# Cyberterrorism:

## Understandings, Debates and Representations

Andrew Whiting, Stuart Macdonald, and Lee Jarvis

**Abstract**

This chapter focuses on understandings and debates around cyberterrorism as well as the effect particular representations of this phenomenon have upon assessing its threat. The chapter begins by introducing various understandings of cyberterrorism and differentiates between narrow and broad conceptions as well as effects and intent based definitions. Moving onto consider the threat of cyberterrorism the chapter identifies an ongoing debate between 'concerned' and 'sceptical' voices as well as those that contest whether cyberterrorism has ever taken place. The chapter then introduces a range of broadly constructivist studies which question the orthodox approach to cyberterrorism as an ontological reality and highlight the importance of media representations of this threat. To illustrate this, the chapter concludes by highlighting findings from a recent study of global news media coverage. It shows that this media is frequently apprehensive in tone, despite the existence of diverse understandings of cyberterrorism and cybersecurity.

**Key words**: Cyberterrorism; Terrorism; Threat; News Media; Cybersecurity

The history of terrorism – if a singular, coherent history, indeed, exists – might be characterized according to two discontinuous trends. First, is an empirical discontinuity which relates to the quite significant transformations that have taken place in the diverse groups conducting terrorist violence, their motivations, the modus operandi employed, the justifications offered, and the communicative impact of such violences. Potentially distinct

from this, however, is a second – conceptual – discontinuity, the changes in how "terrorism" is understood and evaluated since this concept's emergence. It is often noted, for instance, that the term originally referred to the state as wielder – rather than victim – of violence. Less common, yet no less important, is the observation that the contemporary characterization of terrorism as immoral, or even "evil," fits awkwardly with this term's earlier normative connotations. Although very few violent actors, today, would refer to themselves by this moniker – as Louise Richardson put it, terrorism is something "the bad guys do"[1] – this was not always the case. As the Russian revolutionary Nikolai Morozov put it in 1880: "Contemporary terroristic struggle" is "the struggle of force against force, of equal against equal; the struggle of heroism against opposition, of knowledge and education against bayonets and gallows."[2]

Cyberterrorism – perhaps the most significant contemporary addition to the "terrorism" family – speaks to each of these discontinuities. This chapter explores whether the types of activity described as "cyberterrorist" differ from other types of "traditional," "offline" or "non-cyber terrorism" and alongside this asks whether thinking about online activities from counter-surveillance to cyber-attacks as forms of terrorism has implications for existent understandings of this concept.

## I. Defining Cyberterrorism

Although the term 'cyberterrorism' is widely attributed to Barry Collin in the 1980s, its meaning remains hotly contested within the relevant academic literature. One major obstacle to defining the term lies in a broader inability to define terrorism itself.[3] Emerald Archer, for example, comments that, "there is no universally agreed upon definition of terrorism broadly, or cyber terrorism specifically."[4] Ayn Embar-Seddon, similarly, argues that prior uncertainty around terrorism's true meaning poses "a significant barrier to constructing a definition of

cyberterrorism."[5] It is certainly true that, whilst it is often (although not always[6]) viewed as a distinct concept, cyberterrorism inherits definitional issues from its parent concept.

Perhaps the most widely known definition of cyberterrorism surfaced in the testimony of Dorothy Denning on May 23rd 2000 to the U.S. House of Representatives' Special Oversight Panel on Terrorism[7] and has subsequently been used in "numerous articles and interviews."[8] In Denning's understanding, cyberterrorism refers to:

> …the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.[9]

Denning then goes on to add that, "attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples [of cyberterrorism]" and "serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact" but that "attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[10]

In contrast to Denning, another prominent scholar in this field - Gabriel Weimann – offers the following definition: "Cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)."[11] There are four differences between this definition and Denning's. First, whilst Denning's definition does not specify that cyberterrorism has to be conducted via a computer – merely that it must involve an attack "against computers, networks, and the information stored therein"[12] – Weimann's definition focuses on computers as the means, as well as the target, of the attack. Second, Weimann's definition offers no details as to the motivation of the attackers, while Denning highlights the importance of political and social objectives.

Third, for Weimann, cyberterrorism only refers to the use of computers as a weapon against the specific networks upon which critical national infrastructures (CNI) rely. And, fourth, Weimann's definition does not specify that physical violence to people or property or severe economic harm must have ensued in order for an attack to qualify as cyberterrorism.

In spite of their differences, the definitions offered by both Denning and Weimann are similar in that they are both effects-based. Neither Denning's nor Weimann's definition says anything about the actors involved. This is in contrast to others, such as Roland Heickerö, who argue that, "cyber terrorism is not limited to organisations and individuals; states are sometimes also involved."[13] By contrast, Denning's and Weimann's definitions both specify particular results that must have occurred in an attack in order for it to constitute cyberterrorism.

Denning's and Weimann's definitions form part of a broader discussion in which many authors express concern that the term cyberterrorism is used to cover too many different phenomena. Thus, Denning wrote that "cyberterrorism has been used to characterise everything from minor hacks to devastating attacks."[14] Embar-Seddon also takes exception to the inclusion of so diverse a range of activities under the heading of cyberterrorism.[15] For her, acts such as "hacking" constitute "unauthorised access to or use of a computer system"[16] and so should not be categorized as cyberterrorism, which she defines – in a manner similar to Weimann – as: "acts of terrorism carried out through the use of a computer."[17] Moreover, for Embar-Seddon the presence of offline violence is crucial for an act to constitute cyberterrorism.[18] This is echoed by Heickerö[19] and by Maura Conway, who states that to qualify as cyberterrorism an attack must "result in death and/or large scale destruction."[20] Whilst effects-based definitions such as these concentrate on the aftermath of cyber-attacks, others focus instead upon the objectives of an attack's perpetrator. These intent-based definitions tend to view cyberterrorism as, "politically motivated computer attacks [that] are

done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage."[21] Cyberterrorism, here, may be separated from other forms of online activity precisely because of a protagonist's underlying intentions. Jerrold Post, Keven Ruby and Eric Shaw, for example, offer such an understanding, arguing that cyberterrorism is distinguishable by "the degree to which the attack was designed to produce fear and intimidation in the target audience in order to accomplish an ideological goal."[22] These elements of fear and intimidation in the pursuit of broader political or ideological purposes are prominent in many definitions of "terrorism" more generally.

Other attempts to help identify acts as, or differentiate them from, cyberterrorism are observable within the literature. They speak to the criticism that apparently separate phenomena have overlapped to a problematic degree.[23] For example, Denning produces a threefold distinction between activism, hacktivism and cyberterrorism, with activism being the use of the internet for propaganda purposes, hacktivism the merger of activism with hacking techniques to disrupt a target's intended operations (for example a Distributed Denial of Service, DDoS, attack on a website) and finally, cyberterrorism which is distinguished from the two in line with Denning's definition referred to above: the inclusion of damage on a par with "physical acts of terrorism."[24]

Just as there are those who look to impose tighter boundaries on the definition of cyberterrorism, other authors are willing to include a far-greater list of actions under this heading. For example, Angela Clem, Sagar Galwankar and George Buck state that cyberterrorism can be used to: "(1) help plan other terrorist activities; (2) soften a target prior to a physical attack; or (3) generate more fear and confusion concurrent with other terrorist acts."[25] Such a definition is far more expansive than those outlined above. Indeed, some of the activities that might be classed as cyberterrorism in this approach would rarely be

regarded as terrorism if perpetrated in the purely "physical" world: the authors include altering or destroying health insurance records as an example.

Clem, Galwankar and Buck are not alone in offering a very broad definition of cyberterrorism. There are others who do similar, whilst carving cyberterrorism up into distinct sub-categories. For these authors, the key distinctions are not between cyberterrorism and other entities. Rather, they are *within* the concept of cyberterrorism itself. This is illustrated by the following statement from the former United States Deputy Assistant Attorney General John G. Malcolm:

> Cyberterrorism involves the use of computer systems to carry out terrorist acts, which are, in turn, defined by reference to specific criminal statutes. *True* cyberterrorism is characterised by large-scale destruction (or the threat of such destruction) coupled with an intent to harm or coerce a civilian population or government.[26]

General Malcolm thus offers a broad understanding of cyberterrorism as the use of computer systems to conduct terrorism, but then adds another level by arguing that "true" cyberterrorism must have a violent or destructive element – or at least the threat of one – thereby offering an effects-orientated definition of "true" cyberterrorism. A similar example may be found in Kevin Desouza and Tobin Hensgen, who view cyberterrorism "under two lights": conventional (attacks that disrupt information infrastructure)[27] and unique (for example simple communication between terrorists online).[28] George Kostopoulos, meanwhile, distinguishes between *three* "basic types of cyberterrorists": the professionals, the amateurs, and the thieves. The professionals, "aim at inflicting physical or cyber damage onto victim's resources," the amateurs, "find pleasure in applying cyber graffiti" and the thieves, "have immediate personal illicit economic benefit from their actions."[29] Kostopoulos defines cyberterrorism so broadly that practically any misuse of computers, including much

of which would commonly be understood as cybercrime, can be categorised within his threefold classification.

Perhaps the most significant attempt to draw a distinction within the concept of cyberterrorism is the argument that we should talk in terms of "cyberterrorism" and "pure cyberterrorism." While there are those for whom such a distinction is becoming more difficult to discern,[30] Sarah Gordon and Richard Ford argue that cyberterrorism, "involves the use of computer systems to carry out terrorist acts" which includes countless "everyday" functions.[31] Commenting on Denning's definition outlined above, Gordon and Ford state:

> ...she points out that this definition is usually limited to issues where the attack is against 'computers, networks, and the information stored therein,' which we would argue is 'pure cyberterrorism.'...we believe that the true impact of her opening statement ('the convergence of terrorism and cyberspace') is realised not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be.[32]

Gordon and Ford go on to explain that, whilst "pure cyberterrorism" involves attacks using computers to disrupt and damage computer networks, "cyberterrorism" refers to the use of "other factors and abilities of the virtual world...by the terrorist in order to complete his mission." The result of this is that cyberterrorism incorporates a whole host of actions including, for example, the September 11th 2001 attackers using computers to purchase aeroplane tickets to carry out their attack.[33]

In a similar vein to Gordon and Ford, Matthew Devost, Brian Houghton and Neal Pollard distinguish between "information terrorism" and "pure information terrorism."[34] In the table below the authors distinguish between physical and digital terrorist attacks in the information age.

**Figure 1 – "General Methods for Terrorist Attack in information Age"[35]**

| Target | | | |
|---|---|---|---|
| | | Physical | Digital |
| Tool | Physical | (a) Conventional Terrorism (Oklahoma City Bombing) | (b) IRA attack on London Square Mile 4 October 1992 |
| | Digital | (c) Hacker spoofing an air traffic control system to bring down a plane | (d) Trojan horse in public switched network |

In their analysis they conclude that "cell (a) addresses 'traditional terrorism...the authors consider cells (b), (c) and (d) to be information terrorism...the authors believe cell (d) to be 'pure' information terrorism."[36] Using this definition "information terrorism" can therefore refer to a physical act that aims at a high-tech target. In addition, Devost, Houghton, and Pollard acknowledge, in accordance with Gordon and Ford, that cyberterrorism does not necessarily have to refer to destructive actions:

> ...there are more subtle forms of information terrorism (e.g. electronic fund theft to support terrorist operations, rerouting of arms shipments, etc.) which would still be political crimes, but perhaps more dangerous because they are less dramatic than a 'cyber-Chernobyl', and thus more difficult to detect, and can even appear as 'common' crimes.[37]

Distinguishing between a specific "computer on computer" attack and activities which are facilitative or preparatory, but simultaneously including both under the broad heading

"cyberterrorism," has important ramifications not only for how the term is understood[38] but also the assessment of, and response to, the threat it is deemed to pose.

## II. Assessing the Cyberterrorism Threat

In a study of academic opinion around cyberterrorism, Jarvis, Macdonald, and Nouri identified "considerable disagreement" regarding the "extent to which this phenomenon poses a security threat."[39] Simplifying, they characterize this disagreement as a debate between "the concerned" and "the sceptics" – for whom cyberterrorism remains little more than a hyperbolic media construction. Heickerö dichotomizes this debate similarly between those who view the cyberterrorist threat as "real and considerable," and others for whom there is 'no threat at all or only a very limited one."[40] Concerned assessments of cyberterrorism tend to view cyberterrorists as "computer savvy individuals who look for vulnerabilities that can be easily exploited."[41] Due to "the number of potential targets and the lack of proper and adequate safeguards," preventing cyberterrorism is here seen as a "daunting" task for the security services.[42] According to Thomas Homer-Dixon:

> We've realised, belatedly, that our societies are wide-open targets for terrorists. We're easy prey because of two key trends: First, the growing technological capacity of small groups and individuals to destroy things and people; and, second, the increasing vulnerability of our economic and technological systems to carefully aimed attacks.[43]

Such assessments are frequently accompanied by oft-quoted lines such as "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb"[44] and lists of hypothetical nightmare scenarios first expounded by Barry Collin.[45] Moreover, these assessments often point to the possibility of terrorist organisations "recruiting their own internal force or network of highly capable programmers"[46] to exploit the systemic vulnerabilities that exists within computer systems and across networks.

The attractiveness of cyber operations to would-be terrorists is also a product, for many authors, of factors relating to ease, anonymity, and remoteness. In the first instance, cyberattacks are often seen as "easy and cheap to carry out" (requiring nothing more than a laptop and an internet connection) – so much so that anyone, "with a modicum of technological sophistication can carry out some form of attack."[47] Here, terrorists have acquired cyber weapons that offer "new, low-cost, easily hidden tools to support their cause"[48] as well as "inexpensive, yet robust communications intelligence collection capability."[49] Second, the anonymity offered by cyberspace means both that terrorists can be more confident in their communication and planning knowing they are doing so covertly[50] and that they can operate more brazenly (for example, intercepting sensitive information and engaging in counter-surveillance), safe in the knowledge that, "much of this work can be done anonymously, diminishing the risk of reprisal and increasing the likelihood of success."[51] This, alongside the ability to conduct operations remotely across different legal jurisdictions using "proxy servers and IP-change methods to hide their real addresses"[52] poses "tremendous challenges to thwart cyber-terrorist attacks."[53]

The distinction between terrorist use of cyber weapons and online communication pointed to above in efforts to differentiate 'cyber-terrorism' and 'pure cyberterrorism' is further reason for the contestability that surrounds cyberterrorism's threat. That is, while some of the relevant literature concentrates on communication, intelligence, disruption and the use of cyberspace to further physical endeavours, other contributions concentrate on the possibility of terrorists using cyberspace as a launching pad for attacks that may or may not have physical ramifications. Seymour Goodman, Jessica Kirk and Megan Kirk, for instance, outline the following terrorist uses of the internet: support, communication, recruitment, fundraising, research, explicit cyberattack (cyber target), and as a means to attack other (physical) targets.[54] While cyberattack is included in this typology the majority of the focus is

on actions that facilitate "physical terrorism." Thomas Holt, indeed, goes so far as to say that for terrorists "the most significant benefit of the Internet" is their ability to convey their extremist propaganda effectively and "directly control the way that their message is delivered to the general public."[55] Communication, here, is regarded as vital as a means to train new recruits on weapons and tactics as well as to plan and fund future attacks.[56] For Lewis, for example, "the primary use of the internet by terrorists involves information: obtaining it, disseminating it, and using it to advance their goals."[57] He goes on to offer the following summary of terrorists' use of the Internet:

> It is an organizational tool, and provides a basis for planning, command, control, communication among diffuse groups with little hierarchy or infrastructure. It is a tool for intelligence gathering, providing access to a broad range of material on potential targets, from simple maps to aerial photographs. One of its most valuable uses is for propaganda, to relay the messages, images and ideas that motivate the terrorist groups. Terrorist groups can use websites, email and chatrooms for fundraising by soliciting donations from supporters and by engaging in cybercrime (chiefly fraud or the theft of financial data, such as credit card numbers).[58]

Where Lewis focuses on uses of the internet for organisational purposes, other authors writing on cyberterrorism concentrate on the potential it provides for various forms of cyberattack. Audrey Cronin, for example, notes the increasing tendency of terrorists online to turn to hacktivism, "attacks on internet sites, including web defacements, hijackings of websites, web sit-ins, denial-of-service attacks, and automated email 'bombings'… that may not kill anyone but do attract media attention, provide a means of operating anonymously, and are easy to coordinate internationally."[59] In so doing, she points to the wide range of offensive activities opened by terrorist uses of the internet.

One problem confronting this literature, however, is that there remains considerable disagreement as to whether an event of "pure cyberterrorism" has ever occurred.[60] As a result, much of the debate is couched in hypothetical terms, often drawing upon historical analogies of questionable perspicacity. Warnings of a "Digital Pearl Harbour," for example, which posit "a debilitating, full-scale digital assault - in which multiple attacks are launched against telecommunications networks, city power grids, and/or air traffic control systems, causing widespread destruction and possible loss of life," are indicative of this tendency.[61] Even more striking are scenarios such as that offered by Homer-Dixon:

> It's 4 a.m. on a sweltering summer night in July 2003. Across much of the United States, power plants are working full tilt to generate electricity for millions of air conditioners […]. The electricity grid in California has repeatedly buckled under the strain, […]. In different parts of the state, half a dozen small groups of men and women gather. Each travels in a rented minivan to its prearranged destination – for some, a location outside one of the hundreds of electrical substations […]; for others, a spot upwind from key, high-voltage transmission lines. […] Those outside the substations put together simple mortars made from materials bought at local hardware stores, while those near the transmission lines use helium to inflate weather balloons with long silvery tails. At a precisely coordinated moment, the homemade mortars are fired, sending showers of aluminium chaff over the substations. The balloons are released and drift into transmission lines.[62]

The level of detail in this scenario leads one to assume that the author is recounting an actual event, yet it is, in fact, entirely fictional. Homer-Dixon notes that his scenario may have at one point sounded far-fetched, but argues that in a post-September 11th world it should not anymore.[63] Cyber threats such as cyberterrorism are seen as dangerous, "not because of what

they have (or have not) done to date, but precisely, because they threaten to generate serious impacts in the future."[64] As Chad Parks put it in 2003:

> It is true that America has never suffered consequences of a true cyber terrorist attack, yet. On September 10, 2001, it was also true that no organized terrorist group had ever hijacked four airplanes, crashed two into the World Trade Center, one into the Pentagon, and one in a field in Pennsylvania, killing over three thousand Americans.[65]

Nevertheless, there is a competing perspective. Evan Kohlman, for example, argues that the U.S. government's focus on the "doom-and-gloom predictions that cyberterrorists would wreak havoc on the Internet" is misguided and overlooks "the fact that terrorists currently use the Internet as a cheap and efficient way of communicating and organizing."[66] Lewis argues that "the internet is not a weapon that appeals to terrorists,"[67] something reinforced by Giacomello's cost benefit analysis of a hypothetical cyberterrorist attack, and Turki Al-Garni and Thomas Chen's subsequent study of Stuxnet: an attack directed against an Iranian nuclear power station via computer worm that was first discovered in 2010.[68]

All of these authors are of the belief that traditional physical attacks remain the most attractive option to terrorists.[69] Thus, for Denning, "terrorist groups are using the Internet, but they still prefer bombs to bytes as a means of inciting terror."[70] For Michael Stohl, similarly, the lack of clear empirical examples of pure cyberterrorism is a damning indictment of the actual threat posed and concludes that if it is not explainable due to a lack of terrorist motivation, it must be the case that they remain incapable of mounting a sufficiently destructive attack.[71] Either way, many of these authors believe that the potential dangers of cyberterrorism have been "overblown and misdirected."[72]

## III. Characterizing the Cyberterrorism Debate

Clearly there exists a diverse range of understandings of cyberterrorism and the risk that it poses. Despite this diversity, however, academic literature on this phenomenon is overwhelmingly oriented toward a conception of cyberterrorism as an extra-discursive phenomenon. Regardless of whether cyberterrorism is defined narrowly or broadly, assessed as a significant or overblown threat, whether or not it is even deemed to have occurred, there is a general consensus that such a thing as cyberterrorism exists as ontological reality.

This approach to cyberterrorism – as something which, at least in principle, can be captured in our labels and risk assessments – tends to neglect the constitutivity of competing knowledge claims thereof.[73] That is, definitions and understandings of cyberterrorism within different discursive sites – academic, governmental, media, and so on – create that which they purport to describe. And, as a consequence, security issues, such as cyberterrorism, are "made" through social and discursive practice, not "given."[74]

Despite the widespread understanding of cyberterrorism as an ontological reality, a small number of important studies may be identified which have embraced a more sceptical meta-theoretical stance toward cyberterrorism. Myriam Dunn Cavelty, for instance, employs framing theory to explore how cyberterrorism has been "securitized" – or positioned as a "security threat" – within US political discourse.[75] In similar fashion, Maura Conway attempts to "excavate" the development of "cyberterrorism" through an examination of popular, media and scholarly engagements with this term.[76] In so doing, she draws on a similarly constructivist approach to this phenomenon as something which is produced discursively. A related approach, albeit from a different disciplinary background, is evident in the work of Lorraine Bowman-Grieve who utilises social psychology literature to read news representations of "cyberterrorism" through the category of "moral panics."[77]

Alongside these studies there are also a scattering of constructivist explorations of cybersecurity discourse more broadly, wherein cyberterrorism is approached as one of a multitude of (discursively) connected threats. Barnand-Wills and Ashenden, for example, draw on Foucauldian theories of governmentality in order, "to identify a relatively consistent discourse of cyber security that involves trends of uncertainty, risk perception, securitization, and potential militarization"[78] within "current cyber security policy developments in both the United Kingdom and United States."[79] Hansen and Nissenbaum, similarly, apply securitization theory to the 2007 cyber war against Estonia to identify, "three 'security grammars' which they perceive to be distinct to the cyber security sector: hypersecuritizations, everyday security practices, and technifications."[80]

Within this literature a recurring theme is the role played by the media in constructing, and securitizing, the threat of cyberterrorism. For Gabriel Weimann, for instance, "much of the discussion of cyberterrorism has been conducted in the popular media, where journalists typically strive for drama and sensation."[81] For Maura Conway, likewise, "With the aid of the mass media, cyberterrorism came to be viewed as the 'new' security threat *par excellence*."[82]

In order to evaluate claims such as these, we undertook a recent study of over 500 news items, published by a total of 31 different outlets between 2008 and 2013, was conducted in order to offer the first detailed exploration of media representations of cyberterrorism.[83] First, the study demonstrates that the volume of news media coverage of cyberterrorism has increased in recent years.[84] Prior to October 2010, the 31 outlets between them published an average of 4.8 items mentioning cyberterrorism per month. In stark contrast, a total of 35 items mentioning cyberterrorism were published in October 2010 alone. These increased levels of interest were sustained in the 32 months that followed, with an average of 10.6 items published per month. The study identifies two events which contributed

**Commented [CV1]:** I assume this one is not a problem for OUP, but I'm highlighting it just in case.

to this upsurge: first, the release of the UK's National Security Strategy on 18 October 2010 – which identified international terrorism and cyberattack as two of the top tier threats facing the UK[85] – and the associated decision to invest an additional £650m in cybersecurity at a time when other cuts where being made to the defence budget; and, second, the revelations concerning Stuxnet, one of the first known malwares to cause physical damage to critical infrastructure.[86]

Second, media coverage of cyberterrorism is predominantly apprehensive in tone.[87] In total, two-thirds of news items identified in our research evidenced a marked concern with the threat posed by cyberterrorism, whereas just 2% of the items explored in this study took an explicitly sceptical stance to this threat. The concerned items included a number, which contained quite stark warnings of the cyberterrorism threat. Examples included a *Washington Post* article in which Shawn Henry ("who just retired as the FBI's top cyber sleuth") was quoted as saying, "Other than a weapon of mass destruction going off in one of our major cities, this is the most significant threat to our economy and national security"[88] and a CNN piece entitled "There's nothing virtual about cyber attacks" which quoted US Senator Dianne Feinstein's warning that a cyberterrorist could open the floodgates of a dam, disrupt air traffic control or shut down the New York Stock Exchange.[89] Perhaps the most striking use of hyperbole, however, was an article published in the UK's *Daily Mail* under the headline "Why Britain is desperately vulnerable to cyber terror."[90] This presented a detailed description of a digital "Pearl Harbour" in which:

> Power cuts scythed through Britain, plunging cities into darkness … The nationwide panic meant supermarket shelves emptied and petrol stations ran out of fuel … There was no TV, no radio and no mobile networks. After a fortnight, there were riots, and the military, which was itself crippled by mysterious communications glitches, was called in.

This description was followed by the foreboding statement that, "This terrifying scenario may seem like a science fiction movie. But it is exactly the sort of possibility currently being considered at the highest levels in government as part of the National Security Strategy."

Third, the study found that – just as there are diverse understandings of cyberterrorism in the academic literature outlined above – so too are there different constructions of cyberterrorism in news media discourse.[91] The most common depiction of cyberterrorists was as professionals (that is, as individuals with sufficient levels of knowledge of the most complex computer techniques to be able to target the most critical systems), followed by hackers (that is, as individuals who employ nefarious computer techniques to cause disruption and interference, but who lack the skill or motivation to cause serious levels of damage to the most critical systems). Moreover, different depictions were associated with different levels of concern. Depictions of cyberterrorists as hackers or as hacktivists are associated in the news media with below-average levels of concern. By contrast, concern levels were highest when cyberterrorists were represented as professionals. Indeed, none of the items containing this latter construction of cyberterrorists exhibited scepticism as to the threat that they pose.

As well as different constructions of this threat's protagonists, the study also found a range of quite different representations of the referent threatened by cyberterrorism. The most common referents were nation states and critical infrastructures. Others included the private sector, citizens and personal data. Again, different constructions were associated with different levels of concern. Geographically larger referents – especially "the West" or the entire globe – were associated with heightened levels of concern. Items containing this construction of the cyberterrorism threat contained numerous bold assertions, such as "Power and water and other vital services in the West could be crippled"[92] and "the western world has, almost overnight, found itself incredibly vulnerable".[93] A further example is an article

from *Russia Today*, published in 2012 following the discovery of the Flame malware, which quoted Eugene Kaspersky (head of the global IT security company Kaspersky Lab) as saying "I'm afraid it will be the end of the world as we know it … I'm scared, believe me."[94]

Fourth, as this quote from Kaspersky illustrates, the study found that news media discourse frequently employs specific authoritative voices in support of warnings of the threat posed by cyberterrorism. This reliance on "expert" opinion is particularly significant given the disagreement as to whether a cyberterrorism attack has ever taken place. As well as industry experts such as Kaspersky, there is frequent recourse to the views of intelligence professionals and political elites. Examples include a 2010 *Washington Post* article which recounted former FBI Director Robert S. Mueller III's warning that the cyberterrorism threat is "real and … rapidly expanding" and that terrorists have shown a "clear interest" in pursuing "hacking skills," for inflicting further damage upon "our economy and our psyche"[95] and a 2009 BBC report which reported the former Home Secretary David Blunkett's warning that jihadists "could be planning to attack national infrastructure - power grids, telecommunications and the like - via the internet, in order to hit a big and symbolic target: the 2012 London Olympics."[96] The study also found widespread use of analogy and other forms of comparison with offline or historical events to concretize the potential consequences of a cyberterrorism attack.[97] One of the most common examples is, again, warnings of an electronic or cyber Pearl Harbor. Indeed, remarks by Leon Panetta on this possibility were widely reported in 2012.[98] Panetta has also been widely cited as drawing an analogy with 9/11. A *Washington Post* article, for example, quoted Panetta as warning that a digital attack "could be as destructive as the terrorist attack on 9/11," virtually paralyzing the country.[99] Meanwhile, in a report in *The Guardian* in 2009 it was 9/11's unpredictability rather than destructiveness which was put to analogous effect: "just as the 9/11 attacks were an unprecedented attack with unconventional weapons, so too could a major cyber attack."[100]

The same newspaper also later reported on US efforts to bolster resilience to cyberterrorism through legislation "aimed at avoiding a cyber 'Hurricane Katrina' situation in which a disaster is aggravated by a bungled government response."[101] References to specific historical events such as Pearl Harbor, 9/11 and Hurricane Katrina underscore the seriousness of ill-understood technologies and actors for readers, while simultaneously reminding us that unexpected events do occur.

## IV. Conclusion

By introducing some of the key questions raised by the emergence of "cyberterrorism" this chapter has sought to draw attention to this increasingly prominent category of scholarly, political and media discourse. The chapter began by arguing that – despite its comparatively recent emergence – the term is already surrounded by considerable definitional contestability. Although part of this is a product of broader debates, which have long bedevilled its parent concept, also important are the diversity of ways in which those designated "terrorist" engage with cyber technologies. The second section then explored a number of issues around the threat posed by this form of terrorism, differentiating between "concerned" and "sceptical" voices and concluded by exploring how this phenomenon is represented in the international news media. In this final section it was noted that coverage of cyberterrorism has increased markedly over time and that it is predominantly apprehensive in tone. This is despite the existence of quite different understandings of this threat, its referents, and its likely protagonists.

## Bibliography


Collin, Barry. “The Future of Cyberterrorism.” *Crime and Justice International* 13 (1997): 15-18.

Chen, Tom., Jarvis, L., Macdonald, S. *Terror Online: Politics, Law and Technology*. London: Routledge, 2015.

Conway, Maura. “Cyberterrorism: Media Myth or Clear and Present Danger?” In *War and Virtual War: The Challenges to Communities*, edited by Jones Irwin, 79-98, Rodopi: Amsterdam/New York, 2004.

Denning, Dorothy. “Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives,” 2002, accessed January 31, 2012, http://www.stealth iss.com/documents/pdf/CYBERTERRORISM.pdf.

Dunn Cavelty, Myriam. “Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.” *Journal of Information Technology & Politics* 4 (2008): 19-36.

Hansen, Lene., and Nissenbaum, Helen. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53 (2009), 1155-1175.

Jarvis, Lee., Macdonald, Stuart., Whiting, Andrew. “Unpacking Media Discourse on Cyberterrorism: The Significance of Specificity, Status and Scale in Constructions of Threat.” *European Journal of International Security*, 2 (2017): 64-87.

Stohl, Michael, “Cyber Terrorism: a Clear and Present Danger, the Sum of all Fears, Breaking Point or Patriot Games?” *Crime, Law and Social Change* 46 (2006): 223-238.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?" *United States Institute of Peace Special Report* 119 (2004), n.p.

Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict and Terrorism* 28 (2005): 129-149

[1] Louise Richardson, *What Terrorists Want: Understanding the Terrorist Threat* (London: John Murray, 2000).

[2] Cited in *Voices of Terror: Manifestos, Writings and Manuals of Al Qaeda, Hamas, and Other Terrorists From Around the World and Throughout the Ages*, ed. Walter Laqueur (New York, NY: Reed Press, 2004), 78.

[3] There is an extensive literature on the (in)ability of various actors to define terrorism. For introductions, see, amongst many others Bruce Hoffman, *Inside Terrorism* (Chichester: Columbia University Press, 2006); Richard Jackson et al., *Terrorism: A Critical Introduction* (Basingstoke: Palgrave Macmillan, 2011); Brian Michael Jenkins, *The Study of Terrorism: Definitional Problems* (Santa Monica, CA: RAND, 1980); Leonard Weinberg, Ami Pedahzur and Sivan Hirsch-Hoefler, "The Challenges of Conceptualising Terrorism," *Terrorism Studies: A Reader*, eds. John Horgan and Kurt Braddock (Abingdon: Routledge, 2012); Alex P. Schmidt, *The Routledge Handbook of Terrorism Research* (Abingdon: Routledge, 2011); Alex P. Schmidt and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature* (NJ: Transaction, 2005).

[4] Emerald Archer, "Crossing the Rubicon: Understanding Cyber Terrorism in the European Context," *The European Legacy: Toward New Paradigms*, 19 (2009): 607.

[5] Ayn Embar-Seddon, "Cyberterrorism: Are We Under Siege?," *The American Behavioral Scientist*, 45 (2002): 1034.

[6] Embar-Seddon comments that, "…by simply placing the word cyber, computer or information before another word…this can seem to denote an entirely new thing, but often, it does not. These neologisms can create confusion." See Embar-Seddon, "Cyberterrorism: Are We Under Siege," 1034.

[7] Dorothy Denning, "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives," 2002, accessed January 31, 2012, http://www.stealthiss.com/documents/pdf/CYBERTERRORISM.pdf.

[8] Maura Conway, "Cyberterrorism: Media Myth or Clear and Present Danger?," in *War and Virtual War: The Challenges to Communities*, ed. Jones Irwin (Rodopi: Amsterdam/New York, 2004), 84.

[9] Denning, "Cyberterrorism: Testimony."

[10] Ibid.

[11] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict and Terrorism*, 28 (2005): 130.

[12] Denning, "Cyberterrorism: Testimony."

[13] Roland Heickerö, "Cyberterrorism: Electronic Jihad," *Strategic Analysis*, 38 (2014): 556. For more on the possibility of state cyberterrorism see: Lee Jarvis, Stuart Macdonald and Lella Nouri, "State Cyberterrorism: A Contradiction in Terms?," *Journal of Terrorism Research*, 6 (2015): 62-75.

[14] Dorothy Denning, "Terror's Web: How the Internet is Transforming Terrorism," in *Handbook on Internet Crime*, eds. Yvonne Jewkes and Y. and Majid Yar (Devon: Willan Publishing, 2010), 7.

[15] Embar-Seddon, "Cyberterrorism: Are We Under Siege," 1035.

[16] Ibid, 1037.

[17] Ibid, 1035.

[18] Ibid, 1037.

[19] Roland Heickerö, "Cyberterrorism: Electronic Jihad," 555.

[20] Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'use' of the Internet," *First Monday*, 7 (2002), n.p.

[21] Jian Hua and Sanjay Bapna, "How Can We Deter Cyber Terrorism?," *Information Security Journal: A Global Perspective*, 21(2012): 104.

[22] Jerrold M. Post, Kevin G Ruby, and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence*, 12 (2000): 101.

[23] See: Susan Brenner, ""At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law and Criminology*, 97 (2007), 390-398; Bill Nelson et al., *Cyberterror: Prospects and Implications* (Monterey, CA: Centre for the Study of Terrorism and Irregular Warfare, 1999), accessed September 07, 2015, http://www.nps.edu/academics/centers/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf, 15; Weimann, "Cyberterrorism: The Sum of All Fears," 141.

[24] Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, eds. John Aquilla and Ronfeldt, D. F. (Santa Monica, CA: RAND Corporation), 239-288.

[25] A. Clem, Sagar Galwankar, and George Buck, "Health Implications of Cyber-Terrorism," *Prehospital and Disaster Medicine*, 18 (2003): 273.

[26] John G. Malcolm, "Testimony of Deputy Assistant Attorney General John G. Malcolm on Cyberterrorism,' before the Senate Judiciary Committee Subcommittee on Terrorism, Technology, and Homeland Security," (February 24, Washington: DC, 2004). (Emphasis added)

[27] Kevin Desousza and Tobin Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism," *Technological Forecasting and Social Change*, 70 (2003): 387.

[28] Ibid, 388.

[29] George Kostopoulos, "Cyberterrorism: The Next Arena of Confrontation," *Communications of the IBIMA,* 6 (2008): 165.

[30] Roland Heickerö, "Cyberterrorism: Electronic Jihad," 555.

[31] Sarah Gordon and Richard Ford, *Cyberterrorism?* (Cupertino, CA: Symantec, 2003), 4.

[32] Ibid.

[33] Ibid.

[34] Matthew G. Devost, Brian K. Houghton and Neal Allen Pollard, "Information Terrorism: Political Violence in the Information Age," *Terrorism and Political Violence*, 9 (1997): 78.

[35] Adapted from Matthew Devost et al, "Information Terrorism," 78.

[36] Devost et al, "Information Terrorism," 78.

[37] Ibid.

[38] Keiran Hardy and George Williams in their chapter investigating legal definitions of cyberterrorism note that the UK, Australia, Canada and New Zealand have the same "general thrust" but also note that of these definitions only Canada requires that infrastructure targeted be "essential" and only New Zealand requires the act of cyberterrorism to be "likely to endanger life." See Keiran Hardy and George

Williams, "What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism," in *Cyberterrorism: Understanding, assessment and response*, eds. Tom Chen, Lee Jarvis, Stuart Macdonald. (London: Springer, 2014), 1-23.

[39] Lee Jarvis, Stuart Macdonald and Lella Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers," *Studies in Conflict and Terrorism*, 37 (2014): 83.

[40] Heickerö, "Cyberterrorism: Electronic Jihad," 555.

[41] Fawzi Cassim, "Addressing the Spectre of Cyber Terrorism: A Comparative Perspective," *Potchefstroom Electronic Law Journal*, 15 (2012): 381.

[42] Ibid, 388.

[43] Thomas Homer-Dixon, "The Rise of Complex Terrorism," *Foreign Policy*, 128 (2002): 53.

[44] National Research Council, "Computers at Risk" (Washington, DC: National Academy Press, 1991), 7.

[45] Barry Collin, "The Future of Cyberterrorism," *Crime and Justice International*, 13 (1997): 15-18.

[46] Archer, "Crossing the Rubicon," 616.

[47] Michael Vatis, "The Next Battlefield," Harvard International Review, 28 (2006): 58.

[48] John A. Seabian, "Cyber threats and the US economy: Statement for the Record Before the Joint Economic Committee on Cyber Threats and the US Economy." https://www.cia.gov/newsinformation/speechestestimony/2000/cyberthreats_022300.html. Accessed September 7th 2015.

[49] Frank Cilluffo and Paul Pattak, "Cyber threats: Ten Issues for Consideration," *Georgetown Journal of International Affairs*, 1 (2000): 44.

[50] Steven Grogan, "China, Nuclear Security and Terrorism: Implications for the United States," *Orbis*, 53 (2009): 698.

[51] Cilluffo and Pattak, "Cyber Threats," 44.

[52] Hua and Bapna, "How Can We Deter Cyber Terrorism?," 105.

[53] Ibid.

[54] Seymour Goodman, Jessica Kirk, and Megan Kirk, "Cyberspace as a Medium for Terrorists," *Technological Forecasting & Social Change*, 74 (2007): 198-199.

[55] Thomas J.Holt, "Exploring the Intersections of Technology, Crime, and Terror," *Terrorism and Political Violence*, 24 (2012): 341.

[56] Homer-Dixon, "The Rise of Complex Terror," 54.

[57] James A. Lewis. "The Internet and Terrorism." Accessed 7 September 2015. http://csis.org/files/media/csis/pubs/050401_internetandterrorism.pdf, 2.

[58] ibid., 1.

[59] Audrey Kurth Cronin, "Behind the Curve: Globalisation and International Terrorism," *International Security*, 27 (2002-2003): 46-47.

[60] Jarvis, Macdonald, and Nouri, "The Cyberterrorism Threat," 83.

[61] John Podesta and Raj Goyle, "Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World," *Yale Law and Policy Review*, 23 (2005), 516.

[62] Homer-Dixon, "The Rise of Complex Terror," 52-53.

[63] Ibid., 53.

[64] Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal*, 52 (2011): 382.

[65] Chad Parks, "Cyber Terrorism: Hype or Reality?," *The Journal of Corporate Accounting and Finance*, 14 (2003): 11.

[66] Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs*, 85(2006): 115-116.

[67] Lewis, "The Internet and Terrorism," 1.

[68] Turki Al-Garni and Tom Chen (2015) "An Updated Cost-Benefit View of Cyberterrorism," in Tom Chen, Lee Jarvis, and Stuart Macdonald (eds.) *Terror Online: Politics, Law and Technology* (London: Routledge, 2015), 72-85

[69] Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism*, 27 (2007): 388.

[70] Denning, "Cyberwarriors," 70.

[71] Michael Stohl, "Cyber Terrorism: a Clear and Present Danger, the Sum of all Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change*, 46 (2006): 236.

[72] Maura Conway, "Reality Check: Assessing the (Un)likelihood of Cyberterrorism," in *Cyberterrorism: Understanding, Assessment and Response*, Chen, Jarvis and Macdonald, eds., 103-122; Podesta and Goyle, "Lost in Cyberspace?," 517; Weimann, "Cyberterrorism: The Sum of all Fears," 131.

[73] This argument has been made by the authors elsewhere, see, Lee Jarvis, Stuart Macdonald and Andrew Whiting, "Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Discourse," *Global Society* 30 (2016):. 605-623. See also, Charlotte Epstein, "Constructivism or the Eternal Return of Universals in International Relations. Why Returning to Language is Vital to Prolonging the Owl's Flight," *European Journal of International Relations*, Vol. 19, No. 3 (2013), 399-519.

[74] For a recent overview on debates over how this process takes place within securitization theory, see Mark B. Salter and Can E. Mutlu, "Securitisation and Diego Garcia," *Review of International Studies*, 39 (2013): 815-834.

[75] Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics*, 4 (2008): 19-36.

[76] Conway, "Cyberterrorism: Media Myth or Clear and Present Danger?," 79-98.

[77] Lorraine Bowman-Grieve, "Cyber-Terrorism and Moral Panics: A Reflection on the Discourse of Cyberterrorism," in *Terrorism Online: Politics, Law and Technology*, Tom Chen, Lee Jarvis, Stuart Macdonald, eds. (Abingdon: Routledge, 2015), 86-106.

[78] David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk," *Space and Culture,* 15 (2012):10-123, 110.

[79] Ibid., 111.

[80] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, 53 (2009), 1155-1175, 1171.

[81] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?," *United States Institute of Peace Special Report*, 119 (2004), n.p.; See also Weimann, "Cyberterrorism: The Sum of All Fears?," 129–149.

[82] Maura Conway, "The Media and Cyberterrorism: A Study in the Construction of 'Reality.'" Accessed 16 May 2015. http://doras.dcu.ie/2142/1/2008–5.pdf, 43–44.

[83] Chen, T., Jarvis, L., Macdonald, S., and Whiting, A. (2014) *Cyberterrorism and the News Media*. Cyberterrorism Project Research Report (No. 3). Accessed September 7th 2015. www.cyberterrorism-project.org.

[84] Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage," *Perspectives on Terrorism*, 9 (2015), 60-75.

[85] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, Cm 7953.

[86] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53(2011), 23-40.

[87] Jarvis, Macdonald, and Whiting, "Constructing Cyberterrorism as a Security Threat," 60-75.

[88] Sari Horwitz, "Justice Department trains prosecutors to combat cyber-espionage," *Washington Post*, 25 July 2012, available at https://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html (last accessed 26 August 2015).

[89] Bob Greene, "There's Nothing Virtual About Cyber Attacks," *CNN*, 7 October 2012, http://edition.cnn.com/2012/10/07/opinion/greene-cyber-real/ (last accessed 26 August 2015).

[90] Michael Hanlon, "Why Britain is Desperately Vulnerable to Cyber Terror," *Daily Mail* 19 October 2010, available at: http://www.dailymail.co.uk/debate/article-1321729/Why-Britain-vulnerable-cyber-terror-attacks.html (last accessed 26 August 2015).

[91] Lee Jarvis, Stuart Macdonald, Andrew Whiting, "Unpacking Cyberterrorism Discourse: Specificity, Status and Scale in News Media Constructions of Threat," *European Journal of International Security*, 2 (2017): 64-87.

[92] Christopher Williams, "Stuxnet Virus Could be Adapted to Attack the West,'" *The Telegraph*, July 27 2011, accessed July 14 2015, http://www.telegraph.co.uk/technology/news/8665487/Stuxnet-virus-could-be-adapted-to-attack-the-West.html

[93] Dylan Welch, "Cyber Soldiers," *The Sydney Morning Herald*, October 9 2010, accessed July 14 2015, http://www.smh.com.au/technology/technology-news/cyber-soldiers-20101008-16c7e.html

[94] N.A. "'End of the World as We Know It': Kaspersky Warns of Cyber-Terror Apocalypse," *Russia Today*, June 6 2012, accessed August 28 2014, http://rt.com/news/kaspersky-fears-cyber-pandemic-170/

[95] Robert S. Mueller III quoted in Ellen Nakashima, "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat," *The Washington Post*, 4 March 2010, accessed June 28 2015, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

[96] "Is the UK Safe from Cyber Attack?," BBC News, 30 April 2009, accessed 28 June 2015, http://news.bbc.co.uk/1/hi/technology/8025148.stm.

[97] See also, see: Stohl, *op. cit.*, 223-238; Conway, "The Media and Cyberterrorism," *op. cit.*, 1-53.

[98] Adam Samson, "Another Week, Another Threat Against U.S. Banks," *Fox Business*, October 16 2012, accessed December 15 2014, http://www.foxbusiness.com/industries/2012/10/16/another-week-another-threat-against-us-banks/.

[99] Robert O'Harrow Jr., "CyberCity Allows Government Hackers to Train for Attacks," *The Washington Post*, November 26 2012, accessed July 23 2014, http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html.

[100] Bobbie Johnson, "Terrorists Could Use Internet to Launch Nuclear Attack: Report," *The Guardian*, July 24 2009, accessed December 15 2014, http://www.theguardian.com/technology/2009/jul/24/internet-cyber-attack-terrorists.

[101] Daniel Nasaw, "US Takes Steps to Create Infrastructure Against Cyber Attack," *The Guardian*, April 7 2009, accessed December 15 2014, http://www.theguardian.com/technology/2009/apr/07/cyber-security-legislation-usa.