Book chapter :

Nouri, L., Jarvis, L. & Whiting, A. (2015). *Terrorism, Violence and Conflict in the Digital Age: Implications, Opportunities and Challenges.* H. Toros & I. Tellidis (Ed.), Researching Terrorism, Peace and Conflict Studies, Abingdon: Routledge.

Terrorism, Violence and Conflict in the Digital Age

Lee Jarvis, Lella Nouri and Andrew Whiting

Introduction

Cybersecurity throws up obvious and important challenges for the academic discipline of International Relations and the materialist, state-centric ontology around which it has been traditionally organised. Such challenges might also, as a consequence, throw up similar problems for related or derivative fields of enquiry including Terrorism Studies and Peace and conflict studies (PCS). In this chapter, we explore the nature of such challenges as well as the potential of these research traditions to contribute to our understanding of one much-discussed example thereof: cyberterrorism. How, we ask, might these disciplines address this most recent articulation of terrorism? And, how might contemporary debate on cyberterrorism benefit from reflection on earlier discussions in these broad areas? Our discussion proceeds in three stages.

The chapter begins with a brief overview of the diversity of threats that exist within cyberspace today. Here, we identify three broad categories - malicious software, hacking and online disruption. We argue that these share a common logic that centres on the exploitation of vulnerabilities within target systems. A second section then offers a brief discussion of the parameters of Terrorism Studies today, before reflecting on the implications of activities potentially readable as cyberterrorism for this field. Here, we point to longstanding questions around definition, threat and response in terrorism research, as well as the recent broadening of terrorism studies associated with Critical Terrorism Studies (CTS), and especially constructivist analyses therein. Constructions of cyberterrorism, we argue, problematise established responses to these questions. The chapter's third section then turns to literature associated with Peace and Conflict Studies. Here, we argue that this work has value for understanding cyber activities for several reasons. These include, first, a history of debate around the nature of 'violence' that might be put to work for thinking through the implications of non-corporeal or non-physical attacks, for example those targeting data. Second, a longstanding emphasis on interdisciplinary research, that stretches back to the Cold War origins of this field. And, third, an engagement with international issues and analyses that stretches beyond the parameters of states and their relations.

Threats in Cyberspace

On stepping down as head of Microsoft in 2008, Bill Gates noted that he and Paul Allen had dreamt about putting a computer on every desk when they established the company in the 1970s (Beaumont, 2008). Perhaps they did not envision (but likely they did) a world such as today's where computer technology has become so ingrained within daily life: a world where computers reside not only on desks at home and in the office, but in briefcases and pockets, on coffee tables and wrists, and even, now, on the bridges of noses. The proliferation of different devices, the consistent rate at which microprocessors have become smaller and more powerful (Moore's Law), and the continued growth of the Internet has seen computer technology penetrate all manner of aspects of everyday life, from the trivial to the serious.

Digital technologies are now vital to the organisation of political, social and economic life including in the management of critical infrastructure, the storing of consumer and citizen information, the collection and analysis of intelligence on potential security threats, the exchange of billions of pounds of online trade in financial and other markets, and the functioning of military hardware. The extent to which computer technology has penetrated recreational and working lives, as well as the patterns and structures of domestic and international governance, has been likened by some to a 'dependency' (Kizza, 2014, p. 76). If this 'dependency' generates potentially desirable gains in efficiency, reliability and velocity, it also produces new problems associated with 'cyber-threats'. Whilst the nature, motives and manifestation of these have varying levels of complexity and seriousness, such threats typically share an attempt to exploit vulnerabilities permitting unauthorised access to target systems. This is the case in the efforts of 'script kiddies' to deceive 'ordinary' computer users into downloading simple e-mail borne viruses, on the one hand. And, on the other, state-supported experts engaging in acts often understood as cyber-war such as the targeting of critical infrastructure via malicious software.

Although threats in cyberspace often blend different techniques, the most commonly observed are threefold: malware attacks, 'hacking', and online disruption. Malware - which includes viruses, worms and Trojans - refers to "software that has malicious intent to create harm to the computer or network operation" (Zolkipli & Jantan, 2011, p. 199). Examples stretch from simple e-mail attachments such as the ILOVEU bug of 2000 which caused minor damage to a user's computer before sending itself to others via the initial victim's address book, through to modern 'Advanced Persistent Threats' such as Stuxnet, Flame, and Duqu. Although targets may differ radically, the premise beneath these remains the same: locate a vulnerability, then write a piece of software that once delivered will insert foreign code into a 'normal' programme modifying it to perform a function unintended by its user (Chen & Davis, 2008, p. 545).

'Hacking' is a broad term referring to the gaining of unauthorised access to a computer system. As a result, it will likely play a part at some stage of a large proportion of computer-based attacks. However, it is included here as a standalone category due to the prevalence of hacks in recent years responsible either for defacing and disrupting websites, or for the theft and dissemination of sensitive information. Both of these kinds of 'hacks' are commonly, although not exclusively, used by 'hacktivist' collectives. That is, with groups such as Anonymous and the Syrian Electronic Army which select particular targets because of their potential publicity impact, or due to perceptions of the target's corrupt or unjust behaviour. For example, a year after the suicide of Aaron Swartz (the hacker who used the Massachusetts Institute of Technology's computer network to illegally download a number of academic journals from JSTOR) Anonymous defaced MIT's website with a message highlighting the injustice of US computer crime law (Telegraph, 2013). Swartz's hack of JSTOR could itself be considered a prominent example of the other kind of hacking (relating to data theft) but an even more high profile case (certainly in the UK) is that of Gary McKinnon and his accessing of 97 computers (a combination of US military and NASA systems) either in an attempt to coerce the US or to find evidence of UFOs (House of Lords, 2008).

Online disruption - especially via Distributed Denial of Service (DDoS) attacks - represents a different risk again. DDoS attacks attempt to overwhelm the capacity of the servers hosting a particular website by having a large number of computers access the site simultaneously. Although closely associated with hacktivism, it has proved a popular technique for sub-state and state actors alike, being used for example, as part of Anonymous' 'Project

Chanology' attacks on the Scientology website as well as suspected Russian attacks on a number of Georgian websites during the 2008 conflict (Tikk *et al*, 2008, pp. 8-9). Although DDoS can be achieved via coordination with likeminded users, botnets (networks of infected computers working together unbeknownst to their owners) are often used to increase the traffic to a target site beyond manageable numbers.

To date malware, hacks, and DDoS attacks tend to have been used for reasons of financial gain, disruption, accessing information, raising awareness of a cause or injustice, and (less prominently) sabotage. For a number of reasons, however, categorising such attacks is far from straightforward, with the lines separating terms in our cyber-lexicon - which now includes cyberterrorism, cyberwar, cybercrime, cyberespionage, cyberjihad and so on - far from straightforward or uncontested (Jarvis and Macdonald, forthcoming, a). A useful example of this arrives with a hacking attack on the computer systems within Arizona's Department of Public Safety (DPS) on 24 June 2011, which led to the download and release of 'hundreds of law enforcement files' (Sanchez *et al*, 2011). Responsibility for this was subsequently claimed by LulzSec, a hacktivist collective with a more "light hearted" rationale than others.[1] A few days later, LulzSec announced its plans to disband, prompting the following response from the DPS explaining that it would continue to pursue those responsible for the hack:

> The week of June 20, 2011, the Arizona Department of Public Safety became aware that their email system had been compromised by a *known cyberterrorism group*, known as LulzSec. The group appears to have gained access to the email accounts of at least seven DPS employees. The *cyberterrorism group* has posted the stolen information on their website. Law Enforcement agencies are working to identify the source of the cyber-attack and have initiated a joint criminal investigation (Arizona Department of Public Safety, 2011, our emphasis).

'Cyberterrorism group?' Whilst it is clear that the definition of terrorism is far from settled (Jackson *et al*, 2011, pp. 99-123) and definitions of cyberterrorism are perhaps even less so for a number of reasons (Jarvis *et al*, forthcoming), this theft and publication of sensitive materials would seem on first reading at least to have little in common with the instrumental, communicative violences we tend today to associate with terrorism (Jackson *et al*, 2011, pp. 115-118). How is it, then, that a group known primarily for defacing websites, stealing information, and embarrassing governments and major corporations is suddenly deemed 'terrorist'?

In a similar vein, readers may be surprised to discover that cyber-war is now also upon us (at least, according to some experts). James Farwell and Rafal Rohozinski for example, claim that Stuxnet (the computer worm allegedly launched by U.S. and Israeli forces against an Iranian nuclear facility), demonstrated that, "for cyber war, the future is now" (Farwell & Rohozinski, 2011, p. 23). Leading computer security company Symantec (n.d.) corroborated this view, arguing that Stuxnet could have had multiple different purposes, but amongst the 'most obvious' were 'sabotage, destruction, and cyber war'. As with the relationship between the DPS hack and terrorism, Stuxnet's connection to war seems potentially problematic. On the one hand, it seems rash to discount the significance of a piece of malware with a genuinely unprecedented level of complexity and disruption capable of affecting such a key site of Iranian

[1] Although LulzSec have targeted high profile organisations including the United States Senate and the CIA, their mottos are indicative of their actions' motives, or at least rationale: "The world's leaders in high-quality entertainment at your expense" and "Laughing at your security since 2011".

infrastructure. On the other hand, however, wars do not tend to be characterised by seemingly one-off instances of disruption such as this.

Do activities such as these, and their subsequent understanding, meant that war is different in cyber-space than in physical space? And, does the same apply for terrorism, activism, violence, aggression, and so on? Despite the readiness of many to prefix established categories of political violence with ‘cyber’, other authors such as Rid (2013) and Conway (2004) are far more sceptical of the value of such attempts to make sense of (or construct) contemporary developments. To evaluate these debates, this chapter turns now to the value of Terrorism Studies as a potential source for resolving such conceptual and related issues in the light of cybersecurity concerns including those outlined above.

Terrorism Studies and Cyber Threats

The academic field of Terrorism Studies is a comparatively young one that only began its emergence as a recognisable area of scholarly enquiry in the early 1970s (Jackson *et al* 2011: 11). Terrorism research has, as Schmid (2011: 462) notes, “been more often criticized than praised”, for, as Silke (2004: 1-2) provocatively summarises:

> Research on terrorism has had a deeply troubled past. Frequently neglected and often overlooked, the science of terror has been conducted in the cracks and crevices which lie between the large academic disciplines. There has been a chronic shortage of experienced researchers - a huge proportion of the literature is the work of fleeting visitors: individuals who are often poorly aware of what has already been done and naïve in their methods and conclusions. Thus, while the volume of what has been written is both massive and growing, the quality of the content leaves much to be desired.

Critics of what has been termed ‘Orthodox Terrorism Studies’ argue that the field - although, undeniably diverse - replicates or reproduces a problem-solving emphasis that has, until recently, dominated International Relations and Strategic Studies more broadly (see Cox, 1981, p 128). This, in turn, is linked to criticisms of the field’s methodological and analytical limitations, its state-centric ontology, the embedded nature of terrorism experts, and the prioritisation of policy-relevant analysis (Jarvis 2009, pp. 7-13; Ranstorp, 2009, pp. 1-33; Silke, 2009, pp. 34-48; Stump and Dixit, 2013, pp. 1-4). Although similarly diverse, advocates of ‘Critical Terrorism Studies’ tend to argue for greater reflexivity in research, a model of scholarly responsibility organised around critique rather than policy-relevance, and, a movement away from essentialist conceptions of terrorism (Jarvis, 2009, p.14). In this sense, contemporary ‘critical’ approaches might be considered, in part, as an effort to problematise and recast the perennial questions of definition, causation and response within terrorism research, to which we now turn (see Jackson, 2007; Jarvis, 2009, Stump and Dixit, 2013).

Attempts to define ‘terrorism’ as an object of scholarly knowledge - and reflections on the challenges of so doing - have been integral to terrorism research for many years (compare, amongst many others, Schmid and Jongman 1988; Badey, 1998; Kennedy 1999; Silke 2009: 35-48). Indeed, one recent survey identified over 250 such definitions from academic, governmental and intergovernmental sources (Easson and Schmid 2011). Whilst some have met this contestability with resignation, arguing this definitional quest is either unnecessary or even, “inhibiting the proper study of terrorism” (Malik 2000: xvii), others have posited academic, political and policy reasons for its continuation (Jackson *et al* 2011: 107).

Importantly, for our purposes, this definitional contestability has been directly transplanted into the relevant academic literature on cyberterrorism. Of particular debate, in this context, has been the importance of physical violence as a generative characteristic of terrorism in its various incarnations. On one side of this discussion are advocates of a limited, narrow definition of cyberterrorism - sometimes referred to as 'pure cyberterrorism' (Gordon and Ford, 2002, p. 637) - for whom, "an attack should result in violence against persons or property, or at least cause enough harm to generate fear" (Denning, 2000) for it to qualify as cyberterrorism. On the other side of the debate are subscribers to a broader use of the concept, for whom *any* terrorist activity online might qualify as cyberterrorism: whether cyber-attacks, communication via email, or reconnaissance activities (see Gordon and Ford, 2002). As a recent survey of researchers revealed, such discrepancies in the meaning and use of the concept of cyberterrorism are as common as they are for its 'parent' concept. These definitional differences, moreover, have implications for our answer to quite fundamental questions relating to cyberterrorism, including whether or not a cyberterrorist attack has ever even taken place (Jarvis *et al*, 2014, pp. 74-83).

As this suggests, discussions of cyberterrorism throw up considerable challenges for prominent understandings of terrorism. In the first instance, cyber-attacks such as via malware, hacking or efforts at online disruption might require a rethinking of what 'violence' is in the context of terrorism (does data destruction, for example, count as such), as well as a significant broadening of terrorism's current manifestations: from bombs to bytes, and so on. At the same time, broader accounts of cyberterrorism might encourage or even require us to rethink the importance of traditional generative characteristics of terrorism - such as violence - in their entirety. Here, some have argued that cyberterrorism is linked to, yet so distinct from, its progenitors that simplistic formulae of the sort "cyberterrorism = terrorism + computers" fail to recognise the peculiarities of the cyber environment (see Jarvis and Macdonald, forthcoming, b). As Holt (2012: 341) puts it:

> while there is no single agreed upon definition for cyberterror, it is clear that this term must encapsulate a greater range of behavior than physical terror due to the dichotomous nature of cyberspace as a vehicle for communications as well as a medium for attacks. More expansive definitions … provide a much more comprehensive framework for exploring the ways that extremist groups utilize technology in support of their various agendas.

One obvious retort to such arguments would posit 'cyberterrorism' as a misnomer in these discussions; one generated either by misrecognition of the essence of terrorism, or by more wilful attempts to scaremonger or demonise certain groups. On the other hand - taking inspiration from earlier debates including around 'environmental security' (Græger 1996: 111) - we might argue that cyberspace and terrorism are already so firmly linked in political and other discourse that a responsibility to engage with portmanteau terms such as cyberterrorism already exists: whether for the purposes of critique or problem-solving.

Beyond straightforward definitional discussion, references to cyberterrorism pose additional issues for assumptions and typologies common within terrorism research. In spite of its apparent novelties, for example, cyberterrorism would not seem automatically to fit into discussions of 'new terrorism' and the threat posed by networked, transnational, religiously-inspired groups willing to engage in, "mass-casualty attacks against civilians" using "excessive violence" for performative or theatrical effect (Neumann, 2009, p.29). In other words, established conceptions of terrorism and its historical development - whether dichotomous (new/old) or revolutionary ('waves' of terrorism) - might be seen as either limited or misleading once we introduce cyber-activities into terrorism research. Those existing histories might also, moreover, both engender and camouflage threat assessments relating to terrorism that look rather different once cyberattacks are considered. Thus, on the one hand, there is a risk that cyberterrorism's likelihood is evaluated through potentially outdated models of terrorism crafted for offline scenarios - whether as rational actor (Giacomello 2004) or seeker of theatre (Conway 2011) - that may not automatically translate to cyber-domains. Alternatively, it is also possible that a misunderstanding or neglect of possible cyber-attacks engenders incomplete or inadequate models of (offline) terrorism.

A third feature common to much terrorism research is a prioritisation of the issue of responding to terrorism and a widespread sense that scholars working in this field should contribute to the formulation of policies for dealing with its threat to the state and its citizens (Jackson *et al* 2011: 14-15). The possibility of cyberterrorism, we suggest, throws up additional questions in this area too. In the first instance, there is, of course, considerable variation across legal definitions of terrorism which differ markedly between countries. As cyberterrorism is very rarely separated out within legal frameworks - being typically approached simply as one type of terrorism - particular legal settings are therefore central to determining whether any act might be treated as an example of cyberterrorism. One recent comparison (Hardy 2011; Hardy and Williams, forthcoming), for example, identified marked differences in this context between the UK, Canada, Australia and New Zealand. In all of these countries but Canada, a cyber-attack on non-essential infrastructure could be prosecuted as terrorism. Of these four, moreover, only New Zealand has in place a requirement that an attack be likely to endanger life.

A second issue relating to response is the diversity of perspectives on the significance of the threat posed by cyberterrorism more generally (see Jarvis *et al* 2014). On the one hand, there are those who argue that cyberterrorism is both potentially appealing to terrorists and a threat to national security (Collin 1997; Denning 2002). The second view - more common within recent discussion - is that the threat of cyberterrorism has been overdramatized by media and political elites to create a nightmarish scenario which does not represent the real existence of a threat. Thus, Conway (2002, p. 11) for instance, argues that cyberterrorism merely neatly merges two of today's biggest fears – technology and terrorism. Clearly, such discussions are impacted by definitional issues. If, for example, we adopt a broader definition of cyberterrorism that encompasses any use of computers and the Internet by terrorists, then the perceived threat of 'cyberterrorism' automatically increases given the greater feasibility of such activities (see, for example Jarvis *et al*, forthcoming; Weimann, 2006; Conway, 2002).

While debates of this kind have their importance for terrorism research, so do more contemporary constructivist explorations of the discursive imaginaries at play in this latest incarnation of the terrorism threat. Such debates fit more easily with the sympathies of many associated with Critical Terrorism Studies than they do with the problem-solving, policy-driven approach characteristic of alternative forms of terrorism research. For example, Cavelty demonstrates how cyberterrorism is an amalgamation of hyperbole-inspired fear constructed around tropes of randomness, incomprehensibility and uncontrollability (Cavelty, 2007, p. 29). Research of this kind offers a different way of thinking about cyberterrorism that explores the use of language in the framing of threats; examines the intertextuality of constructions of cyberterrorism; questions what discourses do in terms of informing response and action in this context; and, allows scholars of Terrorism Studies to think more broadly about who or what benefits from constructions of the cyberterrorism threat (see, Jarvis *et al*, forthcoming).

As this discussion suggests, activities potentially readable as cyberterrorism throw up considerable challenges for longstanding debates around definition, threat, and response within terrorism research. Discourses around cyberterrorism, moreover, pose interesting new research avenues for constructivist work typically associated with Critical Terrorism Studies. In the following, we turn now to the value of a related field of enquiry - Peace and Conflict Studies - for engaging with such issues. In so doing, we ask whether Terrorism Studies is best, uniquely, or even appropriately positioned to engage with these questions.

Peace and Conflict Studies and Cyber-Threats

As there are difficulties of discussing 'Terrorism Studies' as a unitary discipline, so too does 'Peace and Conflict Studies' (PCS) represent a heterogeneous field of enquiry. It is a field, moreover, that contains within it a diverse range of normative agendas, ontological and epistemological standpoints, and research goals. Although beyond the scope of this chapter to provide an overview of the PCS research agenda, this section seeks to highlight broad features therein which are indicative of this field's capacity and limitations in relation to the analysis of cyber-security issues.

In the broadest sense, PCS is interested in the identification, diagnosis and remedy of conflict and its causes (Galtung, 1996, p. 1). Here, a commitment to investigate the absence of 'peace' within disciplinary and geographical spaces is connected to a critique of narrow and established approaches to violence and a sympathy toward 'trans-disciplinary' and international research (Galtung, 1996, p. 1). This commitment is reflected in research that draws upon disciplines such as Gender Studies, Economics, and Psychology to further understanding of complex intertwined issues (Mayor, 1995; Barbieri, 1996; Tint and Sarkis, 2013).[2] For Terrorism Studies, the embrace of multi-disciplinarity is arguably a more recent development, coming, in part, as a result of criticisms landed against orthodox terrorism studies and its apparent Western-centrism (Chomsky and Herman, 1979; Herman and O'Sullivan, 1989; Jackson *et al* 2011, p.38-39): criticisms that contributed to the formation of the aforementioned CTS research project. The multidisciplinary and international research focus of PCS, coupled with the infancy of cyber-security issues and discourses, gives researchers a golden opportunity to shape debate in this area. Cyber-security concerns are almost always international in nature, and one also only needs to take a cursory glance at many of these to see potential contributions from a multitude of disciplines, including the Computer Sciences, Law, and Politics. Projects with this approach have already begun to emerge[3] and future researchers will need to continue to strive to form and strengthen partnerships with colleagues across disciplinary and national borders where requisite knowledge may not be limited to one institution or discipline.

Linked to this embrace of internationalism is a twofold problem upon which PCS and Terrorism Studies may be able to shed light. This is, first, the appropriateness of the current state-centric international system for dealing with issues of cyber-security; and, second, the

[2] In addition to these sorts of publications several dedicated multidisciplinary intuitions exist for the study of peace, see: The Institute for Economics & Peace, http://economicsandpeace.org/ and The "Gender, Conflict and Peacebuilding" Research centre at PRIO led by Torunn Tryggestad, http://www.prio.no/Projects/Project/?x=770.

[3] See: The Cyberterrorism Project (2014) www.cyberterrorism-project.org.

question of how international cooperation can be encouraged to create a more genuinely international response to such a diffuse problem with little regard for state borders. Taking the first aspect of this problem, we might look to PCS for ways to empower non-traditional security actors and bring others into the fore as part of a genuine effort to cooperate in understanding, managing or even reducing online threats. For example, PCS research into the impact of non-governmental agencies (see: Richmond and Carey, 2005; McDermott, 1998) in peacebuilding operations and humanitarian intervention could yield useful insight into forming effective coalitions in the pursuit of shared cybersecurity goals. Although it would be a gross oversimplification to suggest these two scenarios can be directly compared, this kind of research experience could be useful in efforts to get government, public institutions, the private sector, academia, and the general public working more cohesively on some of the most pressing cyber-security issues.

Alongside the challenge of extended engagement is the question of how to bring states themselves closer together on the topic of cyber-security. It is often said, by those in government and outside of it, that the nation state cannot solve the problems of cyber-security alone. As the UK's recent Cyber Security Strategy (2011, p.22) put it, "though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace". The result of this has been a number of initiatives and partnerships aimed at bringing international governments closer together (European Convention on Cybercrime 2001), creating stronger partnerships with business and industry (Cyber Security Information Sharing Partnership 2013), and educating the average user on Internet safety (Stay Safe Online.org 2014). However, as with elsewhere, the success of such initiatives is a matter of much debate; in particular those agreements that purport to establish functioning cooperation between states. For example, Micheal Vatis acknowledges the significance of the European convention on Cybercrime, that it 'represents the most substantive, and broadly subscribed, multilateral agreement on cybercrime in existence today [...] it offers a relatively comprehensive approach to harmonizing national legislation to address cybercrime'. However, focusing on these headlines misses the numerous problematic details such as a lack of signatories outside Europe, the lack of Russia and China's involvement and how 'the Convention also allows Parties to refuse to assist in many instances where assistance would conflict with domestic law or, notably, where a country claims that providing assistance would prejudice its sovereignty' (Vatis, 2010, pp. 221-222). Thus, if inter-state cooperation remains a desirable end in the realm of cybersecurity, analysts here might benefit considerably from the history of engagement with non-traditional security actors within PCS and (to a lesser extent) terrorism research.

Earlier in this chapter we argued that cybersecurity concerns throw up definitional challenges for terrorism research. Questions of definition have, of course, raged within PCS, too, not least in the minimalist/maximalist debate over this field's appropriate remit. As such, the typology of 'direct', 'structural', 'cultural' and other violences provided by Galtung - and developed by others (see, for example: Christie, 1997; Galtung, 1969, 1985, 1990; Galtung and Höivik, 1971; Christie, 1997) - may offer resources for assessing the stakes and parameters of more contemporary debate around the nature and limits of cyberterrorism. Thus, where Galtung (1985: 145) argued, "Peace Studies should cover both" direct and structural violences, in order to move, "from prevention and control of war to the study of peaceful relations in general" (1985, p. 145), similar advice might be appropriate for the contested nature of 'cyberterrorism', not least given the challenges thrown up by thinking through violence and harm in this context. In other words, perhaps the distinction between terrorist attacks using cyber-technology (narrow approaches to 'pure' cyberterrorism), and more mundane uses of the Internet by terrorist organisations (broader approaches), becomes less appropriate once we move beyond limited conceptions of violence. Moreover, given the lack of traceable - or (in the case of botnets) even obvious agency - within cybersecurity challenges, perhaps the relaxation of criteria of intentionality within broader conceptions of violence might also be useful for understanding phenomena such as cyberterrorism.

Whilst PCS therefore has potential resources for the analysis of contemporary issues (real or constructed) such as cyberterrorism, there are challenges here as well. Important amongst these, is the problem-solving nature of much peace research with its normative emphasis on 'peace-keeping' and 'peace building' (Toros and Tellidis, 2013) might render critical engagement with discourse around cybersecurity more difficult than in other domains. This is, not least, because of the challenges of accessing accurate, reliable information in this area in such a way as to avoid reproducing governmental understandings of threats, events and vulnerabilities. This is not, of course, a new debate, with accusations that peace researchers had become more closely aligned with powerful elites being levelled against the discipline already during the late 1960s and early 1970s (Eide, 1972). Indeed, Matti Jutila, Samu Pehkonen and Tarja Väyrynen go as far as to talk about the discipline's 'decline' arguing that it needs to take heed from the critical turn in Security Studies and reinvent itself as Critical Peace Research in order to 'revitalise' a discipline which is 'barely responding to any external stimulus' (Jutila, Pehkonen, Väyrynen, 2008, p. 631).

This returns us, finally to the value of recent interest in CTS, and in particular constructivist critiques of terrorism that have succeeded in problematising sedimented understandings of terrorism, terrorists and terrorist attacks. Work in this area has opened up space for a questioning of counter-terrorism measures as well as debate around the politics of labelling and threat construction. Studies into cyberterrorism, we argue, should harness the normative appeal of the most radical strands of PCS and CTS research by concentrating on the critique of knowledge claims and the policy frameworks they both support and derive from. This should not, however, mark the end of policy-relevant research in this area, or beyond.

Conclusion

Underpinning this chapter is a view of Terrorism Studies and Peace and Conflict Studies as sharing two characteristics. First, both of these fields - as with all fields of enquiry - are constantly in flux and evolving. Although it is possible to point to the endurance of particular research questions, agendas, theories and methods within each over time, both have changed in the past and will do so again in the future. Second, both of these fields are also heavily contested, and subject to internal debate over their core concepts and purposes. They are also, moreover, influenced by debates and developments from 'outside' their borders: empirical as much as scholarly. As argued above, cyberterrorism does indeed pose challenges for established accounts or conceptions of these fields, but it is far from alone in so doing, and we need also caution against essentialising scholarly paradigms and pursuits that are both porous and dynamic.

With these caveats in mind, our argument in this chapter is that activities that might be described as cyberterrorism pose challenges for scholars interested in each of these areas. In relation to terrorism research, potential security threats such as hacking or online disruption prompt reconsideration of definitional issues at the heart of this enterprise requiring a thinking again of the meaning and importance of categories such as 'violence' which recur throughout established understandings of terrorism. If we are willing to include such activities under the heading 'terrorism', they also, moreover, throw up research agendas and questions on subsidiary debates, including around the causes of terrorism more broadly. As suggested above, established models relating to threat and its drivers might be inappropriate once we expand our conception of what constitutes terrorism. Cyber-activities also pose questions for existing policy proscriptions and frameworks in relation to counter-terrorism. Whilst there might be some broad continuity between the offline and online worlds here (for example the need for international cooperation), there also exist potential particularities in the latter. These include technological particularities - how to prevent viruses, hackers and so forth - but extend beyond this to include such issues as the (cyber)strategic cultures of different states and other actors.

The chapter's final section identified potential value for analysing cyberterrorism within the development and successes of research associated with Peace and Conflict Studies. We argued that this field's international and interdisciplinary focus speaks directly to the nature of contemporary cybersecurity challenges. As, we suggested, does previous conceptual work therein on categories including violence and peace. Thus, research in this tradition - as well as discursive analyses speaking to constructivist work within Critical Terrorism Studies - has real potential for furthering our understanding of 'cyberterrorism' and its significance within contemporary political existence.

Bibliography

Arizona Department of Public Safety (2011) DPS Victim of Cyber Attack, *azdps.com*, http://www.azdps.gov/Media/News/View/?p=316, (accessed 19/01/2014).

Badey, T. (1998) 'Defining International Terrorism: A Pragmatic Approach', *Terrorism and Political Violence* 10 (1), pp. 90-107.

Barbieri, K. (1996) 'Economic Interdependence: A Path to Peace or a Source of Interstate Conflict?', *Journal of Peace Research*, 33 (1), pp. 29-49.

Beaumont, C. (2008) 'Bill Gate's dream: A computer in every home', *The Telegraph*, http://www.telegraph.co.uk/technology/3357701/Bill-Gatess-dream-A-computer-in-every-home.html, (accessed 18/01/2014).

Cavelty, M. (2007) 'Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology and Politics,* 4 (1), pp. 19-36.

Chen, T. M., and Davis, C. (2008) *An Overview of Electronic Attacks*, pp. 532 – 553.

Chomsky, N., and Herman, E. (1979) *The Political Economy of Human Rights, Volume I: The Washington Connection and Third World Fascism*. Nottingham: Spokesman.

Christie, D. J. (1997) 'Reducing Direct and Structural Violence: The Human Needs Theory', *Peace and Conflict: Journal of Peace Psychology* 3 (4), pp. 315-332.

Collin, B. C. (1997) ‘The Future of Cyberterrorism’, *Crime and Justice International*, 13 (2), pp. 15-18.

Conway, M. (2004) ‘Cyberterrorism: Media Myth or Clear and Present Danger?’, in J. Irwin (ed.) *War and Virtual War: The Challenges to Communities*. Amsterdam/New York: Rodopi, pp. 79-98.

Conway, M. (2011) ‘Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur’, *Viewpoints: Privacy and Security* 54 (2), pp. 26-28.

Conway, M. (2002) ‘Reality Bytes: Cyberterrorism and Terrorist ‘Use’ of the Internet’ *First Monday* 7 (11).

Cox, R. (1981) ‘Social Forces, States and World Orders: Beyond International Relations Theory’, *Millennium: Journal of International Studies* 10 (2), pp. 126-155.

Cyber Security Information Sharing Partnership (2013), https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security, (accessed 05/02/2014).

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 31/08/2012).

Easson, J. and Schmid, A. (2011) ‘Appendix 2.1: 250-plus Academic, Governmental and Intergovernmental Definitions of Terrorism’, in A. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. Abingdon: Routledge, pp. 99-157.

Eide, A. (1972) ‘Dialogue and Confrontation in Europe’, *Journal of Conflict Resolution* 16 (4), pp. 511–22.

Farwell, J. P., Rohozinski, R. (2011) ‘Stuxnet and the Future of Cyber War’, *Survival*, 53 (1), pp. 23-40.

Galtung, J. (1969) ‘Violence, Peace, and Peace Research’, *Journal of Peace Research* 6 (3), pp. 167-191.

Galtung, J. (1985) ‘Twenty-Five Years of Peace Research: Ten Challenges and Some Responses’, *Journal of Peace Research* 22(2), pp. 141-158.

Galtung, J. (1996) *Peace by Peaceful Means*. London: Sage.

Galtung, J. (1990) ‘Cultural Violence’ *Journal of Peace Research* 27 (3), pp. 291-305.

Galtung, J. and Höivik, T. (1971) ‘Structural and Direct Violence: A Note on Operationalization’, *Journal of Peace Research* 8 (1), pp. 73-76.

Giacomello, G. (2004) “Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism” *Studies in Conflict and Terrorism* 27 (5), pp. 387-408.

Gordon, S. and Ford, R. (2002) Cyberterrorism? *Computers and Security* 21 (7), pp. 636-647.

Græger, N. (1996) ‘Environmental Security?’, *Journal of Peace Research* 33 (1), pp. 109-116.

Hardy, K. (2011) ‘WWWMDs: Cyber-attacks against Infrastructure in Domestic Anti-Terror Laws’, *Computer Law & Security Review* 27, pp. 152-161.

Hardy, K. and Williams, G. (forthcoming) 'What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism', in T. Chen, L. Jarvis, and S. Macdonald (eds.) *Cyberterrorism: Understanding, Assessment, Response*. New York, NY: Springer.

Herman, E. and O'Sullivan, G., (1989) *The Terrorism Industry: The Experts and Institutions that Shape our View of Terror*. New York: Pantheon Books.

Holt, T. (2012) 'Exploring the Intersections of Technology, Crime, and Terror' *Terrorism and Political Violence*, 24 (2), pp. 337-354.

House of Lords (2008) Judgments - Mckinnon V Government of The United States of America and Another, Opinion of the Lords of Appeal For Judgement in the Cause, http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm, (accessed 21/03/2014).

Institute for Economics & Peace (2014) http://economicsandpeace.org/, (accessed 01/02/2014).

Jackson, R., Jarvis, L., Gunning, J., Breen Smyth, M. (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave Macmillan.

Jarvis, L. (2009) 'The Spaces and Faces of Critical Terrorism Studies', *Security Dialogue* 40 (1), pp. 5-28.

Jarvis, L., Macdonald, S., Nouri. L. (2014) 'The Cyberterrorism Threat: Findings from a Survey of Researchers', *Studies in Conflict and Terrorism* 37 (1), pp. 69-90.

Jarvis, L. & Macdonald, S. (forthcoming, a) 'Locating cyberterrorism: How Terrorism Researchers Use and Regard the Cyber Lexicon', *Perspectives on Terrorism*.

Jarvis, L. & Macdonald, S. (forthcoming, b) 'What is Cyberterrorism? Findings from a Survey of Researchers', *Terrorism and Political Violence.*

Jarvis, L., Nouri, L. & Whiting, A. (forthcoming) 'Understanding, Locating and Constructing Cyberterrorism', in T. Chen, L. Jarvis and S. Macdonald (eds.) *Cyberterrorism: Understanding, Assessment, Response*. New York, NY: Springer.

Jutila, M., Pehkonen, S., Väyrynen, T. (2008) Resuscitating a Discipline: An Agenda for Critical Peace Research, Millennium – Journal of International Studies, 36(3), p. 623-640.

Kennedy, R. (1999) 'Is One Person's Terrorist Another's Freedom Fighter? Western and Islamic Approaches to "Just War" Compared', *Terrorism and Political Violence* 11 (1), pp. 1-21.

Kizza, J. M. (2014) *Computer Network Security and Cyber Ethics*. Jefferson, NC: McFarland & Company.

Malik, O. (2000) *Enough of the Definition of Terrorism*. London: Royal Institute of International Affairs.

Mayor, F. (1995) 'How Psychology can Contribute to a Culture of Peace', *Peace and Conflict: Journal of Peace Psychology*, 1(1), pp. 3-9.

McDermott, A. (1998) 'The UN and NGOs: Humanitarian interventions in future conflicts', Contemporary Security Policy, 19(3), pp. 1-26.

PRIO (2014) Gender, Conflict and Peacebuilding Research, http://www.prio.no/Projects/Project/?x=770, (accessed 01/02/2014).

Neumann, P. (2009) *Old and New Terrorism.* London: Polity Press.

Ranstorp, M. (2009) 'Mapping Terrorism Studies After 9/11, in R. Jackson, M. B. Smyth and J. Gunning, eds., *Critical Terrorism Studies: A new research agenda*. Abingdon: Routledge, pp. 13-33.

Richmond, O. P., Carey, H. F. (2005) *Subcontracting Peace: The challenges of NGO peacebuilding*. Aldershot: Ashgate.

Rid, T. (2013) *Cyber War Will Not Take Place*. London: Hurst & Company

Sanchez, Y. W., Haldane, M., McKinnon, S. (2011) Arizona DPS system hacked: LulzSec group claims responsibility, *azcentral.com*, http://www.azcentral.com/news/articles/2011/06/23/20110623lulzsec-hacks-into-arizona-dps-system-abrk23-ON.html?nclick_check=1, (accessed 19/01/2014).

Schmid, A. and Jongman, A. (1988) *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*. New York, NY: Transaction.

Schmid, A. (2011) 'The Literature on Terrorism', in A. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. Abingdon: Routledge, pp.457-474.

Silke, A. (2004) 'An Introduction to Terrorism Research', in A. Silke (ed.) *Research on Terrorism: Trends, Achievements and Failures*. Abingdon: Routledge. pp.1-29.

Silke, A. (2009) 'Contemporary terrorism studies: issues in research', in R. Jackson, M. B. Smyth and J. Gunning, eds., *Critical Terrorism Studies: A new research agenda*. Abingdon: Routledge, pp. 34-48.

Stay Safe Online.org (2014) https://www.staysafeonline.org/, (accessed 05/02/2014).

Stump, J. and Dixit, P. (2013) *Critical Terrorism Studies: An Introduction to Research Methods.* Abingdon: Routledge.

Symantec (N.D.) 'Duqu: The Precursor to the Next Stuxnet', *Symantec.com*, http://www.symantec.com/en/uk/outbreak/?id=stuxnet, (accessed 19/01/2014)

Tellidis I. and Toros H. (2013) 'Editior's Introduction: Terrorism and Peace and Conflict Studies: Investigating the Crossroad' *Critical Studies on Terrorism* 6 1, pp.1-12.

Telegraph Reporters (2013) 'Anonymous hacktivists target MIT websites over Aaron Swartz suicide', *The Telegraph*, http://www.telegraph.co.uk/technology/news/9800257/Anonymous-hacktivists-target-MIT-websites-over-Aaron-Swartz-suicide.html, (accessed 21/03/2014).

The Cyberterrorism Project (2014) www.cyberterrorism-project.org, (accessed 01/02/2014).

The European Convention on Cybercrime (2001) http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, (accessed 06/02/2014).

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm,, A. M., Vihul, L. (2008) 'Cyber Attacks Against Georgia: Legal Lessons Identified', Cooperative Cyber Defence Centre of excellence, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, (accessed 21/03/2014), pp. 1-45.

Tint, B., Sarkis, C. (2013) ‘And justice for all? Gender based violence and international law in the African context’, *Africa Peace and Conflict Journal*, 6(1), pp. 43-58, http://www.apcj.upeace.org/issues/APCJ_Vol_6.1_June%202013_Final.pdf, (accessed 01/02/2014).

UK Cyber Security Strategy (2011) https://www.gov.uk/government/publications/cyber-security-strategy, (accessed 01/04/2014).

Vatis, M. (2010) 'The Council of Europe Convention on Cybercrime', in *Proceedings of A Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press, pp. 221-222.

Weimann, G. (2006) *Terror on the Internet: The New Arena the New Challenges*. Washington, DC: United Institute of Peace Press.

Weimann, G. “Cyberterrorism: How Real is the Threat?” *United States Institute of Peace Special Report 119* (2009), http://www.usip.org/publications/cyberterrorism-how-real-threat (accessed May 15, 2013.

Weimann, G. (2006) ‘Virtual Disputes: The Use of the Internet for Terrorist Debates’, *Studies in Conflict & Terrorism* 29 (7), pp. 623-639.

Zolkipli, M. F., Jantan, A. (2011) ‘A Framework for Defining Malware Behaviour Using Run Time Analysis and Resource Monitoring’, in Zain, J. M., bt Wan Mohd, W. M., El-Qawasmeh, E. (Eds.) *Software Engineering and Computer Systems, Second International Conference ICSECS 2011, Kuantan, Pahang, Malaysia, June 2011 Proceedings, Part 1*, pp. 199-209.