn Schwartau of infowar.com first used the term ‘Electronic Pearl Harbour’ in testimony before the US Congress as early as 1991 (see Schwartau 1994, 43).[18] This analogy links the cyber security debate to a ‘real’ and successful surprise attack on critical US military infrastructures during World War II while, at the same time, warning against the idea of American invulnerability due to its geographical position. The Pearl Harbour analogy is used with startling frequency in the media as a shorthand description of the likely consequences of a cyberterrorist attack on the United States. A Lexis-Nexis search of major world newspapers found 105 mentions of this and related terms[19] in the ten years between 1994 and 2004.

[18] Ralf Bendrath describes Schwartau as “the rock manager turned preacher of ‘information warfare’” (2003, 49). In the aftermath of 9/11, Schwartau re-released his 1991 novel *Terminal Compromise* under the new title *Pearl Harbour Dot Com*. The following description of the novel is provided on Amazon.com: “It used to take an entire nation to wage a war. Today it takes only one man. Taki Homosoto survived the hell of Hiroshima. Now, more than 50 years later, the time has come for the Americans to feel the flames of his revenge, using his personal army of terrorists and intelligence agents. The US Government and a network of somewhat reluctant allies - invisible and anonymous hackers join forces to battle this powerful enemy. The devastating climax of this one man's plan...this powerful, bitter survivor of *ayamachi*, The Great Mistake, is certain to bring global chaos and economic meltdown. A terrifying thought provoking tale.”

[19] The search was undertaken on 18 August 2004 and used the terms ‘electronic Pearl Harbour’ (68), ‘digital Pearl Harbour’ (35), and ‘cyber Pearl Harbour’ (2).

The term ‘electronic Waterloo’ has found less favour in the media: a Lexis-Nexis search of major world newspapers found just eight mentions of this and related terms between 1998 and 2004.[20] Just one of these appeared in a US newspaper (*The New York Times*), the rest appeared in British (4) and Canadian (3) publications, whose readers may be expected to be more familiar with said battle.[21] Nevertheless, it has been asserted that the Waterloo analogy is the more accurate of the two. This is because the visions conjured up by reference to an ‘electronic Pearl Harbour’ are of a sudden crippling blow against critical infrastructures resulting in chaos and destruction. However, it has been argued that this “bolt-out-of-the-blue scenario” is not the most significant cyberwarfare threat to the United States. The greater danger, according to analysts at the Centre for Strategic and International Studies, is a meticulously planned, carefully executed campaign by a focused adversary with a thorough grounding in information warfare techniques. The most important feature of such a strategy, according to the CSIS document, would be its contribution to important strategic goals as part of a larger-scale, possibly long-term strategy. It would not, in other words, be intended simply to gain the public spotlight, create havoc, or win a temporary edge in battle.

> Although the attack on Pearl Harbour precipitated major strategic change, the attack itself was a single blow that failed to achieve Japan’s strategic objective, which was to force the United States to an accommodation more

[20] The search was undertaken on 18 August 2004 and used the terms ‘electronic Waterloo’ (5), ‘digital Waterloo’ (3), and ‘cyber Waterloo’ (0).

[21] The Battle of Waterloo was fought thirteen kilometres south of Brussels, Belgium between the French, under the command of Napoleon Bonaparte, and the Allied armies commanded by the British Duke of Wellington and Prussian General Blücher. The French defeat at Waterloo drew to a close twenty-three years of war beginning with the French Revolutionary wars in 1792 and continuing with the Napoleonic Wars from 1803. Napoleon's final defeat at Waterloo marked the end of the Emperor's final bid for power, the so-called 'One Hundred Days', and the final chapter in his remarkable career.

> favourable to Japan’s then expansive foreign policy. The more significant information warfare threat would likely resemble not Pearl Harbour but instead Waterloo, where technology, planning, and careful execution were used as part of a long-range plan aimed at altering the world’s political, military and economic order (CSIS 1998, 2).

The almost complete absence of references to an ‘electronic Waterloo’ in the US media is an indication of the necessity for threat images and related analogies to have immediate resonance and attract wide understanding. Their aim is not actually to explain anything about cyberterrorism, but to manufacture fear and to do so in the simplest and most direct way possible.

Weapons of Mass Disruption

In the wake of 9/11, threats to the integrity of America’s information infrastructure have been ascribed a level of urgency analogous to nuclear and biological threats, which has galvanised the relationship between IT and security as a primary policy consideration in the United States (Yould 2003, 75). In September 2002, Richard Clarke, former Special White House Adviser for Cyberspace Security, told ABC News: “[Cyberterrorism’s] much easier to do than building a weapon of mass destruction. Cyberattacks are a weapon of mass disruption, and they’re a lot cheaper and easier” (Wallace 2002). Howard Schmidt, Clarke’s one-time deputy, has also repeatedly referred to the threat from ‘weapons of mass disruption’ (see, for example, McGray 2003). But even before 9/11 the American “cyber-angst” was palpable

(Bendrath 2003).[22] As early as 1999, Congressman Curt Weldon (R-Pennsylvania) placed cyberterrorism at the top of his list of modern threats to the American way of life. Speaking at the InfoWarCon conference to an audience of uniformed military personal, corporate IT managers, computer security consultants, and at least one screenwriter,[23] Weldon said "In my opinion, neither missile proliferation nor weapons of mass destruction are as serious as the threat [of cyberterrorism]" (Poulsen 1999). In May 2001, Senator Robert Bennett (R-Utah), stated "[Attacks against the US banking system] would devastate the United States more than a nuclear device let off over a major city" (Porteus 2001). At around the same time, Michael Specter (2001), author of *The New Yorker* article alluded to above, predicted: "The Internet is waiting for its Chernobyl, and I don't think we will be waiting much longer." Such predictions are not limited to US commentators. A 2003 *Newsweek* article quoted John Naughton, described as "an Internet expert at Britain's Open University," as saying "If I were Al Qaeda, I wouldn't waste time with nuclear weapons. I'd be going to Microsoft training courses" (Adams & Guterl 2003)

In her seminal article on the role of linguistic metaphors, puns, and acronyms in the field of nuclear defence strategy, Carol Cohn demonstrated how specific uses of language were used to de-dramatise the actual threat (see Cohn 1987). With regard to the cyberterrorist threat, exactly the opposite is happening. Far from de-realising the threat, the discourse of cyberterrorism mobilised by the media and assorted 'experts' makes it possible. Mediatised discussion of just about any topic fosters the formulation of buzzwords and catchy phrases. The designation of cyber threats as 'weapons of mass disruption' directly analogous to 'weapons of mass destruction'--

[22] François Debrix uses the term "e-anxiety" (2001, 165).

[23] In an article for *Foreign Policy* magazine, Thomas Homer-Dixon claims that the US Army enlisted the help of some of Hollywood's top screenwriters and directors--including the creators of *Die Hard* and *McGyver*--to dream up possible scenarios for future terrorist attacks (2002, 61).

that is nuclear, biological, or chemical weapons--is, however, both inaccurate and unhelpful in terms of advancing ideas about the relationship between national security and IT. This is true whether one believes such threats are imminent (see Yould 2003, 84-88) or one is sceptical of the cyberterrorist threat. For sceptics, equating the effects of a cyber attack on the US banking system with the effects of the Chernobyl disaster is not only an exaggeration that defies corroboration, but is extremely disingenuous suggesting as it does that the physical (and continuing) death of not just large numbers of people, but literally the whole of a vast territory, is less significant than its digital disconnection (see Cohen 2003, 9-10). The functions of such comparisons are clear however: "Urgency; state power claiming the legitimate use of extraordinary means….*Survival* might sound overly dramatic but it is, in fact, the survival of the unit *as* a basic political unit--a sovereign state--that is the key" [italics in original]. Public perceptions are thus massaged, so that issues such as cyberterrorism, portrayed as having this "undercutting" potential are accepted as having to be addressed prior to all others because, if they are not, the state will cease to exist as a sovereign entity, and all other questions will thus be irrelevant (Wæver 1995, 51 & 53).

IDENTIFYING ANTAGONISTIC ACTORS

The securitization of cyberterrorism is also about specific hostile actors. Traditionally, the focus in security policy analysis has been on potentially threatening states or governments, but in debates about terrorism and information warfare it has been emphasised that non-state actors too may pose a threat. The idea that anonymous adversaries may attempt to penetrate information systems from anywhere in the world breaks with the traditional understanding of security--that the identity, location, and goals of the enemy are known--and increases the sense of fear and insecurity. “The introduction of *non-state enemies* in security thinking implies opening up Pandora’s box, as the number of potential enemies in ‘cyberspace’ is virtually unlimited” [italics in original] (Eriksson 2001, 218). In terms of IT security, Denning has posited five different types of antagonistic actors: insiders, hackers, criminals, corporations, governments, and terrorists (1999, 26-27). The media have concerned themselves, for the most part, with just two of these: hackers and terrorists.

Terrorist Hackers

In the cyberterror scenarios described here, governments and terrorists were portrayed as the main threats, but hackers were also mentioned. Previous to 9/11, the media were fixated on hackers as antagonistic actors. A reliance on cyberterror simulations alone would have made it difficult to securitize the cyberterrorist threat. This was unnecessary however, because hackers, conceived of as computer abusers, had a history of demonisation in movies, on TV, and in the press. Being “familiar, even archetypal characters” (Entman 2000, 15), when the cyberterrorist threat image was being constructed, they were the perfect candidates for identification as potential perpetrators. It is the classic case of the emergence of “the worst-case result [out] of a dialectic between what is observed and what is imagined” (Lipschutz 1995, 2).

The threat of hackers infiltrating the world’s most sensitive military systems is one of the most enduring and popular themes associated with hacking. It was first brought to the public’s attention by the 1983 film *War Games*. In the film, a teenage boy hacks into the computer that monitors and controls the US nuclear and defence system. Believing that it is simply a game-playing machine, the teenager begins a game with the computer. However, the computer believes the game is ‘real’ and begins the countdown to WWIII.

> Wigan (FBI): The Kid Claims he was looking for a toy company. Ha! Ha! That’s great!
>
> McKittrick (System Manager): There is no way a high school punk can put a dime in a telephone and break into our systems. He has got to be working for someone else. He’s got to be!
>
> Wigan: He does fit the profile perfectly: he is intelligent but an underachiever, alienated from his parents, has few friends, a classic case for recruitment by the Soviets. Now what does this say about the state of our country? Have you got any insight into why a bright boy like this would jeopardise the lives of millions?
>
> FBI Agent: No, Sir, he says he does this sort of thing for fun! (War Games 1983)

This scenario resonated deeply with the US public. On his arraignment on charges related to hacking Kevin Mitnick was denied access not only to computers, but also to a phone, because the judge believed that, with the aid of a phone, Mitnick could set off a nuclear attack (see also Ryan 2004, 8-9).

In his book *Hackers*, Paul Taylor describes a 1991 episode of the US chat show *Geraldo* (1998, 178-179). The show’s introduction featured excerpts from the film *Die Hard II*, in which terrorists take over the computers of an airport, while the studio section of the show included an interview with Craig Niedorf (aka Knight

Lightning), who was the subject of a US court case for having allegedly received the source code of the emergency services telephone computer programs. During the course of the program Geraldo repeatedly referred to Niedorf as the ‘Mad Hacker.’ The prosecuting attorney in Niedorf’s case also appeared on the show. Below is an excerpt of the dialogue that ensued:

> Geraldo: Don, how do you respond to the feeling among so many hackers that what they’re doing is a public service; they’re exposing the flaws in our security systems?
>
> Prosecutor: Right, and just like the people who rape a co-ed on campus are exposing the flaws in our nation’s higher education security. It’s absolute nonsense.

And on the issue of punishment of hackers:

> Prosecutor: I don’t think they’re being punished very much at all. We’re having trouble even taking away their gear. I don’t know one of them [who] has done hard time in a prison….even Mitnick who is a real electronic Hannibal Lecter….did not get near any of the punishment that what he was doing entitled him to (as quoted in Taylor 1998, 178).[24]

[24] In the movie *Silence of the Lambs* (1991), Hannibal Lecter (as played by Anthony Hopkins) is a respected psychiatrist turned murderous cannibal.

At the very end of the show, Geraldo asks the prosecutor to give a brief worst-case scenario that could result from the activities of hackers. He replies: “They wipe out our communications system. Rather easily done. Nobody talks to anyone else, nothing moves, patients don’t get their medicine. We’re on our knees” (as quoted in Taylor 1998, 179).

Hackers get a lot of bad press, some of it deserved, some less so. In terms of the securitization of the cyberterrorist threat, the portrayal of hackers as potential adversaries was not restricted to film and television, they were repeatedly identified in the press as the most likely threat actors. The following quote from a 2003 *Newsweek* article entitled ‘Bringing Down the Internet’ is typical:

> If you wanted to write a science-fiction thriller about the day the Internet crashed, you’d start with a computer geek. Armed with nothing but a laptop and a high speed Internet connection, he releases a fast spreading computer virus that in a matter of minutes gives him control of thousands, perhaps millions, of personal computers and servers throughout the world. This drone army launches a silent and sustained attack on computers that are crucial for sending around the billions of packets of data that keep e-mail, the Web and other, more basic necessities of modern life humming. At first the attack seems to be an inconvenience--e-mail traffic grinds to a halt, Web browsing is impossible. But then the problems spread to services only tangentially related to the Internet: automated-teller machines freeze up, calls to emergency numbers fail to get routed to police stations and ambulance services, airport- and train-reservation systems come down. After a few hours, the slowdown starts to affect

> critical systems: the computers that help run power grids, air-traffic control and telephone networks (Adams & Guterl 2003).

According to the authors of this particular scenario, the cascading failures are not just regional or national in scope, but global. And within a few lines of text the perpetrators morph from “hackers” to “geeks” to “terrorists.” The problem is that even if ‘hackers’ managed such a feat, it’s not cyberterrorism unless they engaged in the act for political purposes. Most journalists are either unaware of, or ignore, this caveat. They’re equally ignorant of the BTKP rule. That is the requirement that violence labelled terrorism result in death and/or serious destruction, the so-called ‘break things and kill people’ (BTKP) rule (Giacomello 2003, 8).

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.” 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’ (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, 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’ was thought 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,” said 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 had increased across the United States since the events of 9-11 and law enforcement had traced many of the attacks to Pakistan and Egypt.[25]

The press have labelled some unlikely acts of computer abuse as ‘cyberterrorism’. According to reports, 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 (see Ross 2000, 255). Admittedly, terrorism is a notoriously difficult activity to define; however, the addition of computers to plain old criminality it is not. So what are the functions of these sorts of reports? They result in a widening of the

[25] It was predicted that an escalation in hack attacks would occur in the aftermath of 9-11 (ISTS 2001). 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.

category of cyberterrorism, which is crucial, as no ‘true’ act of cyberterrorism, narrowly defined, has ever yet occurred. In order to make the cyberterrorist threat image credible therefore the cyberterror scenarios must be represented as paroxysmal versions of a cyberterror that starts all the way from the teenage hacker.

It seems that even hackers themselves--albeit probably of the script kiddy variety--have begun to be influenced by their portrayal in the media. The anonymous defacement of two US government Web sites, carried out in late November 2001, read as follows: “we are not hacker, we are just cyberterrorist.” Elsewhere the defacers referred to themselves as “mujihadeens” and threatened “the greatest cyberterrorist attack against American government.” The culprits were almost certainly neither mujihids nor terrorists. It is almost unheard of for a terrorist organisation to refer to themselves as such. In fact many groups use the term ‘army’ in their self-descriptions as evidence of the legitimacy of the group and their cause (e.g. Irish Republican Army, Irish National Liberation Army, New People’s Army, etc.). The perpetrators of the ‘attack’ described above, on the other hand, are evidently more familiar with media portrayals of cyberterrorism than with any ‘real’ cyberterrorists (2001a).

It has been observed that all the various ways of abusing computers and IT can hardly be deemed existential threats to sovereign states (Erikkson 2001, 218). Nonetheless,

> The rhetoric surrounding computer hacking consistently reinforces the potentially catastrophic economic and national security threats posed by malevolent intruders, and at the same time attaches the subject of this threat to young obsessive, self-trained computer aficionados. This raises

> the fundamental question: how can self-trained teenagers be a match for the security devised by governments and corporations that are literally willing to spend billions of dollars safeguarding computer systems and cracking down on computer criminals? (Skibell 2002, 336)

In fact, recently the media have reassessed the hacker-as-terrorist discourse, which had begun to appear increasingly unconvincing. In the wake of 9/11, this discourse has been superseded by the terrorist-as-hacker approach.

Hacker Terrorists

The 9/11 attacks resulted in a complete change in threat perceptions, both in terms of the threat from conventional terrorism and its cyber dimension. Ralf Bendrath details how, in the immediate aftermath of the attacks, newspaper articles addressing the threat of cyberterrorism proliferated (2003, 59-60). A Lexis-Nexis search of major US newspapers showed that in the US newspapers of record, the *Washington Post* and *New York Times*, mentions of cyberterrorism doubled in the aftermath of 9/11 (see Table 2.1). This upswing of interest in cyberterrorism was not limited to the US press, a similar trend was noticeable in British newspapers (see Table 2.2). The question on many people's lips was 'Is Cyber Terror Next?' (Denning 2001).

Once Osama bin Laden and Al-Qaeda had been fingered as the perpetrators of the 9/11 attacks, a steady stream of newspaper articles began to appear suggesting that the latter were now engaged in planning a major cyberterrorist attack.

Table 2.1

Cyberterrorism in US Newspapers Before and After September 11, 2001

Newspaper	*Pre 9/11**	*Post 9/11***	*Total*
	(N)	(N)	(N)
Washington Post	19	41	60
New York Times	15	30	45
Philadelphia Inquirer	10	5	15
Miami Herald	4	7	11
International Herald Tribune	5	3	8

* From first recorded mention in June 1996 to 10 September, 2001.
** 11 September, 2001 to August 2004.
N = Number of articles mentioning the search words
Source: Compiled from Lexis-Nexis archives using the search words 'cyberterrorism,' and 'cyber terrorism.'

Table 2.2

Cyberterrorism in UK Newspapers Before and After September 11, 2001

Newspaper	*Pre 9/11**	*Post 9/11***	*Total*
	(N)	(N)	(N)
Financial Times	16	20	36
Guardian	11	20	31
Times	10	8	18
Independent	7	10	17
Mirror	3	10	13

* From first recorded mention in June 1996 to 10 September, 2001.
** 11 September, 2001 to August 2004.
N = Number of articles mentioning the search words
Source: Compiled from Lexis-Nexis archives using the search words 'cyberterrorism,' and 'cyber terrorism.'

> Though nobody really knew how sophisticated Al Qaeda's computer literacy was, more and more people were afraid of them. This created a kind of vicious circle, with the media dramatising the intelligence estimates and politicians in turn picking up media quotes. It was only a question of time before the plain fear would turn into bold forecasting (Bendrath 2003, 63).

In November 2001, an article appeared in *Information Security* magazine that made the jump from “might” or “could” to “will certainly”:

> Though we have yet to see terrorist groups--such as Hizbollah, HAMAS, Abu Nidal and Al Qaeda--employ hacking or malware to target critical infrastructures, their reliance Ion information technology and acquisitions of computer expertise are clear warning signs. While damage caused by hacktivists--and even cyberterrorists--has been minimal thus far, security experts predict that the nation’s IT infrastructure *will certainly* be a target in the future [my italics] (McAlearney 2001).

While in May 2002 an article in *Newsweek* was headlined ‘Islamic Cyberterror: Not a Matter of If, But of When’ (Hosenball 2002).

In late June 2002, Roger Cressey, who was at that time Chief of Staff of the President’s Critical Infrastructure protection Board, made a (remarkably) similar claim: “Al Qaeda spent more time mapping our vulnerabilities in cyberspace than we previously thought. An attack is a question of when, not if” (Borger 2002; Gellman 2002a & 2002b). This statement resulted in a deluge of press reports musing upon Al Qaeda’s alleged cyber attack plans:

- ‘Report: US Fears Possible Al Qaeda Cyber Attacks. *Reuters*, 27 June
- ‘Cyber-Attacks by Al Qaeda Feared.’ Barton Gellman in the *Washington Post*, 27 June

- ‘US “Fears al-Qaeda Hack Attack.”’ Kevin Anderson in *BBC News Online*, 27 June
- ‘Qaeda Cyberterror Called Real Peril.’ Barton Gellman in the *International Herald Tribune*, 28 June
- ‘US Fears al-Qaida Will Hit Vital Computer Networks.’ Julian Borger in *The Guardian* (UK), 28 June
- ‘Al Qaeda Cyber Alarm Sounded.’ William Mathews in *Federal Computer Week*, 25 July[26]

William Matthews article in *Federal Computer Week* included a prediction by Congressman Lamar Smith (R-Texas) that “There is a 50 percent chance that the next time al Qaeda terrorists strike in the United States, their attack will include a cyberattack.” Finally, on 11 September 2002, a German news agency even went so far as to quote “military sources in Berlin” who allegedly stated that Al Qaeda “might very well be capable of even preventing a possible US attack on Iraq.”

> A Bundeswehr intelligence expert asked: ‘What if the Islamists manage to enter the command and control networks of the US Army and mess up everything?’ Fighter jets and war ships would receive false instructions and commands, troops would be sent in the wrong direction, bombs would not hit the Iraqi positions they were meant for. This conceivable scenario would lead to a ‘military disaster’ (DPP News Agency 2002).

[26] In *The Register*, Thomas C. Green contributed, the tongue-in-cheek, ‘Soon Al-Qaeda Will Kill You on the Internet’ (2002).

The switch in the cyberterrorist threat image, from ‘terrorist hackers’ to ‘hacker terrorists,’ highlights two things: first, guarding against, as well as combating, security threats is clearly made easier if one is able to identify the actors responsible. It is suggested that the process of introducing a threat image onto the political agenda is facilitated by the ability to identify the actor or actors constituting the threat (Livingston 1994, 4). Structurally based threats have greater difficulty attracting attention than those portrayed as actor-based (Eriksson & Noreen 2002, 5-6). So while the identification of the cyberterrorist threat with the amorphous category such as that represented by ‘hackers’ is preferable to the latter, the ability to identify Osama bin Laden and/or Al Qaeda as the source of the cyberterrorist threat is clearly preferable to both of these. Second, certain dramatic events may also have an impact on the resonance of a threat image. The events of 9/11 acted as a trigger factor, revitalising the cyberterrorist threat discourse and the idea of the ‘hacker terrorist’ in particular.

EMERGENCY MEASURES

Wæver’s securitization thesis requires one to study the media more from the perspective of their effects than from their inherent meanings. The purpose of this section is, therefore, to study the effects of the various scenarios, analogies, and general threat images described in this paper, which because they are presented as ‘real,’ and the dangers they display are supposedly immediate, are aimed at convincing the American public that cyberterrorism is imminent and will be extremely destructive, and thus emergency measures are called for. In other words, this ‘worst case’ portrayal of a threat generally results in a proportionate response, in which the imagined threat is used to introduce ‘real’ powers backed up by ‘real’ legislation intended to convey certain imagined scenarios in the mind of, in this case, both hackers and terrorists.

The Pre-9/11 Environment

After the Oklahoma City bombing in 1995, then US President Clinton established the Critical Infrastructure Working Group to address both physical and cyber threats, which eventually gave rise to the Presidential Commission on Critical Infrastructure Protection (PCCIP). The PCCIP’s report *Critical Foundations: Protecting America’s Infrastructures* (1997) was the first comprehensive description and analysis of the cyber threat to the US national infrastructure. The report highlighted a number of the possible targets for cyberterrorism, including Supervisory Control and Data Acquisition (SCADA) systems, which govern the distribution of telecommunications, electric power, and other infrastructure-based services, which subsequently led to the issuing of Presidential Decision Directive 63 (commonly referred to as ‘PDD 63’). “PDD 63 prompted federal agencies to develop critical infrastructure protection plans and encouraged a strategy to protect the nation from cyberattacks” (Raghavan 2003, 302). Various government agencies also began churning out reports addressing the cyberterrorist threat (see Table 2.3). More serious measures were not put in place until after 9/11.

The risk of a massive *conventional* terrorist attack on the United States was emphasised by a number of academics and others before the events of 9/11, but was dismissed by the media (see Nacos 2002, 1-2), which chose to focus on cyberterrorism instead. Central decision-makers were therefore much more attuned to the latter threat than the former. Marcus Sachs, who served in the White House Office of Cyberspace Security and was a staff member of the President's Critical Infrastructure Protection Board, had this to say in 2003:

> We were very shocked in the federal government that the attack didn't come from cyberspace….Based on what we knew at the time, the most likely scenario was an attack from cyberspace, not airliners slamming into buildings….We had spent a lot of time preparing for a cyber attack, not a physical attack (Poulsen 2003).[27]

The Post-9/11 Environment

Previous to 9/11, if one successfully infiltrated a federal computer network, one was considered a hacker. However, following the passage of the PATRIOT Act,[28] 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 2001b; see also Middleton 2002; Levin 2002, 984-985). The law gives government investigators broad powers to track wireless phone calls, listen to voicemail, intercept e-mail messages, and monitor computer use. It also criminalizes

[27] Sachs collaborated on a fiction book entitled *Zero-Day Exploit* (2004) detailing yet another cyberterror scenario. This time a 0-day vulnerability in a particular line of SCADA Master products that are widely used in petrochemical facilities is exploited by attackers resulting in gas stations running out of gas, followed shortly by freight carriers, private individuals, and local police and fire departments. Disaster can only be prevented by Reuben, an elite cyber-security researcher who stumbles across the plot while contracting for the federal government (from Amazon.com product description).

[28] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was signed into law by US President George Bush in October 2001.

Table 2.3

US Government Documents: Cyberterrorism and Critical Infrastructure Protection*

Prepared By	*Year*	*Title*
White House	1998	*Presidential Directive 63: Critical Infrastructure*
General Accounting Office	1999	*Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations*
General Accounting Office	1999	*Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences*
White House	2000	*Defending America's Cyberspace: National Plan for Information Systems Protection*
Department of Justice	2000	*Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet*
General Accounting Office	2000	*Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*
General Accounting Office	2001	*Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities*
National Infrastructure Protection Centre	2001	*Cyber Protests: The Threat to the US Information Infrastructure*
General Accounting Office	2002	*Critical Infrastructure Protection: Significant Homeland Security Challenges Need to be Addressed*
General Accounting Office	2002	*Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*
Congressional Research Service	2003	*Critical Infrastructures: What Makes an Infrastructure Critical?*
General Accounting Office	2003	*Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*
General Accounting Office	2003	*Potential Terrorist Attacks: Additional Actions Needed to Prepare Critical Financial Markets*
White House	2003	*The National Strategy to Secure Cyberspace*
White House	2003	*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*
General Accounting Office	2003	*Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*
General Accounting Office	2003	*Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*
Congressional Research Service	2003	*Terrorism and Security Issues Facing the Water Infrastructure Sector*
White House	2003	*Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.*
General Accounting Office	2004	*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.*
General Accounting Office	2004	*Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*
General Accounting Office	2004	*Technology Assessment: Cybersecurity for Critical Infrastructure Protection*

* All documents are available in full on the Internet.
Source: Compiled from list available at Web site of National Memorial Institute for the Prevention of Terrorism (MIPT) http://www.mipt.org and Internet searching.

break-ins into any computer outside of the United States “that is used in a manner that affects inter-state or foreign commerce or communication of the United States” (USA PATRIOT Act, Section 814). Ralf Bendrath identifies this as the cyber equivalent of the US government’s ‘War on Terrorism,’ as it systematically expands the US’s cyber reach beyond its territory (2003, 61).

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 that would result in the largest reshuffle of US bureaucracy since 1948. At the signing ceremony, Bush said that the “department will gather and focus all our efforts to face the challenge of cyberterrorism” (as quoted in McCullagh 2002).

The Department of Homeland Security merges five agencies that shared 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 (Krebs 2002; McCullagh 2002; Poulsen 2002).

European Union governments also moved to counter computer-assisted terrorism in the wake of 9/11. The Council of Europe rushed through its Convention on Cybercrime in response to the attack, and the UK parliament passed the Anti-Terrorism, Crime and Security Act 2001 (ACSA), broadening the definition of terrorist organisations to include cyberterrorists for the first time, defining these as persons who disrupt or interfere with electronic systems.

CONCLUSION

Policymakers define security on the basis of a set of assumptions regarding vital interests, possible scenarios, and plausible enemies, which grow out of the specific historical and social context of a particular country and some conception of what is "out there" (Lipschutz 1995, 10). As we have seen, the media plays a key role in shaping these assumptions, constructing these scenarios, and generally informing us as to what is "out there." It is thus a prime mover in the process of defining security. The end of the Cold War provided an unprecedented window of opportunity for the movement of a wide range of non-military issues into the realm of security policy.

With the aid of the mass media, cyberterrorism came to be viewed as the ‘new’ security threat *par excellence*.

We cannot predict who will voice security concerns; only with hindsight can we see how much legitimacy an actor *did* possess. Every day some actor seeks to speak security, but the attempt becomes consequential only when society more or less actively backs up the speaker(s). People’s sense of what issues are of political relevance is always an ongoing process, which requires an emphasis on how threat images are discursively constructed, maintained, and altered. Particular emphasis needs to be placed upon the processes whereby national security issues communicatively emerge, and the central role of the media in such emergences, because the political communication/threat image environment shapes both the information available and the ways ordinary people use it in thinking about politics and national security.

Clearly, the American media has been highly successful in ‘speaking’ cyberterrorism into existence. Their reliance on “(hyper-)reality-producing dramas” (Debrix 2001, 153), Pearl Harbour analogies, comparisons of the effects of cyberterrorism with those of WMD, portrayal of hackers as a menace to national security, and general widening of the concept of cyberterrorism, in conjunction with the policy window opened by the events of 9/11 and, consequently, the ability to pinpoint Osama bin Laden and Al Qaeda as certain future cyberterrorists has resulted in the enactment of a raft of emergency measures as detailed in the USA PATRIOT Act and the Homeland Security Act.

It may be that these emergency measures are uncalled for, however. François Debrix suggests that all of the various apocalyptic scenarios, televised simulations, and musings as to the greater lethality of cyber than nuclear attack have ensured that the next Pearl Harbour will never materialise. Why? Because the fear of cyberterrorism has been spread so widely and with such success that should a ‘real’ attack ever occur it couldn’t match these.

> Being conditioned to such a degree of generalised panic, any real cyberterrorist attack that does not follow the simulated scenario and produce the anticipated amount of casualties will fall short of being worthy of people’s attention and worry (Debrix 2001, 156).

The question that then arises is whether the--for the most part--American-constructed cyberterrorist threat image has resonance beyond the borders of the United States?

“Traditionally, the US has been the dominant actor in IT issues. The US is and has been a ‘sender’ of ideas to other states about how to comprehend IT problems and their solutions” (Holmgren & Softa 2003, 15). That is one of the reasons why this paper is focused upon the US case. Nonetheless, threat images are constructed and responded to differently in different countries and regions. This raises a number of questions. Are we, for example, moving toward a converged perception of the cyberterrorist threat in the United States and Europe, or are the images in these different territories more divergent than similar? It is not only national political agendas that ought to be of interest. The description and analysis of how the cyberterrorist threat is being discussed and created within the European security community, particularly within the framework of an EU common foreign and security policy and within NATO, is also an avenue for future research.

What this paper has sought to show is how the cyberterror threat has been amplified in the US media. It is generally difficult to unravel how news frames shape the social construction of reality from the ‘actual’ reality of events. This is especially true in cases where the ‘events’ do not yet have a reality, as is the case with cyberterrorism, and presents particular difficulties if a “consensual interpretation” (Kern, Just, Norris 2003, 281) predominates so that a one-sided frame becomes uncritically taken for granted by politicians, journalists, and the public. ‘Terrorism’ is generally conceived as physical acts of violence intended to produce fear, and conjures up images of exploding bombs and mutilated bodies. The cyberterror threat image builds upon this aspect of terrorism by seeking to convince the public that cyberterrorism will ultimately result in mass casualties. There is another dimension to terrorism, however: the information dimension. And terrorists exploit it every bit as much as the physical. Death and destruction is not terrorists’ ultimate goal; it is power and influence. Terrorists seek political and social change, and their objective is to influence populations in ways that support that change. To accomplish this, they engage not just in physical, but also information operations, and the integration of these.

Up until very recently, cyberterrorism was presented as the sole intersection of terrorism and the Internet, even in the face of contrary independent evidence. The one-sided nature of the analysis only became apparent to many with the release, in February 2002, of a video depicting the murder of *Wall Street Journal* reporter Daniel Pearl via an Islamist Web site and the subsequent release, in Summer 2004, of the videotaped beheadings of a number of Western hostages held in Iraq in a similar fashion. The free availability of these grisly ‘snuff movies’ on the Internet led to a sudden upsurge in journalistic interest in those more mundane terrorist uses of the Net. It is submitted, finally, that the use of the Internet by terrorists to facilitate their activities, whether publicity and propaganda, recruitment, financing, data mining, or other functions, ought to be the subject of a great deal more social scientific research than has yet been undertaken.

REFERENCES

Adams, Jonathan & Fred Guterl. 2003. ‘Bringing Down the Internet.’ *Newsweek* 3 November. http://msnbc.msn.com/id/3339638/

Arquilla, John. 1998. ‘The Great Cyberwar of 2002.’ *Wired* 6(2). http://www.wired.com/wired/archive/6.02/cyberwar.html

Arquilla, John & David Ronfeldt. 1996. *The Advent of Netwar*. California; Rand. http://www.rand.org/publications/MR/MR789/

Arquilla, John & David Ronfeldt. 1993. ‘Cyberwar is Coming.’ *Comparative Strategy* Vol. 12.

Associated Press. 2001. ‘CIA Can’t Compare with Hackers.’ 21 June. http://www.cbsnews.com/stories/2001/06/21/tech/main297811.shtml

Baudrillard, Jean. 1983. *Simulations*. New York: Semiotexte.

Bendrath, Ralf. 2003. ‘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.

Bennett, W. Lance & Robert M. Entman (Ed.s). 2001. *Mediated Politics: Communication in the Future of Democracy*. Cambridge: Cambridge University Press.

Borger, Julian. 2002. ‘US Fears al-Qaida Will Hit Vital Computer Networks.’ *The Guardian* (UK) 28 June.

Buzan, Barry, Ole Wæver, & Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder & London: Lynne Rienner.

Buzan, Barry. 1995. ‘Security, the State, the ‘New World Order,’ and Beyond.’ In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.

Buzan, Barry. 1991. *People States and Fear: An Agenda for International Security Studies on the Post-Cold War Era* (Second Ed.). New York: Harvester Wheatsheaf.

Centre for Strategic and International Studies (CSIS). 1998. *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. Washington DC: CSIS Press.

Cohen, Fred. 2003. ‘Cyber-Risks and Critical Infrastructures.’ *Strategic Security* 2003-02-27.

Cohn, Carol. 1987. ‘Sex and Death in the Rational World of Defense Intellectuals.’ *Signs: Journal of Women in Culture and Society* 12(4).

Cook, Timothy E. 2001. ‘The Future of the Institutional Media.’ In W. Lance Bennett and Robert M. Entman (Ed.s), *Mediated Politics*. New York: Cambridge University Press.

Debrix, François. 2001. ‘Cyberterror and Media-Induced Fears: The Production of Emergency Culture.’ *Strategies* 14(1).

Deibert, Ronald J. 2002. ‘Circuits of Power: Security in the Internet Environment.’ In James N. Rosenau & J.P. Singh (Ed.s), *Information Technology and Global Politics*. Albany: SUNY Press.

Denning, Dorothy. 2001. ‘Is Cyber Terror Next?’ In Craig Calhoun, Paul Price, and Ashley Timmer (Eds.), *Understanding September 11*. New York: New Press. http://www.ssrc.org/sept11/essays/denning.htm

Denning, Dorothy. 1999. *Information Warfare and Security*. Reading, MA: Addison-Wesley.

Der Derian, James. 1995. ‘The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard.’ In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.

DPP News Agency. 2002. ‘’German Intelligence Says Al Qaeda’s Preparing to Attack Western Computer Systems.’ 11 September. http://www.zone-h.org/en/news/read/id=834/

Devost, Matthew G., Brian K. Houghton, & Neal Allen Pollard. 1997. ‘Information Terrorism: Political Violence in the Information Age.’ *Terrorism and Political Violence* 9(1): 72-83.

Devost, Matthew, Houghton, & Neal Alan Pollard. 1996. ‘Information Terrorism: Can You Trust Your Toaster?’ In Robert E. Neilson (Ed.), *Sun Tzu’s Art of War in Information Warfare*. Institute for National Strategic Studies: National Defence University, Washington DC. http://www.ndu.edu/inss/siws/ch3.html

Dunn, Myriam A. 2004. ‘Cyber-Terror: Looming Threat or Phantom Menace?’ Paper presented at the Fifth International CISS Millennium Conference, Salzburg, Austria, July 7-8.

Embar-Seddon, Ayn. 2002. ‘Cyberterrorism: Are We Under Siege?’ *American Behavioral Scientist* 45(6).

Entman, Robert M. 2000. 'Declarations of Independence: The Growth of Media Power After the Cold War.' In Brigitte L. Nacos, Robert Y. Shapiro, & Pierangelo Isernia (Ed.s), *Decisionmaking in a Glass House*. New York: Rowman & Littlefield.

Entman, Robert M. 1993. 'Framing: Toward Clarification of a Fractured Paradigm.' *Journal of Communication* 43(4).

Eriksson, Johan & Giampiero Giacomello. 2004. 'International Relations Theory and Security in the Digital Age.' Paper presented at the International Studies Association (ISA) annual conference Montreal, Canada, 17-20 March. http://www.threat-politics.net/docs/eriksson_isa.pdf

Eriksson, Johan & Erik Noreen. 2002. 'Setting the Agenda of Threats: An Explanatory Model.' *Uppsala Peace Research Papers* No. 6. http://www.pcr.uu.se/publications/UPRP_pdf/uprp_no_6.pdf

Eriksson, Johan. 2001. 'Cyberplagues, IT, and Security: Threat Politics in the Information Age.' *Journal of Contingencies and Crisis Management* 9(4).

Gellman, Barton. 2002b. 'Qaeda Cyberterror Called Real Peril.' *International Herald Tribune*, 28 June.

Gellman, Barton. 2002a. 'Cyber-Attacks by Al Qaeda Feared.' *Washington Post*, 27 June. http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26

Giacomello, Giampiero. 2003. 'Measuring "Digital Wars": Learning from the Experience of Peace Research and Arms Control.' *Infocon Magazine* No. 1. http://www.iwar.org.uk/infocon/measuring-io.htm

Graham, Stephen. 2004. 'War in the "Weirdly Pervious World": Infrastructure, Demodernisation, and Geopolitics.' Paper presented at the conference on Urban Vulnerability and Network Failure, University of Salford, UK, 29-30 April. http://www.surf.salford.ac.uk/documents/UrbanVulnerability/Graham.pdf

Greene, Thomas C. 2004. 'Cyber-Terror Drama Skates on Thin *Black Ice*.' *The Register* 25 February. http://www.theregister.co.uk/2004/02/25/cyberterror_drama_skates_on_thin/

Greene, Thomas C. 2002. 'Soon Al-Qaeda Will Kill You on the Internet.' *The Register* 28 June. http://www.theregister.co.uk/2002/06/28/soon_alqaeda_will_kill_you/

Gronke, Paul & Timothy Cook. 2002. 'Disdaining the Media in the Post 9/11 World.' Paper presented at the annual meeting of the American Political Science Association (APSA), Boston MA, August. http://web.reed.edu/academic/studentgrants/corbandgold/apsa2002.pdf

Holmgren, Jonas & Jan Softa. 2003. 'The Functional Security Agenda in the Nordic States.' *Threat Politics Project*. Sweden: University of Uppsala. http://www.threat-politics.net/docs/softa-functional.pdf

Homer-Dixon, Thomas. 2002. ‘The Rise of Complex Terrorism.’ *Foreign Policy* January/February. http://www.foreignpolicy.com/story/cms.php?story_id=170

Hosenball, Mark. 2002. ‘Islamic Cyberterror: Not a Matter of If, But of When.’ *Newsweek* 20 May. http://archive.infopeace.de/msg01346.html

Institute for Security Technology Studies (ISTS). 2001. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Dartmouth College: Institute for Security Technology Studies. http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm.

Ingles-le Noble, John. 1999. ‘Cyberterrorism Hype.’ *Jane’s Intelligence Review*. http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm

Joint Economic Committee. 2001. *Wired World: Cyber Security and the US Economy*. Washington DC: US Government Printing Office. http://www.house.gov/jec/hearings/6-21-01.pdf

Kern, Montague, Marion Just, & Pippa Norris. 2003. ‘The Lessons of Framing Terrorism.’ In Pippa Norris, Montague Kern, & Marion Just (Ed.s), *Framing Terrorism: The News Media, the Government, and the Public*. New York & London: Routledge.

King, Brad. 2002. ‘Fear and Lockdown in America.’ *Wired* 25 July. http://www.wired.com/news/digiwood/0,1412,54099,00.html

Knudsen, Olav F. 2001. ‘Post-Copenhagen Security Studies: Desecuritizing Securitization.’ *Security Dialogue* 32(3): 355-368.

Krebs, Brian. 2002. ‘Homeland Security Bill Heralds IT Changes.’ *The Washington Post* 25 November. http://foi.missouri.edu/homelandsecurity/homelandsecuritybill.html

Laqueur, Walter. 1999. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press.

Levin, Brian. 2002. ‘Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer Networks in America.’ *American Behavioral Scientist* 45(6).

Lipschutz, Ronnie D. 1995. *On Security*. New York: Columbia University Press.

Livingston, Steven. 1994. *The Terrorism Spectacle*. Boulder: Westview Press.

Marsh, Pearl-Alice. 1995. ‘Grassroots Statecraft and Citizens’ Challenges to US National Security Policy.’ In Ronnie Lipschutz (Ed.), *On Security*. New York: Columbia University Press.

Matthews, William. 2002. ‘Al Qaeda Cyber Alarm Sounded.’ *Federal Computer Week* 25 July. http://www.fcw.com/fcw/articles/2002/0722/web-attack-07-25-02.asp

Mayk, Lauren. 2004. 'Restoring Power Likely to Take Weeks, Not Days.*' Southwest Florida Herald Tribune* 16 August. http://www.newscoast.com/apps/pbcs.dll/frontpage

McAlearney, Shawna. 2001. 'Cyberspace Braces for Escalation and War.' *Information Security* 3(89). http://infosecuritymag.techtarget.com/2001/nov/digest19.shtml

McCullagh, Declan. 2002. 'Bush Signs Homeland Security Bill.' *CNET News* 25 November. http://news.com.com/2102-1023-975305.html

McGray, Douglas. 2003. 'The Minister of Net Defense.' *Wired* 11(05). http://www.wired.com/wired/archive/11.05/schmidt.html
Middleton, James. 2002. 'US Hackers Could Face Life Sentences.' *Vnunet.com* 28 February. http://vnunet.com/News/1129590.

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

National Infrastructure Protection Center (NIPC). 2001a. *NIPC Daily Report* 3 December. http://lists.jammed.com/crime/2001/12/0005.html

Pew Internet & American Life Project. 2003. *Survey with Federal Computer Week Magazine About Emergencies and the Internet*. http://www.pewinternet.org/pdfs/PIP_Preparedness_Net_Memo.pdf

Pollard Neal A. 2004. 'Indications and Warning of Infrastructure Attack.' In Lars Nicander & Magnus Ranstorp (Ed.s), *Terrorism in the Information Age: New Frontiers?* Stockholm: National Defence College.

Pollitt, Mark M. 1998. 'Cyberterrorism: Fact or Fancy?' *Computer Fraud and Security* February.

Porteus, Liza. 2001. 'Feds Still Need to Define Role in Tackling Cyberterror, Panelists Say.' *GovExec.com* 15 May. http://www.govexec.com/dailyfed/0501/051501td.htm

Poulsen, Kevin. 2003. 'Official: Cyberterror Fears Missed Real Threat.' *SecurityFocus.com* 31 July. http://www.securityfocus.com/news/6589

Poulsen, Kevin. 2002. 'Lawyers Fear Misuse of Cyber Murder Law.' *SecurityFocus Online*, 21 November. http://www.theregister.co.uk/2002/11/25/lawyers_fear_misuse_of_cyber/

Poulsen, Kevin. 2001. 'Cyber Terror in the Air.' *SecurityFocus.com* 30 June. http://www.securityfocus.com/columnists/6

Poulsen, Kevin. 1999. 'Info War or Electronic Sabre Rattling?' *ZDNet* 8 September. http://zdnet.com.com/2100-11-515631.html?legacy=zdnn

Presidential Commission on Critical Infrastructure Protection (PCCIP). 1997. *Critical Foundations: Protecting America's Infrastructures*. Washington DC: Critical Infrastructure Assurance Office (CIAO). http://www.ciao.gov/resource/pccip/report_index.htm

Raghavan, Tara Mythri. 2003. 'In Fear of Cyberterrorism: An Analysis of the Congressional Response.' *University of Illinois Journal of Law, Technology, and Policy* 3(1). http://www.jltp.uiuc.edu/recdev/Spring%202003/raghavan.pdf

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

Ross, Andrew. 2000. 'Hacking Away at the Counter-Culture.' In David Bell & Barbara M. Kennedy (Eds.), *The Cybercultures Reader*. London & New York: Routledge.

Ryan, Patrick S. 2004. 'War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics.' *Virginia Journal of Law & Technology* 9(7). http://ssrn.com/abstract=585867

Schwartau, Winn. 1994. *Information Warfare: Cyberterrorism- Protecting Your Personal Security in the Electronic Age* (2nd Ed.). New York: Thunder's Mouth Press.

Skibell, Reid. 2002. 'The Myth of the Computer Hacker.' *Information, Communication & Society* 5(3).

Specter, Michael. 2001. 'The Doomsday Click: How Easily Could a Hacker Bring the World to a Standstill?' *The New Yorker* 28 May.

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

Stone, Andrea. 2001. 'Cyberspace: The Next Battlefield.' *USA Today* 16 June. http://www.usatoday.com/tech/news/2001-06-19-cyberwar-full.htm

Taylor, Paul A. 1999. *Hackers: Crime in the Digital Sublime*. London & New York: Routledge.

Verton, Dan. 2003. *Black Ice: The Invisible Threat of Cyberterrorism*. New York: McGraw Hill.

Wæver, Ole. 1995. 'Securitization and Descuritization.' In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.

Wald, Matthew L. 2004. 'Toppled Power Lines are Posing a Herculean Task in Florida.' *New York Times* 19 August.

Wallace, Chris. 2002. 'Internet as Weapon: Experts Fear Terrorists May Attack Through Cyberspace.' *ABC News.com* 16 September. http://abcnews.go.com/sections/wnt/DailyNews/cyberterror020913.html

West, Darrell M. 2001. *The Rise and Fall of the Media Establishment*. New York: Bedford/St. Martins.

Yould, Rachel. 2003. ‘Beyond the American Fortress: Understanding Homeland Security in the Information Age.’ In Robert Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York: New Press.