Chapter 2
Understanding, Locating and Constructing Cyberterrorism

Lee Jarvis, Lella Nouri, and Andrew Whiting

2.1 Introduction

As the Internet and associated digital technologies continue their expansion throughout social life, the 'cyber' prefix has become applied to a growing list of diverse activities and phenomena. This encroachment into new spheres of social and political existence has cemented the Internet's place as the poster child of globalisation: a lubricant facilitating the exchange of ideas, information and things. Yet, this capacity to shrink social space and accelerate social time has also generated anxieties around the emergence of seemingly new 'cyber-threats' made manifest by opportunities presented by the Internet. Although much discussed, feared and predicted, such threats remain often poorly or variably understood (see McGuire 2014). None more so, perhaps, than cyberterrorism. Indeed, although this term has existed for over 30 years now, there remains very little consensus on many of the most fundamental questions surrounding this term (Jarvis and Macdonald forthcoming). Thus, what cyberterrorism is—and what it is not—remains enormously contested, as does its relation to other types of terrorism and cyber-activity.

As we demonstrate throughout this chapter, there exists a number of very different understandings of cyberterrorism within academic and other literature on this concept. Several authors, for instance, prefer a graduated approach, distinguishing between 'pure' and other types of cyberterrorism. In these cases, the former is often used most sparingly to refer only to attacks on digital targets via digital means, while the latter, in contrast, may incorporate activities such as propagandizing or fundraising online (Malcolm 2004; also Anderson 2009). Desouza and Hensgen (2003:387),

L. Jarvis (✉)
School of Political, Social and International Studies,
University of East Anglia, Norwich, UK
e-mail: l.jarvis@uea.ac.uk

L. Nouri • A. Whiting
Department of Political and Cultural Studies, Swansea University,
Singleton Park, Swansea SA2 8PP, UK

T.M. Chen et al. (eds.), *Cyberterrorism: Understanding, Assessment, and Response*,
DOI 10.1007/978-1-4939-0962-9_2, © Springer Science+Business Media New York 2014

for example, employ the term ‘unique’ cyberterrorism to describe, “…the use of legitimate electronic outlets to facilitate communication among terrorist groups” (Desouza and Hensgen 2003:387). Other authors apply far stricter criteria, questioning whether even seemingly significant disruptions to computer networks might be considered terrorism at all. Here, Soo Hoo et al. (1997:147), for example, ask whether, ‘…network attacks like shutting down a long-distance telephone network or a company’s internal network [might] be considered terrorism?’ For, as they continue, ‘No violence is used; no life-threatening terror is instilled’ (Soo Hoo et al. 1997:147).

That such a familiar term can sustain such different meanings, we argue, raises a number of important questions. Are some understandings of cyberterrorism more accurate or more useful than others, for example (and, if so, why)? Or, are different conceptions of the term a product of the differing motivations and contexts in which it is used? Does the meaning of cyberterrorism change over time? And, do the geographical and jurisdictional differences identified by Hardy and Williams (2014) matter? Finally, are the consequences of using the term cyberterrorism as important as any meaning it might have?

To explore these questions, the chapter begins by identifying four reasons for the contestability of the term cyberterrorism. These concern: (i) Competing views of the significance of different stages of an attack’s preparation, conduct, and consequences for its categorisation; (ii) A debate over whether or not physical—offline—damage is a necessary feature of cyberterrorism; (iii) A lack of clarity around cyber terminology more broadly; and (iv) Collective fears of that which is ill-understood or seemingly uncontrollable: fears that are stimulated, at times, by media hyperbole. The chapter’s second section then locates cyberterrorism within a wider history of terrorist violence, asking whether and how cyber-activities might be located therein. While recognising terrorism’s evolving character and notoriously contestable meaning, we argue that cyber-activities of any sort rarely meet the criteria that many would see as necessary for an act to be considered terrorism. The chapter’s final section then considers three ways in which this tension might be addressed. These are, first, simply to abandon the concept of cyberterrorism as a misnomer or an inappropriate stretching of the language of terrorism. Second, to engage in further definitional work in order to better clarify the types of activity to which the label cyberterrorism might refer. And, third—our preferred route—to eschew the question of definition altogether and explore cyberterrorism as a social construction rather than a coherent and stable ontological phenomenon. In doing this, we reflect on the importance of debates around definition within this context and beyond, and sketch a diversity of potential research areas for future work in this field.

Key Points

- As the Internet’s centrality to social life continues to grow, the ‘cyber’ prefix has been applied to a growing list of activities and entities.
- Despite its prominence, the term cyberterrorism remains a fundamentally contested one.
- This contestability is a product, in part, of different approaches to the concept’s flexibility.

2.2 Defining Cyberterrorism

Although coined in the 1980s (Collin 1997), it was not until a decade later that the concept cyberterrorism really came to prominence. That it did so at this time, in particular, may be linked to two key dynamics. The first, as Bendrath et al. (2007:58) note, was the movement toward a post-Cold War world in which previously stable security imaginaries and assumptions were undergoing dramatic challenges, and rapid, radical, change. A host of seemingly known and predictable threats seemed to disappear with the collapse of the Soviet Union, resulting in the attention of security professionals turning to 'new' types of risk. This presented space for a greater consideration of cybersecurity threats such as cyber-warfare, cyber-espionage, cybercrime, and, of course, cyberterrorism (Stohl 2014). Second, and just as importantly, this period also witnessed the spread of the Internet and the interconnectivity it made possible: national and international, public and private (Harknett 2003:18). This growing sense of interdependence established new fears amongst security experts and political elites, leading some famously to conclude that, "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Academy of Sciences 1991:7).

In the years that have now passed since this earliest interest, the term cyberterrorism has become ever more widely recognised and used. One study from November 2012, for example, estimated that 31,300 magazine and journal articles have now been written on the subject (Singer 2012). This prominence, however, has not translated into anything like consensus on what cyberterrorism means, or how it should be used (something it shares, of course, with the wider concept of terrorism, discussed further below). Thus, some authors, such as Dorothy Denning, are reluctant to identify specific examples of 'cyberterrorism' in their work, preferring to identify, 'damaging acts in support of terrorist objectives' (2010:201–205). Others, instead, argue that identifiable cases of cyberterrorism do indeed exist, and are even willing to include politically motivated website defacement under this term's remit (Olmstead and Siraj 2009:16–17). In the following, we sketch four important reasons for these disagreements. These, we argue, help explain how this term can be applied to activities as diverse as Critical Information Infrastructure disruption, on the one hand, and 'cyber graffiti', on the other (Kostopoulos 2008:165).

The first, and perhaps the most important, reason for the term's contestability is a temporal one. If we divide the perpetration of a terrorist attack into three broadly discrete stages—preparation, conduct, and consequences—it is possible to see how the digital world might be present in any of these. Preparation, for instance, might include target surveillance over the Internet through web mapping programmes such as Google Maps. The conduct of an attack might involve the release of a computer virus, or a Distributed Denial of Service (DDoS) attack that prevents certain websites from functioning. The consequences of an attack, finally, might include permanent damage to digital technologies or data, and so on. Given the myriad ways in which the digital world might be present in an attack, the question becomes which—and how many—of these engagements are necessary to designate such an event 'cyberterrorism'.

One response, and a common one in the academic literature, is to reserve the term for attacks conducted through—and perhaps targeted against—cyber-technologies. Dorothy Denning's (2000) much-cited testimony to the Special Oversight Panel on Terrorism of the US House of Representatives' Committee on Armed Services, for instance, pursued this approach. Here, she positioned cyberterrorism as a product of, 'the convergence of terrorism and cyberspace', arguing:

> It is generally understood to mean unlawful attacks and threats of attack *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 (emphasis added).

Defining cyberterrorism in this way leads to a comparatively narrow understanding of this term in which the *target* (or consequences) of an attack differentiate this type of politically motivated activity from others. This approach contrasts markedly with Gordon and Ford's (2003:4) discussion of Denning's testimony in a Symantec White Paper, in which they argue:

> we believe that the true impact of her opening statement ("the convergence of terrorism and cyberspace") is realized 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.

Although they identify some of the problems associated with excessively broad uses of this term, the understanding developed by Gordon and Ford clearly allows for a much wider spectrum of actions to be discussed as cyberterrorism than does Denning's original account. Indeed, pursuing this broader reading of Denning's formulation, Gordon and Ford (2003:4) are willing to consider understandings of this concept that are sufficiently expansive to incorporate even the online purchase of aircraft tickets for the execution of the September 11th attacks.

The differences between these comparatively narrow and broad approaches to cyberterrorism is reflective of current academic debate in this area. On the one hand, there are authors such as Maura Conway (2002) who wish to distinguish between "terrorist use of computers as a facilitator of their activities" and, "terrorism involving computer technology as a weapon or target" (also Conway 2014). On the other hand are those such as Devost et al. (1997:78) who posit a continuum between terrorism, information terrorism, and pure information terrorism. For these authors, if the target and tools of an attack are 'physical' entities, then the attack is an example of 'traditional terrorism' (Devost et al. 1997:78). However, if either the tools or the target of an attack can be considered 'digital'—London's square mile is offered as an example of a digital target; a hacker conducting a spoofing attack is presented as an example of a digital tool—then the attack is an example of 'information terrorism'. Furthermore, they argue that when target *and* tool are both digital (the example of a Trojan horse in a public switched network is provided) then an attack should be considered 'pure information terrorism' (Devost et al. 1997:78).

If the importance of different stages of an attack's life cycle offers one source of disagreement around the concept cyberterrorism, a second involves the issue of an attack's destructiveness. While many authors reserve the cyberterrorism label for behaviours leading to destruction or damage (physical or otherwise), others, such as Devost et al. (1997:78) are willing to soften this condition. As they argue:

> 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.

A similar flexibility is evident within Kostopoulos' (2008:165) differentiation between three 'basic types of cyberterrorists': the professionals who 'aim at inflicting physical or cyber damage onto victim's resources', the amateurs who 'find pleasure in applying cyber graffiti' and the thieves who 'have immediate personal illicit economic benefit from their actions'. Kostopoulos' emphasis here upon the perpetrator's type and motive thus broadens cyberterrorism to include an array of different behaviours spanning nuisances through to direct attacks. Thus, while a number of scholars argue that, 'violence against persons or severe economic damage' (Conway 2004:84) must occur for an event to be termed cyberterrorism, others believe any terrorist usage of the Internet to constitute a sufficient criterion (Desouza and Hensgen 2003:388).

If the first two areas of contestability are endogenous to the term cyberterrorism and reflect differing levels of importance attached to its constituent parts, the next two are exogenous and concern the way in which the term is used by different actors. So, third, is the regularity with which the term is used interchangeably with other—often also inconsistently used—cyber terminology. As Weimann (2006:132) points out, "…the mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter". Conway (2002), similarly, identifies significant confusion between cybercrime and cyberterrorism. Once we recognise the sheer diversity of cyber-terms in contemporary usage—including, cyberterrorism, cybercrime, hacking, cracking, hacktivism, cyber-activism, cyberwarfare, information warfare, and cyberjihad—it becomes easier still to see how the boundaries of cyberterrorism may escape ready identification (see Macdonald et al. 2013:12–13; Jarvis and Macdonald 2014). This porosity has a real risk of introducing analytical confusion into the concept: muddying what is meant by cyberterrorism and any of its related terminology.

Fourth, and alluded to above, is the role of misleading hyperbole around cyberterrorism (Isenberg 2000), in which "[t]he mass media have added their voice to the fearful chorus with scary front page headlines" (Weimann 2006:151). Indicative here are stories such as that in the UK's Daily Mail, headlined, 'Attack of the Cyber Terrorists' which outlined a hypothetical nightmare scenario including thousands of government web pages suddenly disappearing, tens of millions of pounds being wiped off the share price of companies like Amazon and the entire Internet credit card payment system being put in disarray (Hanlon 2007). This hyperbole feeds off a sense of the uncontrollable and unknown integral to cybersecurity concerns. As Pollitt (1998:8) notes, 'The fear of random, violent victimisation segues well with the distrust and outright fear of computer technology'. Cyberterrorism offers a perfect example of this, incorporating the randomness, incomprehensibility and uncontrollability of terrorism with the complexity and seeming abstractness of technology (Cavelty 2007:29). One result, as Ayn Embar-Seddon (2002:1003), suggests, is the media's tendency to label "…any computer break-in by a 12 year-old script kiddie "cyberterrorism"".

The sense of fear that cyberterrorism produces, coupled with media hyperbole and a lack of understanding of modern digital technologies adds further confusion to this term. These factors are contributory, we argue, to the dualism between physical and cyberspace embraced by some writers and commentators as a way of recognising the latter's distinctiveness. Here, actions unlikely to be deemed 'terrorist' in physical space appear to be viewed differently when they occur in a cyber or digital environment. Others, in contrast, prefer a narrower conception of cyberterrorism, in part because this enables consistency with understandings of non-cyber forms of terrorist violence.

Key Points

- Although coined in the 1980s, the term cyberterrorism became increasingly prevalent at the end of the Cold War because of geopolitical and technological developments.
- There is currently little consensus on the meaning of cyberterrorism, with a major tension between narrow and broad understandings of this concept.
- Reasons for this disagreement include differing approaches to the term's elasticity, a broader confusion amongst 'cyber'-terms, and media hyperbole.

2.3 Locating Cyberterrorism

The previous section outlined four of the most significant factors that contribute to the continuing contestability around the term cyberterrorism. In this section, we build on that discussion by asking what value, if any, there is in even attempting to describe cyber-related activities as terrorism.

'Terrorism', as is well known, is a highly contested term with its own politics. How the term is applied, to whom, and in what contexts, should be thought of as a contingent, rather than an objective, decision. It is a decision, in other words that often reflects political interests and agendas as much as any analytical or 'scientific' considerations (Halkides 1995; Jackson et al. 2011; Gibbs 2012). On top of this, the terrorism label also suffers from considerable "'border' and 'membership' problems" of its own (Weinberg et al. 2004:778) in relation to the kinds of political violence to which commentators are willing to see it applied. Thus, although a number of themes do recur across many different understandings of this term—including (instrumental) violence, political motivation, randomness of targets, theatrical or spectacular violence, the creation of fear in a secondary audience, an effort at communication, non-state perpetratorship, and so on—there currently exists nothing approaching a consensual definition of terrorism amongst either academics or policymakers (Laqueur 1997; Silke 1996; Schmid and Jongman 1988; Fletcher 2006; Gibbs 2012). This lack of consensus is important for us because it helps to account for the quite dramatic changes within understandings of terrorism that have taken place over the 200 years that have now passed since the word was first coined. As Jackson et al. (2011:104–105) note, the term terrorism:

> was originally constructed not to describe the actions of non-state actors such as al-Qaeda, ETA or the Fuerzas Armadas Revolucionarias de Colombia (FARC) to whom we are instinctively drawn when we now hear it. Rather, it was created at the time of the French revolution to refer to the actions undertaken by the state against dissidents and dissenters in their own populations…. Moreover, in its original usage it lacked the negative, pejorative connotations that are now inherent to the term. Indeed, even in the aftermath of World War II, when the term became attached to anti-colonial struggles in Asia, Africa and elsewhere, it lacked, for many, the sense of illegitimacy we now frequently attach to it.

As this suggests, there has been considerable change over time in what the term terrorism both denotes—i.e. what it refers to—and what it connotes—i.e. what associations it calls forth when it is used and heard. That this evolution has taken place itself offers some measure of support for proponents of this lexicon's utility for describing cyber-attacks. For, if the meaning of terrorism has altered so dramatically historically, on what absolute grounds might its application to new types of activity might be denied or critiqued?

If the meaning of the term terrorism has altered so dramatically throughout its history, so too have the types of activities typically included under this label. One prominent account of these change is Rapoport's (2012) 'Four Waves of Modern Terrorism', which seeks to situate terrorism both historically and socially by highlighting transformations within terrorist motivations, weapons and strategies. Thus, Rapoport posits a movement through 'Anarchist', 'anticolonial', 'New Left' and 'Religious' types of terrorism from the late nineteenth century to the present day. Another high profile categorisation centres on the distinction between 'old' and 'new' terrorism (see for example, Burnett and Whyte 2005; Laqueur 1999; Neumann 2009; Schmid and Jongman 1988). 'Old' terrorism is frequently used to refer to groups such as the IRA which are viewed as politically motivated, hierarchically organised, and (often) engaged in the discriminate use of violence against targets they deem legitimate. 'New' terrorism, in contrast tends to refer to the emergence of networked, transnational, religiously-inspired organisations engaged in, "mass-casualty attacks against civilians" using "excessive violence" (Neumann 2009:29). And, where 'old terrorism' is often seen as a backlash to dynamics of empire or other forms of domination, 'new terrorism' is frequently interpreted as part of a response to US-led dynamics of globalisation (Cronin 2002:34).

Whilst there are differences between these two accounts of the history of terrorist violence, they share a view that the actual phenomenon of terrorism—aside from the term's meaning and nuances—has itself undergone considerable, qualitative, change over time. Understanding terrorism as a historically variable entity in this way is again important for thinking about cyberterrorism because it further supports the possibility that previously unheard of activities or violences might be legitimately brought under this label. In other words, because the tactics and targets of terrorism change so dramatically over time we might be wary of efforts to rule out any discussion of cyber- activities as terrorist on *a priori* grounds. Indeed, any number of relevant precedents might be readily identified to help advocates of the 'cyberterrorism' label defend its utility, including eco-terrorism, narco-terrorism, bio-terrorism and so on.

The two above points are, perhaps, the most promising general grounds for resisting attempts to deny any validity to the notion of cyberterrorism outright. Given that the meaning of the word terrorism, and the behaviour to which it is typically applied, have changed so dramatically in 200 years, it would seem difficult to argue that it is simply off limits to actions undertaken with a keyboard rather than a bomb or a gun, for example. Yet, the term obviously cannot refer to anything and everything. As the label terrorism becomes attached to an ever-wider range of behaviours, its meaning inevitably becomes further diluted (see Weinberg et al. 2004). Are there, then, any reasons to accept the application of the language of terrorism to new types of activity in principle, but, at the same time, to resist its use in the cyber domain in practice?

One possible challenge here is the widespread assumption that some kind of violence—often understood as a threat to human security—is necessary for an action to be designated terrorism (Schmid and Jongman 1988). Some acts undertaken in the digital realm—whether real at the moment or still only hypothetical—clearly have the capacity to meet this assumption. If a hacker was able to access air traffic control systems, for example, this would obviously meet this criterion, as would the initial examples given by Denning (2000:71), when she described as cyberterrorism "attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss." It is less clear, however, whether causing harm to property might be considered a form of violence rather than criminal damage, sabotage or vandalism, for instance. Moreover, while we might be willing to use the term violence to describe an individual destroying another's computer with a hammer, we might be more suspicious of its application to an individual's destruction of data, on the same computer, via a virus (see Gordon and Ford 2002:640). If we turn to some of the broadest, umbrella, uses of the term cyberterrorism considered in the opening section—those that allow for the use of the term in relation to any combination of cyber technologies and terrorism—then we might be more wary still.

This criterion of violence might be more manageable than first impressions suggest given that some legal accounts of terrorism—such as the UK Terrorism Act (2000)—expand this term to encompass attacks that bring about, "serious damage to property" in section 1(2)(b). Indeed, as Hardy and Williams (2014) note, section 1(2)(3) of this act, allows for the interpretation of the term to include, the use or threat of action "designed seriously to interfere with or seriously to disrupt an electronic system." On top of this, there are established, and important, traditions of thinking about violence away from direct, physical forms of harm within sociology, peace studies and beyond (for instance, Galtung 1969; Bourdieu et al. 1999). Thus, while removing mention of physical violence may work to dilute the concept's legal and academic value, for some (Post et al. 2000:100), it is at least possible to think through DDoS attacks and the spreading of computer viruses as violences—and therefore potentially as terrorisms—depending on how these terms are themselves approached. As Laqueur (1996:25) notes, "in its long history terrorism has appeared in many guises."

A further issue here is the importance placed upon theatre, performativity, fear and intimidation within many academic definitions of terrorism (Cowen 2006; Conway 2014). Scholars often cite the importance of media coverage and publicity as a primary way of separating this form of violence from others (Tsfati and Weimann 2002). Yet, in the context of 'cyberterrorism', it is possible to argue that, "attack scenarios put forward, from shutting down the electric power grid to contaminating the water supply … are unlikely to have easily captured, spectacular (live, moving) images associated with them" (Conway 2011:28). These examples of 'cyberterrorism' would undoubtedly cause severe disruption for populations and governments. They might be unlikely, however, to have a traumatising effect on audiences in the way that events such as 9/11 or the 2005 Madrid bombings appear to have done, given the broadcasting and endless recycling of images of those attacks (Gillespie 2006; Shoshani and Slone 2008). For authors such as Conway (2011:28) this absence of obvious theatricality is one important impediment to cyberterrorism's likelihood. On the other hand, this emphasis on terrorism as theatre could simply be viewed as a corollary of the contemporary prominence of organisations such as al Qaeda and their preference for high profile, spectacular attacks (Hoffmann 2001): a preference that is not, by any means, representative of the history of terrorist violence.

Key Points

- Because terrorism has such a varied history, it is possible and legitimate to explore whether new types of activity can be described in this way.
- If violence is seen as a central aspect of terrorism, this poses a challenge for some of the widest understandings of cyberterrorism.
- The importance of theatre and performativity within 'terrorism proper' raises further questions about the plausibility of the cyberterrorism concept.

2.4 Constructing Cyberterrorism

This chapter thus far has argued two things. First, that there exists a considerable diversity of understandings of cyberterrorism. This diversity, we noted, has real implications for thinking about the range of activities that might be incorporated under this concept. Second, we have also argued that the definition or discussion of cyber-activities as examples or instances of *terrorism* is a far from straightforward task. This is not, of course, to say that to do so is impossible, worthless, or doomed to fail. Rather, to suggest that real attention needs to be given to the extent to which actions undertaken in the cyber-domain can be reconciled with the constituent parts or characteristics of terrorism as typically understood (violence, theatricality, and so forth).

Three distinct routes present themselves in response to this dilemma. In the first instance, one might conclude that the types of activity typically labelled cyberterrorism (whether actual or hypothetical) bear so little resemblance to 'terrorism proper' that the term cyberterrorism is itself a misnomer. Here, a parallel debate within contemporary discussion on 'state terrorism' might be instructive, given the recurrence of similar questions therein around the flexibility of terrorism as a concept (compare, for example, Stohl and Lopez 1988; Blakeley 2007, 2009; Jackson et al. 2010; Jackson et al. 2011; Stohl 2014). As Andrew Silke suggested of terrorism and state terrorism: "while there are similarities between the two, they are ultimately two different creatures" (cited in Stohl 2012:45). Cyberterrorism may be viewed in an equivalent way: as similar to, but ultimately different from, non-cyberterrorisms. An argument of this sort does not, of course, necessarily imply that cyber-attacks or their threat are neither serious nor real. Rather, it suggests that whatever such activities might be, they are not cyber*terrorism*. Or, perhaps better, that whatever such activities might be, there is little value in *thinking about* them as cyberterrorism.

A second, and different, response would be not to argue against the label cyberterrorism *per se*. Rather, to appeal instead for greater conceptual and definitional work in order further to clarify the relationship between terrorism and cyberterrorism. With greater interpretive labour and some form of sustained debate around cyberterrorism's meaning, parameters, types, and so forth, it is possible that its specific nature—and its connection to other types of violence—might become gradually clearer. Beyond any conceptual value, greater definitional work of this sort might have additional analytical benefit. Explaining the causes of cyberterrorism, for example, might be made easier by a more sophisticated account of what precisely the term means. Policy issues of response and responsibility might also be assisted by further clarity of denotation (see Legrand 2014; Carlile and Macdonald 2014). There may also be normative reasons for the undertaking of such an enterprise, where greater certainty over cyberterrorism's meaning might assist in our construction of ethical judgements about the (il)legitimacy of a spectrum of cyber-activities. As Meisels (2009:348) has argued on the concept of terrorism more broadly: "Terrorism ought to be strictly defined. It is too central a concept to the moral understanding of our contemporary world to remain obscure."

An alternative approach to each of the above, and the one explored in the remainder of this section, would be to pursue a different type of research agenda entirely. Rather than attempting to define what cyberterrorism is, this approach involves redirecting our gaze instead to *how* cyberterrorism is socially constructed or produced. In the following we outline what such an approach might entail, before discussing some of its strengths and limitations.

In recent years there has emerged a much-discussed burgeoning of academic literature on terrorism. One important, and controversial, dynamic within this has been the development of an explicitly and self-consciously 'critical' scholarship that set out to challenge the assumptions and conventions of Terrorism Studies as previously constituted. One key dimension—or 'face' (Jarvis 2009)—of this scholarship has been a collection of broadly constructivist studies exploring representations of terrorism in political language, popular culture, policy documents and so on (see Jackson et al. 2011:50–73). Because constructivist in tone, these studies tend to share three common ontological premises (see Guzzini 2005). First, that the world around us is constituted, in part, by our beliefs and ideas about it. Second, that our beliefs about the world—the knowledge we have of the world—are themselves socially constructed and maintained: there is no objective, direct correspondence between our ideas and the world of things. And, third, that there is an important dynamic of interaction between these two dimensions such that our ideas and social realities shape, reinforce and impact on one another.

In the context of terrorism, this type of approach leads to the pursuit of very different research projects to those typical of more established studies in this area. As Hülsse and Spencer (2008:572; also Jackson et al. 2011) argue, such a perspective changes the very nature of terrorism, such that this phenomenon is no longer seen as a brute material fact; but rather, as a, "…a social construction, hence a social fact produced in discourse". As they continue, this rethinking of what terrorism *is* has repercussions for how and what might be studied:

> Accordingly, research needs to focus on the discourse by which the terrorist actor and his or her actions are constituted. Terrorism can only be known through the terrorism discourse. This is why we suggest a shift of perspective in terrorism studies, from the terrorist to terrorism discourse. Instead of asking what terrorism is like (what structures, strategies and motivations it has), we need to ask how it is constituted in discourse (Hülsse and Spencer 2008:572).

And, although arguments of this sort may raise philosophical questions about the nature of terrorism's existence, they need not imply any outright denial thereof:

> Analyzing terrorism as a concept that is used in practice by various social actors is not to deny that terrorism exists but to say that what counts as terrorism has to be represented and communicated for it to exist. Hence, it is the use of the symbol terrorism and communities' orientations towards it that are central. Indeed, for a completely constructivist approach, whether or not terrorism exists is less important than *how* terrorism and terrorists are constructed in practice and the identities and policies that are authorized therein (Stump and Dixit 2012:212).

For the phenomenon of cyberterrorism with which this book engages there is obvious and significant scope for the application of social constructivist insights in future research. Building on the recent explorations of terrorism noted above, as well as on related studies within International Relations, Foreign Policy Analysis and Political Science, these works could engage with a range of important, and as yet under-researched, questions. Chief amongst these, we suggest, are the following.

First, there is scope for exploring precisely how cyberterrorism is constructed in political and other forms of discourse. What language is used to describe this phenomenon and its threat, for example? What are the key tropes, predicates, metaphors and other rhetorical building-blocks that structure contemporary discussion? Within this, it would be crucial to explore how cyberterrorism is positioned spatially and temporally. So, for the former, is it depicted as an internal or external security threat, for example? Is it seen as amorphous and everywhere, or a threat that is located only in particular spaces of socio-political life? In terms of the latter, to what extent do claims about cyberterrorism's novelty and uniqueness link to and help exaggerate this threat? How, moreover, is cyberterrorism presented as a threat today, and which referent objects are employed in these constructions: are corporations, national security architectures, ordinary citizens or others seen, typically, as its target? There is scope here also, finally, for exploring the consistency of constructions of cyberterrorism. Do these change over time and across space, or do similar themes emerge in separate discourses? And, crucially, are there deviant, counter-hegemonic, or oppositional discourses at work that challenge seemingly accepted knowledge in this area? Who, if anyone, resists dominant constructions of this threat?

Second, there is also considerable scope for explorations of intertextuality in constructions of cyberterrorism. To what extent, for example, do representations of cyberterrorism link to and build on constructions of terrorism more broadly? Do we encounter the same rhetoric (perhaps of evil, of religious inspiration, of sleeper cells, and so on) being employed to describe this phenomenon (see Jackson et al. 2011:50–73), or are there distinctive rubrics at work in this context? Likewise, are there overlaps with the way the Internet is imagined in other social and political contexts? Do constructions of cyberterrorism rely, for instance, on fears of the digital realm as unregulated and dangerous? If so, do these reproduce or change broader discourses on the cyberworld? And, does the cyber- prefix work to amplify or reduce the constructed threat of cyberterrorism? Finally, to what extent do different representations of cyberterrorism connect to one another? Do policymakers, for example, draw on discursive resources from media or fictional depictions of this threat, and if so which and in what contexts?

A third set of research questions would focus on performative or political questions regarding what discourses of cyberterrorism actually 'do'. For example, how do representations of this phenomenon make possible and/or foreclose particular policy responses? Do constructions of this threat apportion responsibility for mitigating or responding to it, and if so how? Are specific technologies, actors or strategies prioritised in discourses on how to counter cyberterrorism? And, from where does the responsibility of actors privileged in these discourses derive: is it their expertise, or their location in particular socio-political sites, for example? Finally, where do normative questions around issues of legitimacy, rights or justice emerge in discussions of cyberterrorism? If they do, how are these articulated, and what type of limits or exceptions to the range of potential counter-measures are posited?

Fourth, a constructivist approach of this sort would also explore in whose interests discourses on cyberterrorism work. Who, if anyone, benefits from constructions of this entity, and, indeed, from efforts to amplify or minimise the threat that it poses? Are there discernible economic, political or other motivations behind discourses in this area, for example? How one responds to these questions is likely to be impacted by one's epistemological commitments: by the knowledge claims, in other words, one is willing to make. Here, 'thinner' or more 'conventional' constructivist analyses would tend to view cyberterrorism discourses as the creation of particular actors and their interests; as instruments, put otherwise, to achieve certain things. 'Thicker' or more 'critical' constructivisms, in contrast, would tend to view the identities, interests and subject positions of those actors as themselves constituted by discourses on cyberterrorism. Viewed thus, the 'cyberterrorist', the 'security professional' and the interests of each might be deemed part of, not separate from, such discursive frameworks.

As the above suggests, there exists immense scope for constructivist research into cyberterrorism. Such research might, we suggest, offer a valuable route for circumventing some of the difficulties of definition outlined in this chapter's opening sessions. A major strength of a constructivist approach such as that sketched above is that it allows an engagement with the concept of cyberterrorism *in spite of* the definitional complexities and debates that surround it. Cyberterrorism undoubtedly has a social and political existence, even if we believe this to be a purely rhetorical one. Policymakers and experts employ this language, funding is dedicated to its prevention, film producers hypothesise attack scenarios, and academics speculate on its existence and threat in books such as this! However contested a concept it may be, there are good grounds, therefore, for resisting the temptation to abandon it completely. As Jackson (2010:12) argued in relation to the (no less contested) concept of terrorism:

> …pragmatically, the term 'terrorism' is currently so dominant within existing political structures, the academy, and the broader culture, that critically-oriented and responsible scholars cannot really afford to abandon it without risking marginalisation. …it must be engaged with, deconstructed, challenged and used in more rigorous ways.

The flipside of this is that an approach of this sort may have limited policy relevance or problem-solving utility for those tasked with preventing, responding to, or assessing the threat of cyberterrorism. Constructivist approaches may be able to contribute far less to the types of debate explored in the later chapters of this book, given their emphasis on *how* cyberterrorism and its threat are constructed. How serious a limitation one perceives this to be will likely depend, in part, on one's view of academic roles and responsibilities. Is it our task, as students or analysts of cyberterrorism to quantify its risk and seek to prevent it? Or is our role to engage with social and cultural productions of 'cyberterrorism' with an eye to deconstructing dominant knowledge claims or practicing other forms of critique? While there are no definitive answers to these questions, there is, undoubtedly, a debate to be had along these lines. And, as outlined in this book's introduction, each of the chapters contained in this edition contributes to this discussion in one way or another.

Key Points

- The difficulties of describing cyber-activities as examples of (cyber)terrorism might be met by abandoning the term altogether, or by working toward a more accurate or consensual definition of this term.
- An alternative approach to either of these is to pursue a constructivist line of enquiry, and ask not *what* cyberterrorism is, but *how* it is constructed.
- An advantage of a constructivist framework is that it helps scholars to engage with this concept in the absence of any settled understanding of its meaning.
- A potential disadvantage might be constructivism's limited problem-solving utility.

2.5 Conclusion

In this chapter we have explored the value as well as some of the challenges associated with the concept of cyberterrorism. In so doing, we argued that there exists a general lack of consensus around fundamental questions relating to this term. The chapter's second section explored the possibility of locating cyberterrorism within the broader historical context of terrorism as itself a fluid and changing phenomenon. Historical variations in the meaning and methods of terrorism, we argued, potentially open space for incorporating cyber-activities under this heading. At the same time, doing so may not be entirely straightforward given the lack of similarity between current understandings of cyberterrorism and widespread assumptions around 'terrorism proper'. The chapter concluded by suggesting three competing ways to confront these challenges in an effort to add direction to an increasingly confused debate. Our view is that a constructivist framework offers the greatest potential for engaging with the concept of cyberterrorism in spite of its challenges, not least because it already exists as a category of discourse and hence social reality.

We finish our discussion, finally, by highlighting Collier and Mahon's useful reminder that, "when scholars take a category developed from one set of cases and extend it to additional cases, the new cases may be sufficiently different that the category is no longer appropriate in its additional form" (cited in Weinberg et al. 2004). This is important, because if we are to allow discussion of cyber-activities under the heading of terrorism, it is likely that this broader concept itself will be changed. This may be or may not be desirable, depending, in part, on one's view of terrorism's analytical, political or normative utility. Nonetheless, it requires consideration, not least given the term's resonance in current academic, political and media discourse.

Key Points

- Research into cyberterrorism needs to move beyond questions of definition, to recognise that cyberterrorism as a category of discourse is already a social reality. As such, it is one that requires serious analytical and critical engagement.
- If we are to allow discussion of cyber-activities under the heading of 'cyberterrorism', then it likely that our broader concept of 'terrorism' will change.

Further Reading and Resources

Conway M (2004) Cyberterrorism: media myth or clear and present danger? In: Irwin J (ed) War and virtual war: the challenges to communities. Rodopi, Amsterdam, pp 79–95

Denning D (2000) 'Cyberterrorism: testimony before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives. http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf. Accessed 31 Aug 2012

Denning D (2010) Terror's web: how the Internet is transforming terrorism. In: Jewkes Y, Yar M (eds) Handbook on internet crime. Wilan Publishing, Devon, pp 194–213

Gordon S, Ford R (2002) Cyberterrorism? Comput Secur 21(7):636–647

Weimann G (2006) Terror on the Internet: the new arena the new challenges. United Institute of Peace Press, Washington, DC

Weinberg L, Pedahzur A, Hirsch-Hoefler S (2004) The challenges of conceptualizing terrorism. Terrorism Polit Violence 16(4):777–794

References

Anderson K (2009) Hacktivism and politically motivated computer crime. Encurve. http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Accessed 3 Aug 2012, pp 1–15.

Bendrath R, Eriksson J, Giacomello G (2007) From 'cyberterrorism' to 'cyberwar', back and forth: how the United States securitized cyberspace. In: Eriksson J, Giacomello G (eds) International relations and security in the digital age. Routledge, Abingdon

Blakeley R (2007) Bringing the state back into terrorism studies. Eur Polit Sci 6(3):228–235

Blakeley R (2009) State terrorism and neoliberalism: the north in the south. Routledge, London

Bourdieu P et al (1999) The weight of the world. Social suffering in contemporary society. Policy Press, Oxford

Burnett J, Whyte D (2005) Embedded expertise and the new terrorism. J Crime Conflict Media 1(4):1–18

Carlile L, Macdonald S (2014) The criminalisation of terrorists' online preparatory acts. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Cavelty M (2007) Cyber-terror—looming threat or phantom menace? The framing of the US Cyber-Threat Debate. J Inform Technol Pol 4(1):19–36

Collin BC (1997) The future of cyberterrorism. Crim Justice Int 13(2):15–18

Conway M (2002) Reality bytes: cyberterrorism and terrorist 'use' of the Internet. First Monday 7(11), (n.p.)

Conway M (2004) Cyberterrorism: media myth or clear and present danger? In: Irwin J (ed) War and virtual war: the challenges to communities. Rodopi, Amsterdam, pp 79–95

Conway M (2011) Against cyberterrorism: why cyber-based terrorist attacks are unlikely to occur. Viewpoints: Privacy Secur 54(2):26–28

Conway M (2014) Reality check: assessing the (un)likelihood of cyberterrorism. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Cowen T (2006) Terrorism as theater: analysis and policy implications. Publ Choice 128(1–2):233–244

Cronin A (2002/2003) Behind the curve globalisation and international terrorism. Int Secur 72(3):30–58

Denning D (2000) Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Accessed 4 Feb 2012

Denning D (2010) Terror's web: how the Internet is transforming terrorism. In: Jewkes Y, Yar M (eds) Handbook on internet crime. Wilan Publishing, Devon, pp 194–213

Desouza KC, Hensgen T (2003) Semiotic emergent framework to address the reality of cyberterrorism. Technol Forecast Soc Change 70(4):385–396

Devost MG, Houghton BK, Pollard NA (1997) Information terrorism: political violence in the information age. Terrorism Polit Violence 9(1):72–83

Embar-Seddon A (2002) Cyberterrorism: are we under siege? Am Behav Sci 45(6):1033–1043

Fletcher G (2006) The Indefinable Concept of Terrorism. J Int Criminal Justice 4(5):894–911

Galtung J (1969) Violence, peace and peace research. J Peace Res 6(3):167–191

Gibbs J (2012) Conceptualization of terrorism. In: Horgan J, Braddock K (eds) Terrorism studies: a reader. Routledge, Abingdon, pp 41–62

Gillespie M (2006) Transnational television audiences after September 11. J Ethnic Migrat Stud 32(6):903–921

Gordon S, Ford R (2002) Cyberterrorism? Comput Secur 21(7):636–647

Gordon S, Ford R (2003) Cyberterrorism? Symantec security response. Symantec, Cupertino

Guzzini S (2005) The concept of power: a constructivist analysis. Millenn J Int Stud 33(3):495–521

Halkides M (1995) How not to study terrorism. Peace Rev 7(3/4):253–260

Hanlon M (2007) Attack of the cyber terrorists. The Daily Mail. http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html. Accessed 2 Aug 2012

Hardy K, Williams G (2014) What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Harknett R (2003) Integrated security: a strategic response to anonymity and the problem of the few. Contemp Secur Pol 24(1):13–45

Hoffmann B (2001) Change and continuity in terrorism. Stud Conflict Terrorism 24(5):417–428

Hülsse R, Spencer A (2008) The metaphor of terror: terrorism studies and the constructivist turn. Secur Dialog 39(6):571–592

Isenberg D (2000) Electronic pearl harbor? More hype than threat. CATO Institute. http://www.cato.org/publications/commentary/electronic-pearl-harbor-more-hype-threat Accessed 7 Sept 2012.

Jackson R (2010) In defence of 'terrorism': finding a way through a forest of misconceptions. Behav Sci Terr Pol Aggr 3(2):1–15

Jackson R et al (2010) Introduction: terrorism, the state and the study of political terror. In: Jackson R et al (eds) Contemporary state terrorism: theory and practice. Routledge, London, pp 1–11

Jackson R et al (2011) Terrorism: a critical introduction. Palgrave, Basingstoke

Jarvis L (2009) The spaces and faces of critical terrorism studies. Secur Dialog 40(1):5–29

Jarvis L, Macdonald M (Forthcoming) What is cyberterrorism? Findings from a survey of researchers. Terrorism Polit Violence

Jarvis L, Macdonald S (2014) 'Locating Cyberterrorism: how Terrorism researchers use and view the Cyber Lexicon', Perspectives on Terrorism 8(2):52–65

Kostopoulos G (2008) Cyberterrorism: the next arena of confrontation. Comm IBIMA 6(1): 165–169

Laqueur W (1977) Terrorism. Little Brown, Boston, MA

Laqueur W (1996) Postmodern Terrorism: New Rules for an Old Game. Foreign Affairs 75(5)

Legrand T (2014) The citadel and its sentinels: state strategies for contesting cyberterrorism in the UK. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Macdonald S, Jarvis L, Chen T, Lavis S (2013) Cyberterrorism: a survey of researchers. Cyberterrorism project research report (No. 1), Swansea University. Available via: www.cyberterrorism-project.org

Malcolm JG (2004) '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

McGuire M (2014) Putting the 'cyber' into cyberterrorism: re-reading technological risk in a hyperconnected world. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Meisels T (2009) Defining terrorism—a typology. Crit Rev Int Soc Polit Philos 12(3):331–351

National Academy of Sciences (1991) Computers at risk: safe computing in the information age. Computer Science and Tele-communications Board. National Academy Press, Washington, DC

Neumann P (2009) Old and new terrorism. Polity Press, Cambridge

Olmstead S, Siraj A (2009) Cyberterrorism: the threat of virtual warfare. CrossTalk: J Defense Software Eng 22(7):16–18

Pollitt M (1998) Cyberterrorism—fact or fancy. Comput Fraud Secur 3(2):8–10

Post J, Ruby K, Shaw E (2000) From car bombs to logic bombs: the growing threat from information terrorism. Terrorism Polit Violence 12(2):97–122

Rapoport D (2012) The four waves of modern terrorism. In: Horgan J, Braddock K (eds) Terrorism studies: a reader. Routledge, Abingdon, pp 41–62

Schmid A, Jongman A (1988) Political terrorism. Transaction, Piscataway

Shoshani A, Slone M (2008) The drama of media coverage of terrorism: emotional and attitudinal impact on the audience. Stud Conflict Terrorism 31(7):627–640

Silke A (1996) Terrorism and the blind men's elephant. Terrorism and Political Violence 8(3): 12–28

Singer PW (2012) The cyber terror bogeyman. Armed Forces J. http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer. Accessed 16 Sept 2013

Soo Hoo K, Goodman S, Greenberg L (1997) Information technology and the terrorist threat. Survival 39(3):135–155

Stohl M (2012) State terror: the theoretical and practical utilities and implications of a contested concept. In: Jackson R, Sinclair J (eds) Contemporary debates on terrorism. Routledge, Abingdon, pp 43–49

Stohl M (2014) Dr. Strangeweb: or how they stopped worrying and learned to love cyber war. In: Chen T, Jarvis L, Macdonald S (eds) Cyberterrorism: understanding, assessment, and response. Springer, New York

Stohl M, Lopez G (eds) (1988) Terrible beyond endurance? The foreign policy of state terrorism. Greenwood Press, New York

Stump J, Dixit P (2012) Toward a completely constructivist critical terrorism studies. J Int Relat 26(2):199–217

Tsfati Y, Weimann G (2002) www.terrorism.com: terror on the Internet. Stud Conflict Terrorism 25(5):317–332

Weimann G (2006) Terror on the Internet: the new arena the new challenges. United Institute of Peace Press, Washington, DC

Weinberg L, Pedahzur A, Hirsch-Hoefler S (2004) The challenges of conceptualizing terrorism. Terrorism Polit Violence 16(4):777–794