Reality Check: Assessing the (Un)Likelihood of Cyberterrorism

Maura Conway

Chapter Overview
This chapter argues that debates around the threat posed by cyberterrorism have been dominated by a focus on issues relating to technological potentialities. To balance this, it focuses on the 'terrorism' aspect of cyberterrorism, arguing that it is important to situate cyber attacks within an analysis of terrorist interests and options. Doing so, it argues, leads to a far more optimistic forecast of the likelihood of cyberterrorism than is common, for four reasons. First, the costs of cyber attacks – although difficult to estimate – are vastly higher than those of non-cyber equivalents, such as car bombings. Second, terrorist groups typically lack the mastery to carry out successful cyber attacks which are exponentially more difficult than non-cyber terrorism. Third, the destructive potential of non-cyber attacks can be far more readily materialised than that of cyber attacks. And, fourth, cyberterrorism lacks the theatricality of more conventional attacks and therefore is likely to be less desirable to terrorist groups. Taken together, these four arguments indicate that cyberterrorism remains far less likely than is frequently supposed.

Introduction

A January 2013 article on the prominent technology news website ArsTechnica headlined 'Security Pros Predict "Major" Cyber Terror Attack This Year' reports upon the results of a survey of computer security professionals at the October 2012 Information Systems Security Association conference in Anaheim, California. The survey found that of 105 attendees surveyed, 79 percent believed, "there will be a 'major' cyberterrorism event within the next year." Read the piece more closely however and it emerges that what the survey respondents actually believe is that there will be some sort of large-scale attack on the information technology powering some element of America's critical infrastructure (i.e. the electrical grid, energy sector, financial institutions, etc.). In fact, the survey didn't mention cyberterrorism; it "didn't give a definition for a major cyber attack" at all. "We left that to the security professionals to interpret for themselves," a representative from the company that conducted the survey is reported as saying; "[t]he general idea of the question was 'is something big going to happen?'" (Gallagher 2013). Unfortunately, the assumption that any 'big' attack with a cyber-component may be deemed 'cyberterrorism' is commonplace as is the assertion that cyberterrorism is just around the corner. There is no doubt that cyber insecurity and thus cyber threats are serious, increasing, and warrant attention, including from IT professionals, media, scholars, and policymakers. It is certainly the case that, globally, critical cyber infrastructures are insufficiently secured and are thus highly vulnerable to attack. However, the widespread assumption that such an attack will be of a cyberterrorist sort completely omits the calculations likely to be made by terrorists in weighing the costs and benefits of cyberterrorism versus other methods available to them. Such calculations are at least as important, if not more so, than the technological aspects of cyberterrorism. Just because IT professionals, journalists, policymakers, and some scholars tend to narrow their thinking to and thence privilege the technology, it should not be assumed that terrorists are of a similar mind. The technology is only half the story, in other words; this chapter addresses the other half (compare with Wilson, this volume).

My approach here is two-pronged. I begin by briefly revisiting definitional issues (see Conway 2002a, 2002b, 2003a, 2007, 2012; Hardy & Williams, this volume; Jarvis, Nouri & Whiting, this volume). This is necessary, because any 'reality check' on cyberterrorism – such as that offered in this chapter - requires a reminder that terrorism is not merely 'something big', hence cyberterrorism may not be defined as 'something big in cyberspace.' Having underlined the importance of the 'terrorism' in cyberterrorism, the greater part of the chapter is taken-up with a comparison of cyberterrorism with car bombing that again privileges a terrorism over a technology approach. This is a useful comparison, it is posited, because those hyping the cyberterrorism threat have a tendency to equate opportunity with outcome rather than reflecting upon whether something that *could* happen is in fact *likely* given the potential perpetrators' motives, capabilities, and ends.

Underlining the 'Terrorism' in Cyberterrorism

It is today commonplace when dealing with computers and the Internet to create new words by placing the handle 'cyber,' 'electronic,' or 'information'—often shortened to simply 'e' or 'i'—before another word. This may appear to denote a completely new phenomenon, but often it does not and confusion ensues. Cyberterrorism is the convergence of cyberspace and terrorism. Not the convergence of cyberspace and 'something big' or even the convergence of cyberspace and 'something bad'—although, as will be illustrated below, a cyber-attack would probably need to be both 'big' and 'bad' to be properly deemed cyberterrorism. But the convergence of cyberspace and *terrorism*, the latter of which is something, albeit subject to a high level of definitional contestation, that has a long history and a basic outline shape. First, in order for an attack to be classified as terrorism, it must have a political motive; that an attack is carried out via the Internet does not make this requirement any less necessary. To fail to recognise the importance of motive is to seriously mischaracterize what it is that constitutes terrorism. The second necessary requirement for traditional or 'real world' terrorism is violence or the threat of violence. The problem that arises here is that although 'real world' political violence—and violence more generally—is very heavily studied, virtual 'violence' is a relatively new phenomenon and thus under-researched. It is clear enough that the destruction of another's computer with a hammer is a violent act, but should destruction of the data contained in that machine, whether by the introduction of a virus or some other technological means, also be considered 'violence'? (Gordon & Ford 2002, 640). And even if destruction of data or systems meets the 'violence' threshold, can disruption do likewise? Two well-known definitions of cyberterrorism are compared below with respect to their treatment of motive, violence, and a number of other points germane to the follow-up comparison between cyberterrorism and Vehicle-Borne Improvised Explosive Devices (VBIED) attacks.

The US Naval Postgraduate School's Professor Dorothy Denning's definitions of cyberterrorism are probably the most well-known and respected. Denning's (2007: 124) most recent definition of cyberterrorism is as follows:

> highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property.

Denning (2007: 125) goes on to say that:

> To fall in the domain of cyberterror, a cyber attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism, and it must be conducted for political

> and social reasons. Critical infrastructures…are likely targets. Attacks against these infrastructures that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or billion dollar banking losses would be examples.

Another well-known definition was proposed by Mark M. Pollitt in his article 'Cyberterrorism: Fact or Fancy?' (1998) in which he unified a definition of cyberspace with a well-known definition of terrorism. For Pollitt, cyberspace may be conceived of as "that place in which computer programs function and data moves." He employed the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d): "The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience." Pollitt arrived at the following definition of cyberterrorism by combining these two: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Pollitt 1998, 9).

Denning's and Pollitt's definitions share similarities, but also significant differences. A crucial point on which Denning and Pollitt are in agreement is that an act may not be classified as cyberterrorism absent a (socio-)political motive. Even very large scale attacks carried out for purposes of, say, self-enrichment, one-upmanship, or similar are thus excluded. With regards to the impacts of a cyberterrorist attack however, Denning's definition appears wider than Pollitt's as she explicitly distinguishes between traditional terrorism's physical violence against persons and property as opposed to cyberterrorism's "acts of destruction and disruption against digital property." Pollitt, on the other hand, refers fairly unambiguously to activity that "results in violence" against persons (see also Schmitt 2013, 123; Hardy & Williams, this volume). Both definitions nevertheless prohibit classification of everyday terrorist uses of the Net (e.g. for social networking, radicalisation, researching and planning, financing, and other purposes) as cyberterrorism as these are not in themselves either directly violent or massively disruptive or destructive. Both definitions also rule out (distributed) denial of service ((D)DoS) attacks and similar. An additional issue covered by both definitions are the wider intimidatory or coercive purposes of terrorism and thence also cyberterrorism. An interesting case in this respect is recent revelations, contained in previously classified intelligence reports, of al-Qaeda's interest in hacking into and disabling US drones' satellite links and remote controls (Whitlock & Gellman 2013). If successful, this would not in itself be terrorism however, in the same way as IRA bombings were counted as terrorist acts, but IRA bank robberies were largely not. This is because the former had a terror-inducing and thus directly coercive purpose, but the latter were largely a funding mechanism. For interference with a drone to be classified as an act of cyberterrorism under either of the two definitions under discussion here, I suggest, al-Qaeda operatives would need to hack into and take control of a drone and then successfully re-route and re-aim it to cause civilian fatalities.

The fourth pertinent issue worth drawing attention to in regard to definition is Denning's requirement that for an attack to be labelled cyberterrorism it should be undertaken by 'non-state actors'. This contrasts with Pollitt's approach that mentions 'clandestine agents', in addition to 'sub-national groups'. If the 2010 Stuxnet attack on Iran's Natanz nuclear facility was a joint operation by the United States and Israel (Denning 2012), then it might be conceived as cyberterrorism on Pollitt's definition. It is, however, ruled out as such by Denning's, and the same may be said for the 2007 cyber attacks on Estonia (Rid 2013, 6-7). Both the Estonia attacks and Stuxnet were nevertheless described in the press and elsewhere—including by the Estonian government—as instances of cyberterrorism (see, for example, Agence France Presse 2007; Baltic News Service 2007; Finch 2007; Lloyds 2014). The fifth and final definitional issue I want to address is Denning's and Pollitt's differing

perspectives on the role of cyberspace in cyberterrorism. Denning is clear in her definition that cyberterrorism must use cyberspace as the method of attack and not just its target. This clearly distinguishes her approach from Pollitt's as the latter's definition would appear to include, for example, a car bomb attack on an Internet hub while Denning's emphatically does not (see also Macdonald et al. 2013, 9). This distinction is, I suggest, as important in respect of the cyber component of the definition of cyberterrorism as the motive and violence issues are to the terrorism component of same. In fact, Pollitt's definition would appear to allow for the label of cyberterrorism to be retrospectively applied to a whole range of attacks, including bomb attacks on electricity sub-stations, telephone exchanges, etc., undertaken decades prior to the invention of the term. This is the main reason why Denning's definition is preferred over Pollitt's in this chapter.

It should be clear at this stage that carefully categorising cyber attacks using a well-thought-out definition excludes a great many types of activity typically held-up by journalists, policymakers, and others as cyberterrorism from being conceived as such. Journalists, for example, regularly mix mention of cyberterrorism with terrorist 'use' of the Internet, hacktivism (i.e. activist hacking), hacking, and even cyberwar, as if these activities are all on a par with each other or even indistinguishable. Newspaper headlines such as 'Cyber Terror is the New Language of War' (Dorgan 2013), 'Cyber Spies Terror War; MoD and Treasury Targeted' (Riley 2011), and 'Terrorists "Gaining Upper Hand in Cyber War"' (The Independent 2010) are prevalent. Taking the terrorism components of cyberterrorism seriously rather than myopically focusing on its cyber aspects provides considerable clarification. Application of Denning's criteria having eliminated everything from website defacements to Stuxnet from the domain of cyberterrorism, there is nonetheless a range of cyber activities that, were they to have a political motive and a message-generation component and that resulted in massive disruption or violence, could—would?—be termed cyberterrorism. So why haven't we yet seen any such attacks?

The position adopted in this chapter is that there are a number of factors that distinguish cyberterrorism from 'real world' terrorism that cause cyberterrorism to remain an outside threat. Cyber-based activities, it will be argued herein, don't tend to work as terrorism, and the domination of debate in this area by 'The IT Crowd' (Singer & Friedman 2014)—rather than, if you like, 'The Terrorism Studies Crowd'—has skewed assessment of risk. From a terrorism perspective, the costs largely outweigh the significantly less than assured destructive capacities and publicity benefits likely to accrue to a cyberterrorist attack (compare with Wilson, this volume). This chapter concentrates on four major factors that weigh against the likelihood of cyberterrorism occurring: (i) cost factor; (ii) complexity factor; (iii) destruction factor; and (iv) media impact factor. Denning has observed that "For a politically-motivated cyber-attack to be considered an act of cyber-terror, it would have to be serious enough to actually incite terror on a par with violent, physical acts of terrorism such as bombings" (Denning 2012, 678). Each of these factors will therefore be considered not just in respect of cyberterrorism, but also in respect of 'Vehicle-Borne Improvised Explosive Devices' (VBIEDs) or, in common parlance, 'car bombs.' No act of cyberterrorism has ever yet occurred, car bombing, on the other hand, has a long and bloody globe-spanning history and continues to prove a spectacularly attractive terrorist option (Davis 2008). Following a detailed weighing-up of the pros and cons of cyber-attack versus car bombing the conclusion arrived at is that traditional low-tech 'real world' terrorist attacks will continue to be more effective and therefore 'attractive' than their cyber variant for some time to come.

Cyberterrorism Versus VBIED Attacks

This section compares instances of car bombing with non-instances of cyberterrorism. This has some difficulties as an approach, as one might imagine. It is rather difficult to compare things that have an actual existence and can therefore be described, counted, costed, etc. and those that do not. The seeming implausibility of such an undertaking notwithstanding, the insistence of journalists, policymakers, IT security professionals, and others that catastrophic cyberterrorism is imminent requires analysis and counter-argument. Those involved in the cyberterrorism debate cannot draw on either history or experience to bolster their positions, as a major cyberterrorist incident has never yet occurred. For this reason, different scenarios or stories about the possible course of future events are providing the grounds on which decisions must be made. The upshot of this is that a multitude of actors with their various, and often divergent, interests are competing with each other by means of their versions of the future, which are particularly subject to political exploitation and instrumentation (Deibert 2002, 118). Cyberterrorism has thus taken on a rather grandiose 'sci-fi' character. The comparison below is therefore by way of a reality check in which some of those potential attacks that would fit Denning's definition of cyberterrorism are compared with a form of terrorism that is so contemporarily 'doable' that in some countries and regions it has come to be mundane or commonplace: VBIED attacks.

'Vehicle-Borne Improvised Explosive Device' (VBIED) is the term used to describe a 'home-made' as opposed to off-the-shelf explosive device housed and delivered in a vehicle. The most common type of VBIED is a car bomb (see, for example, Table 6.1), but a range of other vehicles from bicycles to boats have been employed. Some analysts even consider the planes on 9/11 as VBIEDs, albeit these were not carrying explosives additional to their fuel. Car bombs are remarkably effective weapons as they offer a highly innocuous way to transport large amounts of explosives and/or flammable material to a target while the content of the vehicle's fuel tank lends the blast additional power and the body of the vehicle itself produces copious shrapnel. In recent years, suicide VBIEDs have been used extensively, including in Iraq (see Table 6.1), Afghanistan, and elsewhere. Other countries or conflicts in which VBIEDs have been widely deployed include Colombia, India, Israel, Lebanon, Northern Ireland, Pakistan, Russia, and Sri Lanka. VBIED attacks have been chosen for comparison with cyberterrorism in this chapter precisely because of their long history, wide geographical spread, and contemporary ubiquity, but also because this form of attack is neither the easiest nor the most complex type of terrorism. It is not the cheapest or the most expensive. It is neither the flashiest nor the most attention-getting. It might be described as mid-range terrorism and thus an appropriate comparator.

The four factors with respect to which VBIED attacks and cyberterrorism are compared below are those that have been evidenced by experience to matter, to varying extents, to almost all terrorists. Put another way, these are the factors, it is suggested, that would be taken into account by terrorists in the early stages of planning an attack and evaluating the desirability of cyber versus more traditional methods. In terms of the comparison, some of the arguments may strike the reader as more convincing than others; I'm less interested however in the merits of each comparison taken separately than in the compelling nature of considering them in tandem.

Cost Factor

Even though exact figures are difficult to obtain, one thing is clear, car bomb construction is cheap. The first World Trade Centre attack in 1993 killed six people and injured more than a thousand; the truck bomb is estimated to have cost $400 to construct (Giacomello 2004, 397). In April 1995, the Oklahoma City bombing, which prior to 9/11 was the largest terrorist attack on US soil in history, killed 168 people. It is estimated to have cost less than

US$5,000, which was outlaid for fertiliser, fuel, and van rental fees (Michel & Herbeck 2001, 176). The 9/11 attacks—although not strictly VBIED attacks—were also relatively cheap to carry out; the *9/11 Commission Report* estimated that it cost just $400,000 - $500,000 in total financing over nearly two years, including living expenses for and other payments to the nineteen hijackers (2004, p.172; see also Wilson, this volume). VBIED attacks are commonplace in on-going conflicts, such as in Iraq and Afghanistan. The US Department of Defense's Joint Improvised Explosive Device Defeat Organisation (JIEDDO) estimated that the average cost to construct a car bomb in Afghanistan in 2006—the most recent year for which such information is (publicly?) available—was just $1,675 (Ackerman 2011).

If the exact cost of VBIED construction is difficult to estimate due to the diversity of components used, significant cost disparities depending on where the vehicle and/or other components are purchased, and so forth, the challenge of estimating the cost of a potential cyberterrorism attack is exponentially greater. Giampiero Giacomello nevertheless engaged in a speculative analysis that addressed precisely this issue in 2004. In his 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism,' Giacomello considered the cost of two common cyberterrorism scenarios: a cyber attack on a hydroelectric dam and a cyber attack on air traffic control systems. He estimated the cost of the dam attack at $1.2 – 1.3 million with potential fatalities of between 50 – 100 and the cost of the air traffic attack at $2.5 – 3 million with the potential for 250 – 500 casualties (Giacomello 2004, 397-398). The dam attack, he pointed out, "would look like an attractive investment, if it were not the case that a suicide bomber would cause roughly the same amount of casualties at a fraction of that cost" (Giacomello 2004, 397). Now consider that according to the author of the definitive analysis of Stuxnet, testing for that attack, "must have involved a fully-functional mock-up [uranium enrichment test bed] operating with real uranium hexafluoride" (Langner 2013, 20). This puts the cost of just a portion of that attack at (conservatively) tens of millions of dollars. As such, there is every appearance therefore that Giacomello got it right when he concluded that on the basis of financial considerations alone "cyberterrorism would be a highly inefficient solution for terrorists, due to high costs and meagre returns" (2004, 388).

Complexity Factor

VBIEDs are relatively simple to build and deliver. Bicycles, scooters, motorcycles, cars, vans, mini-buses, trucks, and tankers are everywhere. Many people own small vehicles and so are already in possession of an important component of the finished device; larger vehicles can be bought, rented, or stolen. In terms of a delivery mechanism, VBIEDs are highly innocuous and therefore difficult to guard against. Fertiliser is the other major component of many VBIEDs. Large amounts of it can still be purchased easily (and relatively cheaply) due to its wide legitimate use in agriculture, despite governments' efforts to place curbs on sales of large amounts due to its explosive capacities. A great many groups and individuals have the necessary expertise to themselves construct and/or to educate others how to construct VBIEDs. These include members or former members of terrorist organisations, such as Hamas, Hizbollah, the Liberation Tigers of Tamil Eelam (LTTE), and the Provisional IRA, and increasing numbers of violent jihadi bomb-makers active in Afghanistan, Iraq, and elsewhere. Individuals with no known links to any terrorist organisation have also demonstrated the capacity for VBIED-construction; these include Timothy McVeigh and Terry Nichols, the perpetrators of the Oklahoma City bombing, and Anders Breivik, who deployed a VBIED against government offices in Oslo, Norway on 22 July, 2011 that killed 8 people and injured over 200.

There has been heightened concern amongst policymakers, law enforcement agencies, and others since the 9/11 attacks regarding the proliferation of "how to" information online devoted to explaining, amongst other things, the technical intricacies of making VBIEDs. In

fact, as early as 1997, the US Department of Justice had concluded that the availability of bomb-making information played a significant role in facilitating terrorist and other criminal acts (pp.'s 15 – 16). Today, there is easy online access to various types of forums and content containing bomb-making information. The level of threat posed by this remains a source of debate with some commentators insisting that legislation must be put in place to outlaw such online content, and others pointing out both that this material is already easily accessible in bookstores and libraries (Leonard 2013) and also that much of the information is unreliable or simply wrong (Kenney 2010). Sophisticated terrorist organizations do not need to rely on the Internet for developing their bomb-making skills, but disaffected individuals prepared to use terrorist tactics to advance their politics, of whatever stripe, appear to have increasing recourse to online content. While Faisal Shazad, the failed Times Square car-bomber, is said to have travelled to acquire his bomb-making skills in Pakistan where he received three to five days of training (Hoffman 2010), Anders Breivik produced a new type of fertiliser bomb through combining knowledge from different recipes he located on the Internet (Aasland Ravndal 2012, 17). The main point here is that rudimentary bomb-making skills can be easily and quickly obtained in a number of different ways. On the other hand, the failed Times Square attack, along with the failed car bomb attacks planned and carried out by medical doctors in central London and at Glasgow airport in June 2007, shows that even relatively unsophisticated real-world attacks have a level of difficulty and are routinely unsuccessful. Cyberterrorism can be expected to have an exponentially greater margin of difficulty.

In a March 2010 speech, then FBI Director (2001 – 2013) Robert Mueller observed "Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyber attacks." That may very well be true, but 'wanting' to do something is quite different from having the ability to do the same. Violent jihadis' IT knowledge is not superior to the ordinary publics. Research found that of a random sampling of 404 members of violent Islamist groups, 196 (48.5%) had a higher education, with information about subject areas available for 178 individuals. Of these 178, some 8 (4.5%) had trained in computing, which means that out of the entire sample, less than 2% of the jihadis came from a computing background (Gambetta & Hertog 2007, 8 – 12) And not even these few could be assumed to have mastery of the complex systems necessary to carry out a successful cyberterrorist attack. Journalists therefore need to stop elevating so-called 'script-kiddies' to potential cyberterrorists and insinuating that just because some group has the capacity to establish a website, distribute content online, and/or engage in DDoS attacks the next step is a major attack by them using the Internet. This threat framing has taken on renewed salience in the wake of recent 'attacks' by the al-Qassam Cyber Fighters and the Syrian Electronic Army, which have been repeatedly characterised as cyberterrorism.

Many people respond to the above arguments by saying that if one doesn't have the requisite know-how in-house, an alternative option is to hire "outsiders" to undertake a cyberterrorism attack on one's behalf. This would force the terrorists to operate outside their own trusted circles and thus leave them ripe for infiltration however. Moreover, even if contact with "real" hackers was successful, the terrorist group would be in no position to gauge their competency accurately; they would simply have to rely on trust. This would be very personally and operationally risky (Conway 2003b, 10 – 12). Turning to the possibility of online crowd sourcing as a response to these types of challenges then; if proxies could be employed to actually commit acts of cyberterrorism, terrorists would improve their ability to avoid culpability or blame altogether. The problem with this is two-fold: first, it would require gathering a 'crowd' which would, in turn, require fairly wide dissemination of information about the activity to be undertaken thus opening-up the very real possibility of the attack plans coming to the attention of the authorities. Second, the terrorists would lose

control over when, where, how, or even *if* the attack took place. This might be advantageous in terms of instigating low-level 'real world' (e.g. jihadi-inspired lone actor terrorism) and cyber operations (e.g. (D)DoS attacks), but is not a suitable method for undertaking a major cyberterrorism operation. Furthermore, while the potential anonymity provided by crowd sourcing might protect the instigators from being detected, it would also lose them their credit for the attack. On the basis of technical knowhow alone, then, cyberterrorism is not feasible.

Destruction Factor

Stuxnet is the only cyber attack to date that is agreed to have caused actual physical destruction. This, moreover, was to a system and not to human beings. VBIEDs, on the other hand, have a long and very widely proven history of destruction of lives and property. "Trucks and vans can easily deliver the explosive equivalent of the bomb load of a B-24 (the workhorse heavy bomber of the Army Air Forces in World War Two) to the door step of a prime target. Even the average family SUV with 10 cubic feet of cargo space can transport a 1000-pound bomb" (Davis 2008, 8). Indeed, some authors go so far as to portray the September 11 attacks as simply a scaled-up version of the 1993 van-bombing of the World Trade Centre. Basically, the entire range of ground transportation options is available for attacks based on the same fundamental principles. The destruction to lives and property that can be wrought by such devices is, unsurprisingly, potentially massive.

One of the deadliest such attacks was carried out by radical Islamists in closely-timed suicide truck bomb attacks on the US Marine barracks and French members of the Multinational Force in Lebanon on 23 October 1983 in Beirut. The combined death toll from the attacks was 305. The already-mentioned Oklahoma City Bombing killed 168 people, including 19 children and three pregnant women, injuring nearly 700 others. The "single worst terrorist incident" of the Northern 'Troubles' took place on 15 August, 1998 in the town of Omagh in County Tyrone (Police Ombudsman for Northern Ireland 2001, 1). On that Saturday afternoon, the Real IRA—a dissident offshoot of the Provisional Irish Republican Army—parked and subsequently detonated a car filled with 500 lbs of fertiliser-based explosive in the town, killing 29 people, including a woman pregnant with twins, and injuring some 250 others. The Northern Ireland conflict was characterised by a long string of car bombings that began in Belfast in 1972, but that has since been eclipsed by the alacrity with which the VBIED has been deployed in the Iraq conflict. It is estimated that some 664 *suicide* VBIED attacks alone took place in Iraq between March 2003 and December 2010 (see Table 6.1). Nine separate car bombs exploded in Baghdad on a single Sunday in October 2013. The blasts, which hit eight different Shiite-majority areas in and around the Iraqi capital, killed at least 54 people and wounded more than 90. The pan-Arab news channel Al-Arabiya reported that at the time of the blasts the Iraqi government had actually restricted many Baghdad residents from using their cars in an attempt to thwart car bombings (Al-Arabiya 2013).

The 'worst' terrorist attacks are generally conceived as those that have the highest number of fatalities and injuries associated with them. The destruction of human lives is not the only type of destruction associated with VBIED attacks however, many of which also cause enormous property damage. In addition to the fatalities associated with it, the Oklahoma City bombing blew the front from the targeted Alfred P. Murrah building and "caused major damage to adjacent structures, touched off car fires, and blew out glass windows and doors in a three-square-mile area on the north side of downtown Oklahoma City" (Oklahoma City Police Dept. 1995, 1). While the Omagh bomb killed the greatest number of people in a single terrorist attack in Northern Ireland, the property destruction associated with it was minimal compared to that wrought by the Provisional IRA's 1992 to 1996 mainland bombing campaign. Total combined property damage arising from the 1991

Table 6.1 Documented Civilian Casualties from Suicide VBIEDs in Iraq, 20 March 2003 – 31 Dec. 2010

	Suicide bike or scooter bomb	**Suicide car bomb**	**Suicide truck or minibus bomb**	**Suicide fuel tanker bomb**	**Total Suicide VBIED***
Events (n[%])	15 (2%)	532 (53%)	49 (5%)	6 (1%)	664 (66%)
Civilian deaths (n[%])	194 (2%)	4358 (36%)	906 (7%)	625 (5%)	7072 (58%)
Civilian injuries (n[%])	442 (1%)	12224 (40%)	2967 (10%)	1690 (6%)	19989 (65%)
Civilian casualties (n[%])	636 (1%)	16582 (39%)	3873 (9%)	2315 (5%)	27061 (63%)
Injured-to-killed ratio	2:3	2:8	3:3	2:7	2:8
Mortality in victims (%)	31%	26%	23%	27%	26%

**Results do not total across suicide bomb subtypes for two reasons because not ot all suicide VBIEDs were described in adequate detail to identify vehicle sub-type.*

Adapted from Table 1 (p.907) in Hsiao-Rei Hicks et al. (2011).

Baltic Exchange truck bomb, 1992 Bishopsgate Road dump truck bomb, 1996 Canary Wharf car bomb, and 1996 Arndale Centre van bomb was estimated to exceed $5 billion (Davis 2008, 133 – 137). Anders Behring Breivik's 2011 car-bombing of the government quarter in Oslo severely damaged the building in which the Prime Minister's office was housed and surrounding buildings. Discussion is on-going in Norway at time of writing as to whether the four most badly damaged buildings (i.e. H-block, Y-block, R4, and S) should be preserved and refurbished or demolished and replaced. The cost of preserving and refurbishing H-block and Y-block alone has been estimated at over $100 million (Sandelson & Smith 2013).

Giacomello's 'Bangs for the Buck' article considered not just the cost in terms of preparation for a cyber attack and lives lost, but also the cost of a "Cyber attack on computer systems regulating regional electric power, combined with physical attacks on transmission and distribution network." The potential outcome of the latter were described as "Regional electricity shortages that persist for a week; health risks from heat/cold; interruption of production schedules; destruction of physical capital" (Giacomello 2004, 399) with an estimated total potential cost of $25 billion. A combined physical and cyber attack as just described, it should be noted, would be greatly more complex to successfully carry out than either a standalone cyber attack or a standalone physical attack. Furthermore, the same article contains an estimate for potential costs associated with "Widespread terror against key elements of public economy across nations (malls, restaurants, movie theatres, etc.)" at fully ten times that of the complex combined physical and cyber attack. It is speculated in the article that "widespread terror" of the sort just described would result in a significant and sustained decline in economic activity in public spaces and an associated drop in consumer confidence that could have potential costs of $250 billion (2004, 399). Indeed such "widespread terror" has already been generated in many countries by the use of relatively cheap VBIEDs, while also having devastating impacts on lives and property and inflicting, in addition, huge financial costs on governments, insurers, and others, as illustrated herein. An additional important point made by Giacomello and germane to this analysis is with respect to the electricity blackout that afflicted the north eastern United States and eastern Canada on 14 August 2003:

> If, one the one hand, it proved that the North American power grid could be compromised with vast repercussions, on the other, it showed that, contrary to some appearance, modern societies and economies are also more resilient. Although the blackout affected 50 million people, there were very few injuries or fatalities. Most people reacted calmly and hospitals and emergency services continued to function properly (2004, 400).

Granted the above blackout, and those that affected a host of European countries in summer 2003, were relatively short-lived with most lasting for a maximum of one to two days; they are illustrative however of the relative lack of destruction generally arising from lights-out events.

Media Impact Factor

Schmid and De Graaf, characterize terrorism as a form of violent communication. In fact, "without communication," they argue, "there can be no terrorism" (1982, 9). This explains the large literature on the intersection of media and terrorism and the oft-repeated claim that media and terrorists enjoy a symbiotic relationship. In his text, The Anatomy of Terrorism, David Long opined that, "The media's mission to cover the news and the terrorist's ability to "create" news have led to a symbiotic relationship between the two, one in which the media not only convey the news but help the terrorists create it (1990, 119; see also Carruthers 2000, 168; Hoffman 2006, 195). Long goes on to employ the metaphor of theatre to explain terrorism; Mark Juergensmeyer drawing on the same metaphor suggests that we view terrorism not as a tactic but as what he calls "performance violence," which has two major components. First, such acts are dramas designed to have an effect on their audiences. In the case of terrorist violence, those who witness it via the news media are part of what occurs. Second, according to Juergensmeyer, the term "performance" also implies the notion of "performative," which refers to certain kinds of speech that are able to perform social functions (i.e. their utterance has a performative impact).

> Like vows recited during marriage rites, certain words not only represent reality but also shape it: they contain a certain power of their own. The same is true of some nonverbal symbolic actions, such as the gunshot that begins a race, the raising of a white flag to show defeat, or acts of terrorism (2000, 124).

The performative and propagandistic nature of terrorist acts is central to many of the available definitions of terrorism. According to Schmid and De Graaf:

> Terrorism cannot be understood only in terms of violence. It has to be understood primarily in terms of propaganda. Violence and propaganda have much in common. Violence aims at behaviour modification by coercion. Propaganda aims at the same through persuasion. Terrorism is a combination of the two (1982, 14).

The events of 9/11 underscored that moving images are crucial for a truly spectacular terrorist event. The attacks on the World Trade Center were a fantastic piece of performance violence: a lavish visual event. More traditional VBIED attacks are also impactful; they advertise themselves. Not only do they kill and injure those in their vicinity and destroy surrounding buildings, but they are loud: their sound can often be heard for miles. They can generate a percussive wave that can often be felt at long distances. And, in our mobile telephone-saturated world, such attacks increasingly have spectacular live moving images associated with them. This gives rise to a number of associated or sub-factors: VBIED attacks generate live on-the-scene reporting, which makes compelling viewing and thus attracts large audiences; these attacks must be reported, even in authoritarian states; they are not generally apprehended nor can they generally be reported as accidents. The problem with respect to cyberterrorism, from a terrorism perspective, is that many of the hypothesised attack

scenarios, from shutting down the electric power grid to contaminating a major water supply, fail on all of the above accounts. In terms of theatricality, such attacks would likely have no easily captured spectacular (live) moving images associated with them, something we—as an audience—have been primed for by the 9/11 attacks. The only commonly forwarded cyberterrorism scenario that would have this performance value would be interfering with air traffic control systems to crash planes, but hasn't it been shown that planes can be much more easily employed in spectacular 'real world' terrorism? And besides, is it not the case that all of the infrastructures just mentioned and others besides are much easier and more spectacular to simply blow-up?

On a related note, but perhaps even more importantly, a terrorist event that has the possibility of being portrayed as an accident is a failed attack. Consider the observation that:

> Publicity would be also one of the primary objectives for a terrorist attack. Extensive coverage has been given to the vulnerability of the US information infrastructure and to the potential harm that could be caused by a cyberattack. This might lead terrorists to feel that even a marginally successful cyberattack directed at the United States may garner considerable publicity. Some suggest that were such a cyberattack by a terrorist organization to occur *and become known to the general public*, regardless of the level of success of the attack, concern by many citizens may lead to widespread withdrawal of funds and selling of equities [my emphasis] (Rollins & Wilson 2007, 5).

In testimony before a US Senate committee Howard Schmidt, the Obama administration's onetime Cybersecurity Coordinator, made a similar observation: "…during NIMDA and Code Red, we to this day don't know the source of that. It could have very easily been a terrorist…" (US Senate Committee on the Judiciary 2004, 28). These observations betray a fundamental misunderstanding of the nature and purpose(s) of terrorism, particularly its attention-getting function. A terrorist attack with the potential to be hidden, portrayed as an accident, or otherwise remain unknown is unlikely to be viewed positively from a terrorism perspective. One of the most important aspects of the 9/11 attacks in New York from the perpetrators' viewpoint was surely the fact that while the first plane to crash into the WTC could have been accidental, the appearance of the second plane confirmed the incident as a terrorist attack in real time (as, of course, did subsequent events in Washington DC and Pennsylvania). This is a characteristic of all VBIEDs; stationary vehicles do not generally explode absent their containing explosives and being triggered to do so. If one considers that, in addition, many contemporary VBIED attacks are at the same time suicide attacks, it becomes clear that deniability (as suggested in, for example, Collins & McCombie 2012, 89) is not a major concern of many contemporary terrorists nor has it ever been. On the contrary, "[c]oercion requires attribution", which explains why "terrorist spend as much time marketing their exploits as they do fighting, bombing, assassinating, and so on" (Gartzke 2013, 46 – 47).

Conclusion

Stuxnet cannot be classed as an act of cyberterrorism on the basis of either of the definitions of cyberterrorism described in this chapter's opening section. It is, however, connected to the cyberterrorism debate given that it is accepted by many to be the most consequential cyber attack to have yet occurred. It was, by all accounts, an enormously complex attack to get right, involving for its development and deployment an estimated 10,000 person hours of coding by a team or teams of individuals and costing anywhere from millions to tens of millions of US dollars (Halliday 2010; Langner 2013, 20; US Senate 2010; Zetter 2010). In fact, such was the complexity and cost of this undertaking that it is generally agreed that it could not have been carried out by any entity other than a state or states (Langner 2013, 20; see also Gross 2011; Halliday 2010). The damage caused by the Stuxnet worm to the Iranian

nuclear programme is said to have put it back at least two years (Langner 2013, 15) and thus was a major event not only in the cyber realm, but in international affairs more generally.

Now let's consider the Boston Marathon bombing. If the VBIED attacks described throughout this paper were of a mid-range sort of terrorism in terms of their complexity, cost, and destructive outcomes, the Boston Marathon attack was of the lowest-level type of 'real world' terrorism imaginable. At a cost of $100 to $180 each (Bucktin 2013; Wallack & Healy 2013), the two pressure-cooker bombs were considerably less expensive than a VBIED in even Afghanistan. The complexity of both the bombs themselves and the overall attack strategy was low. Given their design, the Tsarnaev brothers may have based the devices construction on instructions contained in al-Qaeda in the Islamic Maghreb's (AQIM) English language magazine *Inspire*, which is freely available on the Internet (Leonard 2013). The cheap financial cost and low level of sophistication of the attack notwithstanding, it cost two young women and a child their lives and 14 others their limbs, and is estimated to have caused upwards of $333 million in property damage, lost sales, medical costs, etc. (see Dedman & Schoen 2013 for breakdown). So while the Stuxnet attack was complex and high-cost, the Boston Marathon attack was easy and low-cost. And while Stuxnet caused disruption and destruction, it caused no direct harm to human beings. The starkest difference between Stuxnet and the Boston Marathon bombings however was their widely differing media impacts. A search of 'All English Language News' on Lexis-Nexis on 20 October 2013 returned 881 items with 'Stuxnet' in the headline, but 2,482 items with 'Boston Marathon Bombing' in the headline. Put another way, a conservative estimate puts the amount of media coverage afforded the Boston Marathon attack at almost triple that of Stuxnet, illustrating once again that it is perfectly possible for cheap and easy attacks to trump their costly and complex counterparts.

It may be true, therefore, that from a technological perspective, "Stuxnet has proved that cyber terrorism is now a credible threat" (Collins & McCombie 2013, 89). Not from a terrorism perspective however. As Dunn-Cavelty (2011) has pointed out, "careful threat assessments…necessarily demand more than just naval-gazing and vulnerability spotting. Rather than simply assuming the worst, the question that must be asked is: Who has the interest and the capability to attack us and why?". Cyberterrorism should not therefore ever be considered in isolation from more traditional forms of terrorism as if its cyber component renders it separate to the latter; thence the focus on careful definition and comparison in this chapter.

In their 2002 paper, Brenner and Goodman pose the question: "Why has cyberterrorism not yet manifested itself? And follow-up with: "This is concededly something of a mystery. There are no reliable answers as to why cyberterrorism remains an as-yet unrealized phenomenon" (Brenner & Goodman 2002, 44). On the contrary, as illustrated in this chapter, there are at least four pretty straightforward and convincing reasons for why no act of cyberterrorism has ever yet occurred. VBIED construction is cheap. Cyberterrorism scenarios vary hugely in their potential size and scope and for this and other reasons are thus hugely difficult to cost; having said this, even the most conservative analyst would probably be forced to agree that no major cyberterrorism attack is likely to cost less than the average price of construction of a VBIED. Cost need not be a determining factor however; the complexity issue is a different matter. VBIED construction is relatively easy. The components are widely available and the know-how accessible via personal connections, bookstores, libraries, and online. The know-how necessary to cause the necessary levels of disruption, destruction, or even violence for a cyber attack to be deemed cyberterrorism is unlikely to be readily available to terrorists and therefore risky to obtain. The potential for destruction of a cyberterrorism attack is difficult to estimate too, but the available evidence suggests that wide disruption or destruction, not to say fatalities, would be costly and difficult

to achieve. Cheap and easy methods, such as VBIED attacks, can be widely destructive however, which accounts for their contemporary ubiquity. Finally, apart from practical matters relating to cost, complexity, and destructive capacity, cyber-based activities are unlikely to work as terrorism precisely for the reasons they are touted in other realms: stealth and deniability; attention-getting and credit-claiming are at the core of terrorism. Arguments such as the latter have been eclipsed by arguments based on modern societies' technological vulnerabilities on the one hand and potential terrorists' capabilities on the other. The capacity to launch a cyberterrorism attack, which is itself challenged herein, bears very little relationship to the actual likelihood of attack however. "Many threats are conceivable, but relatively few actually materialize" (Gartzke 2013, 51). Cyberterrorism is therefore conceivable, but very unlikely. Why? Because 'real world' attacks are cheaper and less complex while also being significantly destructive of lives and property and, importantly, emotionally impactful so therefore also attention-getting to an extent that cyberterrorism will struggle to achieve.

Guide to Further Reading and Resources

Dr. Thomas Rid of King's College London's Department of War Studies explains the concept of cyberterrorism and explores the risks associated with militants conducting attacks through the Internet (7 mins).
http://www.youtube.com/watch?v=cPTPpb8Ldz8

'Squirrel Power!'
This 2013 *New York Times* article is perhaps my favourite shut-down-the-power-grid-scenario detailing as it does the very real threat posed by Kamikaze squirrels!
http://www.nytimes.com/2013/09/01/opinion/sunday/squirrel-power.html?pagewanted=all&_r=0

Video (2Hrs 10Mins) of UK House of Commons Science and Technology Committee hearing on cyber attacks on 17 November, 2010 with contributions from, amongst others, Prof. Ross Anderson, University of Cambridge; Professor Bernard Silverman, Chief Scientific Adviser, UK Home Office; Dr Steve Marsh, Deputy Director, Office of Cyber Security, UK Cabinet Office; Professor Mark Welland, Chief Scientific Adviser, UK Ministry of Defence.
http://www.parliamentlive.tv/Main/Player.aspx?meetingId=7009

Video (2Hrs 11Mins) of UK Public Accounts Committee hearing on cyber security on 13 March, 2013 with contributions from, amongst others, Prof. Sadie Creese, Professor of Cybersecurity, Oxford University; Dr. Thomas Rid, Kings College London; Mark Hughes, Managing Director of Security for British Telecom; Oliver Robbins, Deputy National Security Adviser, UK Cabinet Office.
http://www.bbc.co.uk/democracylive/house-of-commons-21784442

References

Aasland Ravndal, Jacob. 2012. 'A Post-Trial Profile of Anders Behring Breivik.' *CTC Sentinel* 5(10): 16 – 20.

Ackerman, Spencer. 2011. '$265 Bomb, $300 Billion War: The Economics of the 9/11 Era's Signature Weapon.' *Wired* 8 Sept. http://www.wired.com/dangerroom/2011/09/ied-cost/

Agence France Presse. 2007. 'EU Should Class Cyber Attacks as Terrorism: Estonia.' *Agence France Presse* 7 June.

Al-Arabiya. 2013. 'Car Bombs Kill at Least 54 people in Baghdad Area.' *Al-Arabiya* 27 Oct. http://english.alarabiya.net/en/News/middle-east/2013/10/27/Car-bombs-explode-across-Baghdad-killing-at-least-16-people.html

Baltic News Service. 2007. Cyber Terrorism is not Only Estonia's Problem – Russian Senator.' *Baltic News Service* 25 June.

Brenner, Susan W. and Marc D. Goodman. 2002. 'In Defense of Cyberterrorism: An Argument for Anticipating Cyber-attacks.' *University of Illinois Journal of Law, Technology & Policy* No.1: 1 – 58.

Bucktin, Christopher. 2013. 'Boston Bombers on a Budget: "Shoestring" Terrorist Brothers' Bombs Cost Less than £120 to Make.' *The Mirror* (UK) 24 April. http://www.mirror.co.uk/news/world-news/boston-bombers-budget-shoestring-terrorist-1852203

Carter, Shan and Amanda Cox. 2011. 'One 9/11 Tally: $3.3 Trillion.' *The New York Times* 8 Sept. http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html

Collins, Sean and Stephen McCombie. 2012. 'Stuxnet: The Emergence of a New Cyber Weapon and its Implications.' *Journal of Policing, Intelligence and Counter Terrorism* 7(1): 80 – 91.

Conway, Maura. 2002a. 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet.' *First Monday* 7(11).

Conway, Maura. 2002b. Cyberterrorism. *Current History* 101(659): 436 – 444.

Conway, Maura. 2003. 'Cyberterrorism: The Story so Far.' *Journal of Information Warfare* 2(2): 33 – 42.

Conway, Maura. 2003b. 'Hackers as Terrorists? Why it Doesn't Compute.' *Computer Fraud and Security* Iss.12 (Dec.): 1 – 13.

Conway, Maura. 2007. 'Cyberterrorism: Hype and Reality.' In E.L. Armistead (Ed.), *Information Warfare: Separating Hype from Reality*. Washington, DC: Potomac Books.

Conway, Maura. 2012. 'What is Cyberterrorism and How Real is the Threat? A Review of the Academic Literature, 1996 – 2009.' In P. Reich and E. Gelbstein (Ed.s), *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*. Hershey, PA: IGI Global.

Dedman, Bill and John Schoen. 2013. 'Adding up the Financial Costs of the Boston Bombings.' *NBC News* 30 April. http://usnews.nbcnews.com/_news/2013/04/30/17975443-adding-up-the-financial-costs-of-the-boston-bombings?lite

Denning, Dorothy. 2007. 'A View of Cyberterrorism Five Years Later.' In K. Himma, Ed., *Internet Security: Hacking, Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett Publishers.

Denning, Dorothy. 2012. 'Stuxnet: What Has Changed?' *Future Internet* 4(3): 672 – 687.

Dorgan, Byron. 2013. 'Cyber Terror is the New Language of War.' *The Huffington Post* 18 July.

Dunn-Cavelty, Myriam. 2011. 'Cyberwar: A More Realistic Threat Assessment.' International Relations and Security Network (ISN). http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=129764&lng=en

Dunn-Cavelty, Myriam. 'Cyber-Terror: Looming Threat or Phantom Menace? The Framing of the U.S. Cyber-threat Debate.' *Journal of Information Technology and Politics* 4(1): 19 – 36.

Gallagher, Sean. 2013. 'Security Pros Predict "Major" Cyber Terror Attack This Year.' *Ars Technica* 4 Jan. http://arstechnica.com/security/2013/01/security-pros-predict-major-cyberterror-attack-this-year/

Gambetta, Diego and Stefan Hertog. 2007. 'Engineers of Jihad.' Sociology Working Papers, No. 2007–10, Department of Sociology, University of Oxford. http://www.nuff.ox.ac.uk/users/gambetta/Engineers%20of%20Jihad.pdf

Gordon, Sarah and Richard Ford. 2002. 'Cyberterrorism?' *Computers & Security* 21(7): 636 – 647.

Gross, Michael Joseph. 2011. 'Stuxnet Worm: A Declaration of Cyber-War.' *Vanity Fair* April. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

Halliday, Josh. 2010. 'Stuxnet Worm is the "Work of a National Government Agency."' *The Guardian* (UK) 24 Sept. http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

Hsiao-Rei Hicks, Madelyn, Hamit Dardagan, Peter M. Bagnall, Michael Spagat, John A. Sloboda. 2011. 'Casualties in Civilians and Coalition Soldiers from Suicide Bombings in Iraq, 2003 – 10: A Descriptive Study.' *The Lancet* 378(9794): 906 – 14.

Lloyds. 2014. 'Cyberterrorism.' http://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2013/cyber-terrorism

Kenney, Michael. 2010. 'Beyond the Internet: *Mētis*, *Techne*, and the Limitations of Online Artifacts for Islamist Terrorists.' *Terrorism and Political Violence* 22(2).

Langner, Ralph. 2013. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington, VA: The Langner Group. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Leonard, Andrew. 2013. 'Homemade Bombs Made Easier.' *Salon* 26 April. http://www.salon.com/2013/04/26/homemade_bombs_made_easier/

Michel, Lou and Dan Herbeck. 2001. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing*. New York: Harper.

Oklahoma City Police Department. 1995. *Alfred P. Murrah Building After Action Report*. Oklahoma City: Oklahoma City Police Department. http://web.archive.org/web/20070703233435/http://www.terrorisminfo.mipt.org/pdf/okcfr_App_C.pdf

Police Ombudsman for Northern Ireland. 2001. 'Statement by the Police Ombudsman for Northern Ireland on Her Investigation of Matters Relating to the Omagh Bombing on August 15 1998.' Belfast: Police Ombudsman for Northern Ireland. http://www.policeombudsman.org/Publicationsuploads/omaghreport.pdf

Pollitt, Mark. 1998. 'Cyberterrorism: Fact or Fancy?' *Computer Fraud & Security* Iss.2: 8 – 10.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: Hurst & Co.

Riley, Ed. 2011. 'Cyber Spies Terror War; MoD and Treasury Targeted.' *Daily Star* (UK) 13 June.

Rollins, John and Clay Wilson. 2007. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Washington, DC: Congressional Research Service.

Sandelson, Michael and Lyndsey Smith. 2013. 'Oslo Government Headquarters Building Fate Due for New Review.' *The Foreigner* 20 Sept. http://theforeigner.no/pages/news/oslo-government-headquarters-building-fate-due-for-new-review/

Schmitt, Michael N. (Ed.). 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge UK: Cambridge University Press. https://www.ccdcoe.org/249.html

Sengupta, Kim. 2010. 'Terrorists 'Gaining Upper Hand in Cyber War"'. *The Independent* (UK) 6 Feb. http://www.independent.co.uk/news/uk/home-news/terrorists-gaining-upper-hand-in-cyber-war-1890913.html

Singer, Peter. 2012. 'The Cyber Terror Bogeyman.' *Armed Forces Journal* 150(4): 12 – 15.

Singer, Peter and Alan Friedman. 2014. *Cybersecurity and Cyberwar: What Everybody Needs to Know*. Oxford: Oxford University Press.

US Department of Justice. 1997. 'Report on the Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which

Such Dissemination May Be Subject to Regulation Consistent with the First Amendment to the United States Constitution.' Washington, DC: US Department of Justice. http://cryptome.org/abi.htm

US Senate. 2010. 'Securing Critical Infrastructure in the Age of Stuxnet.' Washington, DC: US Senate Committee on Homeland Security and Government Affairs. http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet

Wallack, Todd and Beth Healy. 2013. 'Tsarnaev Brothers Appeared to Have Scant Finances.' *The Boston Globe* 24 April.

Whitlock, Craig and Barton Gellman. 2013. 'U.S. Documents Detail al-Qaeda's Efforts to Fight Back Against Drones.' *The Washington Post* 4 Sept. http://www.washingtonpost.com/world/national-security/us-documents-detail-al-qaedas-efforts-to-fight-back-against-drones/2013/09/03/b83e7654-11c0-11e3-b630-36617ca6640f_story_2.html

Zetter, Kim. 2010. 'Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target.' *Wired* 23 Sept. http://www.wired.com/threatlevel/2010/09/stuxnet/