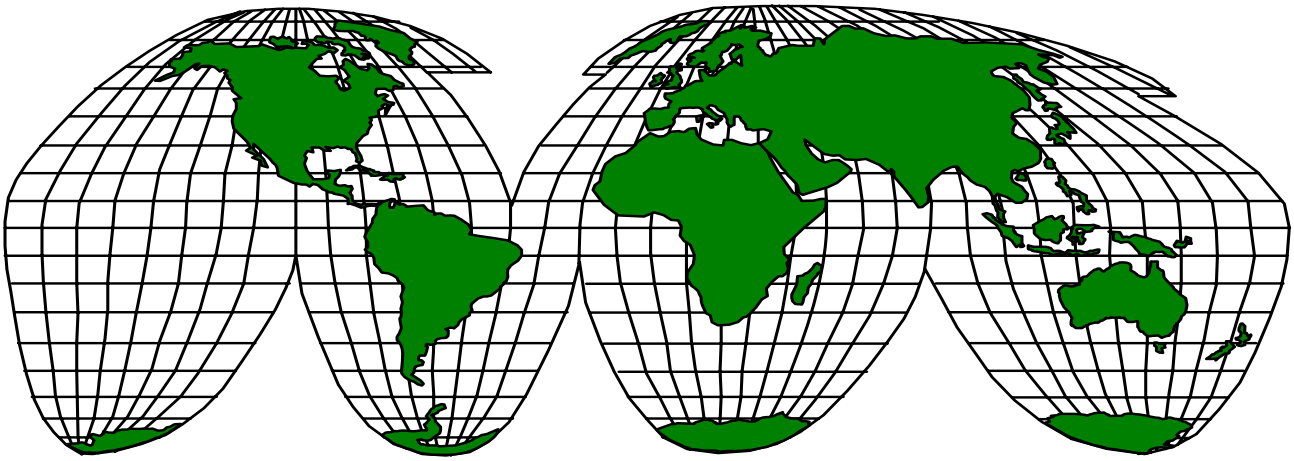

Working Papers in International Studies
Centre for International Studies
Dublin City University

Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures

Maura Conway

School of Law and Government
Dublin City University

Working paper 5 of 2008

Centre for International Studies
School of Law and Government
Dublin City University
Ireland

Tel. +353 1 7007720
Fax + 353 1 7007374
Email cis@dcu.ie
Web: www.dcu.ie/~cis

Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures

Maura Conway

> [Cyberterrorism] isn't so much a threat to national security as a threat to civilisation
>
> (Paul Vixie, quoted in Adams and Guterl 2003)[1]

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

A central element of the post-11 September 2001 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 deadly attacks by terrorists on (and with the help of) the computerized infrastructures that now constitute the critical underpinnings of everyday urban life in the US. This depiction of computerized systems as a super-critical infrastructure and thus the Achilles heel of advanced industrial societies, has been further fuelled by the use of everyday urban infrastructures as both weapons and targets of mass murder in the physical attacks of 2001 (Graham 2004).

Following the collapse of the USSR, a number of developments highlighted the growing influence of information technology in the realms of both national and international security. Examples include the high level of IT capability displayed by US troops in the first Gulf War (1990–91) and the increasingly global nature of media coverage, as demonstrated in the Somali (1993) and Balkan conflicts (1992–99). More recently, increased systems failures resulting from the activities of hackers, as evidenced by the cyber-attack(s) targeting Estonia in May 2007 and the growing use of the internet for 'infowar' purposes by al-Qaida and a plethora of other sub-state political violence groups, have garnered substantial attention. The growing dependence of states, particularly of the US, on information technology was highlighted by these and other events, prompting fears of a radically new security threat: the possibility of information systems serving as both weapons and targets of attack.

This cyber-threat became the object of increased attention from the US federal government in the 1990s, in close connection with the more general critical infrastructure protection debate (see Dunn, this volume). A particular concern was that enemies of the US, unable to defeat US forces on the conventional battlefield, would pursue alternative approaches to inflicting damage on the sole remaining superpower (Pollard 2004: 43). The events of 11 September 2001 were therefore doubly shocking for many US government officials: Not only were the attacks appalling in themselves, but the conventional (though asymmetric) nature of the attacks was also completely unexpected. Far from reducing the fear of cyber-attack however, for many, the 2001 attacks only served to increase the credibility of the cyber-threat.

According to a study released in June 2001, 75 per cent of internet users worldwide believe in the existence of cyberterrorism. The survey conducted in 19 major cities around the world found that 45 per cent of respondents agreed completely that 'computer terrorism will be a growing problem,' while 35 per cent of respondents agreed somewhat with the same statement (Poulsen 2001). In a July 2002 survey conducted by the American Business Software Alliance, 82 per cent of information technology professionals were said to believe that US businesses were ill equipped to deal with cyberterrorism (King 2002), while a survey carried out by *Federal Computer Week* and the Pew Internet and American Life Project in 2003 found that about half of US citizens fear terrorists will launch cyber-attacks 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 fear of cyberterror is in the zeitgeist. This chapter seeks to show how this threat image took root there and eventually came to be viewed as the ultimate threat to critical infrastructures.

The chapter's core argument is that US media outlets have been significant contributors not just to the dissemination, but to the actual discursive construction of the contemporary cyberterrorist threat and, further, that it is their emphasis on the (imagined) fatal connectivity between virtual networks and physical infrastructures that makes the concept of cyberterror so powerful. The chapter is divided into four sections. The first section explores the chapter's theoretical underpinnings, particularly the important role of the mass media in framing the threat and thus in agenda-setting. Section two focuses on how fears associated with terrorism and technology are linked in so-called 'shut-down-the-power-grid scenarios' to hype the

threat to critical infrastructures from cyberterrorists. In section three, two popular analogies associated with the cyberterror threat discourse are investigated: the possibility of an 'electronic Pearl Harbor' and the equation of cyber-attack tools, so-called 'weapons of mass disruption', with the threat from 'weapons of mass destruction' (WMD). The identification of specific antagonistic actors is crucial to successful threat construction; the shift in media focus from terrorist hackers to hacker terrorists is therefore at the centre of section four. Finally, the conclusion looks at the consequences the cyber-terror threat image has for the critical infrastructure debate, particularly the effects of cyberterror's 'hyperreal' character as displayed in the media and the interplay between threat construction, apocalyptic expectations, and actual occurrences.

THEORETICAL UNDERPINNINGS: THREAT POLITICS

Traditional security studies views threat images as relatively unproblematic and assumes that real-world threats 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 is no natural or self-evident correlation between the substance of a threat image and whether it has an impact on the political agenda (see Buzan 1991, Buzan et al. 1998). They argue instead that the formation of agendas depends on power and politics, particularly on the ability of an actor or actors to 'speak' a threat into existence. Threat is first constructed in the individual consciousness; individuals view something as a threat. The next step is for an actor or 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. Very often, this happens through the dissemination of newspaper stories,

magazine articles, television documentaries, and eventually mass-market books and movies.

In the context of mass media, this process of formulating problems, finding scapegoats, and coming up with solutions has been labelled 'framing.' 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 usually followed by verbalization: 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 and 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 policy fields, while national security policy is invariably viewed as the foundation of all security policy (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 into the political agenda.

Agenda-Setting

The agenda-setting model of the media posits that the mass media have an influence on what the public recognizes as important issues, and the theory has been supported by a wealth of empirical studies. There are two main approaches in this area: One focuses on elites, and the other is pluralist-based. The elite approach focuses on formal political power and highly-placed decision-makers, the second approach broadens the concept of the 'political agenda' to include such factors as the agenda(s) of the media. The contention here is that the US news media act as the main source of political information for mass publics – both within the US, 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 '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: 85f.). 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 organizations, it is not unreasonable to suggest that the news media is *the* dominant intermediary organization in American democracy' (2002: 1). As a purveyor of threat frames, therefore, the mass media is unparalleled.

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 and Noreen 2002: 8). The term 'cyberterrorism' unites two significant modern fears: fear of technology and fear of terrorism. Both of these fears are evidenced in this quote from Walter Laqueur, one of the most well known scholars of terrorism: '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, therefore, both technology and terrorism are perceived as more ominous than known threats (Embar-Seddon 2002: 1034).

Fear of terrorism, conceived of as random, incomprehensible, and uncontrollable violence, may strike one as relatively 'normal'; fear of technology 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. Many people are therefore fearful that technology will become the master and humankind 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 (1991: 8): the idea that all of the functions controlled by individual computers will

connect to form a singular system such that, eventually, our entire existence will be managed by an all-powerful, but uncontrollable, network (see also Sandwell 2006: 47). 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, one of the key critical infrastructures of society, appear particularly fearsome. The result is that many people now feel themselves to be '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.[3] Two of the best-known scenarios[4] are those designed by the prominent analyst of information warfare, John Arquilla of the Naval Postgraduate School in Monterey, California 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 and cascading power failures ensure that 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 drug cartel in Colombia and various Asian triads.

Arquilla's scenario is somewhat tongue-in-cheek, and eventually – the scenario runs to over 20 printed pages – he 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- or sub-state actors (Arquilla and 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 is eventually found to be behind the attacks seeks to conceal itself by taking on the name 'People For a Free World', which is reminiscent of the names of a number of terrorist organizations, including the Weatherman group 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 of 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 the US reliance on ICT is the country's 'Achilles 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 infowar specialists, including John Arquilla, sketch the impacts of a hypothetical series of escalating cyber-attacks: the collapse of air traffic control systems, resulting in multiple airplane crashes; overloaded digital networks, resulting in the collapse of finance and e-commerce networks; and 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 strong resemblances to Arquilla's contribution to *Wired* just a few months earlier, but there are also some striking differences. On the one hand, the described outcomes of the cyber-attack(s) are very 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. Nobody in the media seems quite sure whether states or terrorists pose the greater threat. Many journalists deliver a mixed message and warn that both types of actors are equally threatening.[5] 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 2001 an

article in *USA Today* entitled ‘Cyberspace: The Next Battlefield’ asserted that ‘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). After 11 September 2001, however, the spectre of cyberterror took on a new urgency.

In 2003, Dan Verton, a technology journalist,[6] wrote *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 virtual and physical attacks on critical infrastructures in the US Pacific Northwest (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 organizations, 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-Qaida members, aided by Russian hackers and a number of disgruntled energy company employees with right-wing sympathies. The effects of the attacks are described as lasting for weeks in some areas, months in others. Emergency services, medical facilities, businesses, banks, government offices, industrial plants, and manufacturing firms are all depicted as susceptible to failures and disruptions to such an extent that some are forced to close their doors for good (Verton 2003: 14f.). One sceptical reader describes Verton’s work 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).[7] However, such contentions are accepted and acceptable because in our media-saturated world, events can be at once 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: 15f.)

He thus transforms his imaginings from prediction to reality and evokes the ultimate threat to the key assets of modern societies. 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 being 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 the next spectacular terrorist act will occur both everywhere and nowhere at the same time through the use of the internet, which

is presently employed as an object of leisure or a necessary support for work, but which will very soon mutate into the world's deadliest weapon (2001: 156). Barry Sandwell concurs, adding that 'the most extreme manifestations of cyberfear are articulated around metaphors of boundary dissolving threats, intrusive alterities, and existential ambivalences created by the erosion of binary distinctions and hierarchies that are assumed to be constitutive principles of everyday life' (2006: 40). Some of the distinctions that continue to be eroded and which are invoked in the media to justify the continued hyping of the cyberterror threat include those separating the inside from the outside, the offline versus the online world, and the 'real' or physical from the virtual or imagined. This fits with Debrix's assertion that popular fears have taken on a new gravity and emergency responses have become everyday realities in media-saturated societies, but particularly in the US after 11 September 2001. Debrix goes on to suggest 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' (2001: 153). In an age where information becomes knowledge, it is increasingly difficult to distinguish cyberterrorism from its media representations.

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 critical infrastructure systems. It is worth keeping in mind that system failures – widespread water contamination, power failures, chronic flight disruptions, and other cyberterror scenarios – are events that occur routinely and without affecting national security. 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. With respect to electrical power, most outages occur due to natural phenomena such as severe weather, as attested, for example, by the impact of 2005's Hurricane Katrina on New Orleans. Nevertheless, the hitherto purely speculative threat to critical infrastructures from politically motivated and cyber-savvy foes continues to animate far more people than the proven, albeit non-purposeful and even quotidian, destructive capacity of operator error, acts of nature, and similar.

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 Harbor’. The comparison of so-called ‘weapons of mass disruption’ with ‘weapons of mass destruction’ is another popular play on words.

Electronic Pearl Harbor

Winn Schwartau of infowar.com first used the term ‘Electronic Pearl Harbor’ in testimony before the US Congress as early as 1991 (see Schwartau 1994: 43).[8] The Pearl Harbor analogy has since been used with startling frequency in the media as a shorthand description of the likely consequences of a cyberterrorist attack on the US. A Lexis-Nexis search of major world newspapers found 105 mentions of this and related terms[9] in the ten years between 1994 and 2004. The function of this analogy is to link 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 the US being invulnerable due to its geographical position. The analogy has immediate resonance and attracts wide understanding, which is perhaps unsurprising given that Pearl Harbor has become linked in popular consciousness with the events of 11 September 2001, to which it is often compared, which is again unsurprising considering that the story and visuals associated with the Japanese attack were doubtless fresh in the minds of many Americans in September 2001 given the release of the blockbuster movie *Pearl Harbor* in May of that year. However, while the Pearl Harbor analogy works very well, in terms of immediately conjuring up images of a sudden crippling blow against critical infrastructures resulting in chaos and destruction, it doesn’t actually explain anything about cyberterrorism,[10] but works instead to manufacture fear in the simplest and most direct way possible.

Weapons of Mass Disruption

In the wake of 11 September 2001, threats to the integrity of the US information infrastructure have been ascribed a level of urgency analogous to nuclear and biological threats, which has galvanized the relationship between IT and security as a primary policy consideration in the US (Yould 2003: 75). In September 2002, Richard Clarke, former special White House adviser for Cyberspace Security, told ABC News: '[Cyberterrorism is] 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 11 September 2001, the American 'cyber-angst' was palpable (Bendrath 2003).[11] As early as 1999, Congressman Curt Weldon (R-Pennsylvania) had 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, 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 that '[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), the author of *The New Yorker* article mentioned above, predicted: 'The Internet is waiting for its Chernobyl, and I don't think we will be waiting much longer.'

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-dramatize threats (see Cohn 1987). With regard to the cyberterrorist threat, exactly the opposite is happening. Far from de-realizing the threat, the discourse of cyberterrorism mobilized by the media and assorted 'experts' makes the threat seem real and palpable. Mediatized 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' – that is nuclear, biological, or chemical weapons – is, however, both inaccurate and unhelpful in terms of advancing an understanding of the relationship between national security and IT. This is true whether one believes such threats are imminent (see Yould 2003: 84–8) or is sceptical of the cyber-terrorist 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 of an entire vast territory, is less significant than its digital disconnection (see Cohen 2003: 9f.).

IDENTIFYING ANTAGONISTIC ACTORS

Exploring the mediation of threat construction also requires analysis of the identification of 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 emphasized that non-state actors may also 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: 26f.). 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. Before 11 September 2001, the media were fixated on hackers as antagonistic actors. Hackers, conceived of as computer abusers, had a history of being demonized in movies, on TV, and in the press. As '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. This development constitutes a 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 jeopardize 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 (Skibell 2002: 342; see also Ryan 2004: 8f.).

In his book *Hackers*, Paul Taylor describes a 1991 episode of the US chat show *Geraldo* (1999: 178f.). 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, show host Geraldo Rivera 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:

> Rivera: 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 1999: 178).[12]

At the very end of the show, Rivera 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 1999: 179).

Hackers get a lot of bad press. In terms of the hyping of the cyberterrorist threat, the portrayal of hackers as potential adversaries was not restricted to film and television; they were also 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 and 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 would not constitute cyberterrorism unless they engaged in the act for political purposes. Most journalists are either unaware of this

caveat or ignore it, with the result that the press have labelled some unlikely acts of computer abuse as ‘cyberterrorism.’

According to newspaper reports, sending pornographic e-mails to minors, posting offensive content on the internet, defacing web pages, using a computer to cause US$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 (see Conway 2003: 34f.). And yet, none of these actions could be described as terrorism – some of them are not even criminal – had they been accomplished without the aid of computers (see Ross 2000: 255). Admittedly, terrorism is notoriously difficult to define; however, the addition of computers to plain old crime certainly does not fall in this category. So what then are the functions of these sorts of reports? They result in a widening of the 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 kiddie variety – have begun to be influenced by their portrayal in the media. The anonymous defacement of two US government websites, 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 mujahideen nor terrorists, and were evidently more familiar with media portrayals of cyberterrorism than with any ‘real’ cyberterrorists.

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 discourse surrounding computer hackers belabours the potentially catastrophic economic and national security threats posed by malicious intruders, while for a long time identifying the subject of this threat as young, self-trained computer geeks. This raised the fundamental question of how obsessive, self-taught teenagers could overcome the security devised by governments and corporations that together have spent billions of dollars seeking to safeguard those same systems and cracking down on cyber-criminals (Skibell 2002: 336)? In fact, more recently, the media have reassessed the hacker-as-terrorist discourse, which had begun to appear increasingly unconvincing, and in the wake of 11 September 2001, this discourse was superseded by the terrorist-as-hacker approach.

Hacker Terrorists

The 11 September 2001 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: 59f.). 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 11 September 2001. The question on many people's lips was 'Is Cyber Terror Next?' (Denning 2001).

Once Osama bin Laden and al-Qaida had been fingered as the perpetrators of the 11 September 2001 attacks, a steady stream of newspaper articles began to appear suggesting that the latter were now engaged in planning a major cyberterrorist attack. So although there was no evidence available by which to measure al-Qaida's IT literacy, more and more people came to believe and fear that it was substantial. This resulted in the creation of a hyper-mediated vicious circle: the media dramatized the intelligence estimates, and the politicians in turn picked up media quotes, which they then relayed back in other media fora, and so on. Within a very short time, unsubstantiated fears had transformed into forecasts (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 on 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)

Furthermore, in May 2002, an article appeared in *Newsweek* that 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 and 2002b). This statement resulted in a deluge of press reports musing upon al-Qaida's alleged cyber-attack plans in 2002:

- '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[13]

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.'

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 and Noreen 2002: 5f.). So

while the identification of the cyberterrorist threat with an amorphous category such as that of 'hackers' is preferable to the latter, the ability to identify Osama bin Laden and/or al-Qaida 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 11 September 2001 acted as a trigger factor, revitalizing the cyberterrorist threat discourse and the idea of the 'hacker terrorist' in particular.

CONCLUSION

Finally, what were some of the effects of the cyberterror threat image as constructed in the US media and described in the foregoing? While so-called 'cyberpanics' may have imaginary origins, they can also have very real consequences (Sandwell 2006: 46).

The risk of a massive *conventional* terrorist attack on the US was emphasized by a small number of academics and others before the events of 11 September 2001, but was dismissed by the media (see Nacos 2002: 1f.), which chose to focus on cyberterrorism instead. Key decision-makers were therefore much more attuned to the latter threat than the former. Marcus Sachs,[14] 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 about the convergence of policymakers' fear of technology with their fear of terrorism:

> 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)

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. This points to why 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. The political communication/threat image environment shapes both the information available and the ways in which not just ordinary people, but also political elites, use it in thinking about politics and national security.

Demonstrating the effects of the media's influence on publics and decision-makers is always difficult due to the indirect and complex dynamics involved; clearly, however, the US media has been highly successful in 'speaking' cyberterrorism into existence. Their reliance on '(hyper-)reality-producing dramas' (Debrix 2001: 153), Pearl Harbor 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 11 September 2001 and, consequently, the ability to cast Osama bin Laden and al-Qaida as certain future cyberterrorists has resulted in the hyping of an (imagined) fatal connection between virtual networks and critical infrastructures that, to date, has very little real form or substance.

This conclusion may not be quite as disturbing as it might first appear, however, for François Debrix suggests that all of the various apocalyptic scenarios, televised simulations, and musings as to the greater lethality of virtual over nuclear attacks have, in fact, ensured that a virtual Pearl Harbor will never materialize. The reason is that the fear of cyberterrorism has been spread so widely and with such success that should a 'real' attack ever occur, it couldn't match expectations: '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).

REFERENCES

Adams, J. and Guterl, F. (2003) 'Bringing down the internet', *Newsweek*, 3 November 2003. Online. Available HTTP: <http://msnbc.msn.com/id/3339638/> (accessed 17 August 2007).

Arquilla, J. (1998) 'The great cyberwar of 2002', *Wired*, 6, 2. Online. Available HTTP: <http://www.wired.com/wired/archive/6.02/cyberwar.html> (accessed 17 August 2007).

Arquilla, J. and Ronfeldt, D. (1993) 'Cyberwar is coming', *Comparative Strategy*, 12: 141–65.

—— (1996) *The Advent of Netwar*, Santa Monica, CA: Rand. Online. Available HTTP: <http://www.rand.org/publications/MR/MR789/> (accessed 17 August 2007).

Baudrillard, J. (1983) *Simulations*, New York: Semiotexte.

Bendrath, R. (2003) 'The American Cyber-Angst and the real world: Any link?' in Latham, R. (ed.) *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York: The New Press, pp. 49–73.

Borger, J. (2002) 'US fears al-Qaida will hit vital computer networks', *The Guardian*, 28 June 2002.

Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*, Boulder and London: Lynne Rienner.

Buzan, B. (1991) *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd edn, New York: Harvester Wheatsheaf.

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

Cohen, F. (2003) 'Cyber-risks and critical infrastructures', *Strategic Security*, 2, 27: 1–10.

Cohn, C. (1987) 'Sex and death in the rational world of defense intellectuals', *Signs: Journal of Women in Culture and Society*, 12, 4: 687–718.

Collin, B.C. (1996) 'The future of cyberterrorism', paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago. Online. Available HTTP: <http://afgen.com/terrorism1.html> (accessed 17 August 2007).

Conway, M. (2003) 'What is cyberterrorism? The story so far', *Journal of Information Warfare*, 2, 2: 33–42.

Cook, T.E. (2001) 'The future of the institutional media', in Bennett, W.L. and Entman, R.M. (eds) *Mediated Politics*, New York: Cambridge University Press, pp. 182–200.

Debrix, F. (2001) ‘Cyberterror and media-induced fears: The production of emergency culture’, *Strategies*, 14, 1: 149–68.

Deibert, R.J. (2002) ‘Circuits of power: Security in the internet environment’, in Rosenau, J.N. and Singh, J.P. (eds) *Information Technology and Global Politics*, Albany: SUNY Press, pp. 115–42.

Denning, D. (1999) ‘Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy’, in Arquilla, J. and Ronfeldt, D. (eds) *Networks and Netwars*, Santa Monica, CA: Rand. Online. Available HTTP: <http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf> (accessed 17 August 2007).

—— (2001) ‘Is cyber terror next?’ in Calhoun, C., Price, P. and Timmer, A. (eds) *Understanding September 11*, New York: The New Press. Online. Available HTTP: <http://www.ssrc.org/sept11/essays/denning.htm> (accessed 17 August 2007).

Der Derian, J. (1995) ‘The value of security: Hobbes, Marx, Nietzsche, and Baudrillard’, in Lipschutz, R. (ed.) *On Security*, New York: Columbia University Press, pp. 24–45.

Devost, M.G., Houghton, B.K. and Pollard, N.A. (1997) ‘Information terrorism: Political violence in the information age’, *Terrorism and Political Violence*, 9, 1: 72–83.

Embar-Seddon, A. (2002) ‘Cyberterrorism: Are we under siege?’ *American Behavioral Scientist*, 45, 6: 1033–43.

Entman, R.M. (1993) ‘Framing: Toward clarification of a fractured paradigm’, *Journal of Communication*, 43, 4: 51–8.

—— (2000) ‘Declarations of independence: The growth of media power after the Cold War’, in Nacos, B.L., Shapiro, R.Y. and Isernia, P. (eds) *Decisionmaking in a Glass House*, New York: Rowman & Littlefield.

Eriksson, J. and Noreen, E. (2002) ‘Setting the agenda of threats: An explanatory model’, *Uppsala Peace Research Papers*, 6. Online. Available HTTP: <http://www.pcr.uu.se/publications/UPRP_pdf/uprp_no_6.pdf> (accessed 17 August 2007).

Eriksson, J. (2001) ‘Cyberplagues, IT, and security: Threat politics in the information age’, *Journal of Contingencies and Crisis Management*, 9, 4: 200–10.

Gellman, B. (2002a) ‘Cyber-attacks by Al Qaeda feared’, *Washington Post*, 27 June 2002. Online. Available HTTP: <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26> (accessed 17 August 2007).

—— (2002b) ‘Qaeda cyberterror called real peril’, *International Herald Tribune*, 28 June 2002.

Graham, S. (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 2004. Online. Available HTTP: <http://www.surf.salford.ac.uk/documents/UrbanVulnerability/Graham.pdf> (accessed 17 August 2007).

Greene, T.C. (2002) ‘Soon Al-Qaeda will kill you on the internet’, *The Register*, 28 June 2002. Online. Available HTTP: <http://www.theregister.co.uk/2002/06/28/soon_alqaeda_will_kill_you/> (accessed 17 August 2007).

—— (2004) ‘Cyber-terror drama skates on thin black ice’, *The Register*, 25 February 2004. Online. Available HTTP: <http://www.theregister.co.uk/2004/02/25/cyberterror_drama_skates_on_thin/> (accessed 17 August 2007).

Gronke, P. and Cook, T. (2002) ‘Disdaining the media in the post 9/11 world’, paper presented at the Annual Meeting of the American Political Science Association APSA, 29 August – 1 September 2002, Boston, MA. Online. Available HTTP: <http://people.reed.edu/~gronkep/docs/apsa2002.pdf> (accessed 17 August 2007).

Hosenball, M. (2002) ‘Islamic cyberterror: Not a matter of if, but of when’, *Newsweek*, 20 May 2002. Online. Available HTTP: <http://archive.infopeace.de/msg01346.html> (accessed 17 August 2007).

Ingles-le Noble, J. (1999) ‘Cyberterrorism hype’, *Jane’s Intelligence Review*. Online. Available HTTP: <http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm> (accessed 17 August 2007).

Joint Economic Committee (2001) *Wired World: Cyber Security and the US Economy*, Washington, DC: US Government Printing Office. Online. Available HTTP: <http://www.house.gov/jec/hearings/6-21-01.pdf> (accessed 17 August 2007).

King, B. (2002) ‘Fear and lockdown in America’, *Wired*, 25 July 2002. Online. Available HTTP: <http://www.wired.com/news/digiwood/0,1412,54099,00.html> (accessed 17 August 2007).

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass*

Destruction, Oxford: Oxford University Press.

Lipschutz, R.D. (1995) *On Security*, New York: Columbia University Press.

Livingston, S. (1994) *The Terrorism Spectacle*, Boulder: Westview Press.

McAlearney, S. (2001) 'Cyberspace braces for escalation and war', *Information Security*, 3, 89. Online. Available HTTP: <http://archive.infopeace.de/msg00639.html> (accessed 17 August 2007).

McGray, D. (2003) 'The minister of net defense', *Wired*, 11, 5. Online. Available HTTP: <http://www.wired.com/wired/archive/11.05/schmidt.html> (accessed 17 August 2007).

Pew Internet & American Life Project (2003) *Survey with Federal Computer Week Magazine About Emergencies and the Internet*. Online. Available HTTP: <http://www.pewinternet.org/pdfs/PIP_Preparedness_Net_Memo.pdf> (accessed 17 August 2007).

Pollard, N.A. (2004) 'Indications and warning of infrastructure attack', in Nicander, L. and Ranstorp, M. (eds) *Terrorism in the Information Age: New Frontiers?* Stockholm: National Defence College, pp. 41–57.

Pollitt, M.M. (1998) 'Cyberterrorism: Fact or fancy?' *Computer Fraud and Security*, February: 8–10.

Porteus, L. (2001) 'Feds still need to define role in tackling cyberterror, panelists say', *GovExec.com*, 15 May 2001. Online. Available HTTP: <http://www.govexec.com/dailyfed/0501/051501td.htm> (accessed 17 August 2007).

Poulsen, K. (1999) 'Info war or electronic sabre rattling?' *ZDNet*, 8 September 1999. Online. Available HTTP: <http://zdnet.com.com/2100-11-515631.html?legacy=zdnn> (accessed 17 August 2007).

—— (2001) ‘Cyber terror in the air’, *SecurityFocus.com*, 30 June 2001. Online. Available HTTP: <http://www.securityfocus.com/columnists/6> (accessed 17 August 2007).

—— (2003) ‘Official: Cyberterror fears missed real threat’, *SecurityFocus.com*, 31 July 2003. Online. Available HTTP: <http://www.securityfocus.com/news/6589> (accessed 17 August 2007).

Ross, A. (2000) ‘Hacking away at the counter-culture’, in Bell, D. and Kennedy, B.M. (eds) *The Cybercultures Reader*, London & New York: Routledge, pp. 254–67.

Ryan, P.S. (2004) ‘War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics’, *Virginia Journal of Law & Technology*, 9, 7: 1–57. Online. Available HTTP: <http://ssrn.com/abstract=585867> (accessed 17 August 2007).

Sandwell, B. (2006) ‘Monsters in cyberspace: Cyberphobia and cultural panic in the information age’, *Information, Communication & Society*, 9, 1: 39–61.

Schwartau, W. (ed.) (1994) *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, New York: Thunder’s Mouth Press.

Skibell, R. (2002) ‘The myth of the computer hacker’, *Information, Communication & Society*, 5, 3: 336–56.

Specter, M. (2001) ‘The doomsday click: How easily could a hacker bring the world to a standstill?’ *The New Yorker*, 28 May 2001. Online. Available HTTP: <http://www.michaelspecter.com/ny/2001/2001_05_28_doomsday.html> (accessed 16 October 2007).

Stone, A. (2001) ‘Cyberspace: The next battlefield’, *USA Today*, 16 June 2001. Online. Available HTTP: <http://www.usatoday.com/tech/news/2001-06-19-cyberwar-full.htm> (accessed 17 August 2007).

Taylor, P.A. (1999) *Hackers: Crime in the Digital Sublime*, London: Routledge.

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

Wæver, O. (1995) 'Securitization and descuritization', in Lipschutz, R. (ed.) *On Security*, New York: Columbia University Press, pp. 48–55.

Wallace, C. (2002) 'Internet as weapon: Experts fear terrorists may attack through cyberspace', *ABC News.com*, 16 September 2002. Online. Available HTTP: <http://www.911jobforums.com/archive/index.php/t-14870.html> (accessed 23 September 2007).

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

Yould, R. (2003) 'Beyond the American fortress: Understanding homeland security in the information age', in Latham, R. (ed.) *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York: The New Press, pp. 74–98.

---

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

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

[3] A number of academic analyses of cyberterrorism also include such scenarios, see Collin 1998; Devost, Houghton, and Pollard 1997.

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

[5] 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 (Joint Economic Committee 2001: 6–10).

[6] 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 de-hype 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 significant amount of the commentary on cyberterrorism produced by *ZDnet* ('Information Resources for IT Professionals').

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

[8] Ralf Bendrath describes Schwartau as 'the rock manager turned preacher of 'information warfare'' (Bendrath 2003: 49). In the aftermath of 11 September 2001, Schwartau re-released his 1991 novel *Terminal Compromise* under the new title *Pearl Harbor 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.'

[9] The search was undertaken on 18 August 2004 and used the terms 'electronic Pearl Harbor' (68), 'digital Pearl Harbor' (35), and 'cyber Pearl Harbor' (2).

[10] A team at the Center for Strategic and International Studies has pointed out that the term 'electronic Waterloo' is more accurate, but it is much less used (see CSIS 1998: 2).

[11] François Debrix uses the term 'e-anxiety' (Debrix 2001: 165), while Barry Sandwell refers to 'cyberphobia', 'cyberfear', and 'cyberparanoia' (Sandwell 2006: 40 and 47).

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

[13] In *The Register*, Thomas C. Greene contributed the tongue-in-cheek article 'Soon Al-Qaeda Will Kill You on the Internet' (Greene 2002).

[14] Sachs collaborated on a fiction book entitled *Zero-Day Exploit: Countdown to Darkness* (Rob Shein 2004, Syngress Media) 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).