The Cyberterrorism Threat:

Findings from a Survey of Researchers

Abstract

This article reports on a recent research project exploring academic perspectives on the threat posed by cyberterrorism. The project employed a survey method, which returned 118 responses from researchers working across 24 different countries. The article begins with a brief review of existing literature on this topic, distinguishing between those concerned by the imminent threat of cyberterrorism, and other, more sceptical, views. Following a discussion on method, the article's analysis section then details findings from three research questions: (i) Does cyberterrorism constitute a significant threat? If so, against whom or what?; (ii) Has a cyberterrorism attack ever taken place?'; and, (iii) What are the most effective countermeasures against cyberterrorism? Are there significant differences to more traditional forms of anti- or counter-terrorism? The article concludes by reflecting on areas of continuity and discontinuity between academic debate on cyberterrorism and on terrorism more broadly.

Key words: Cyberterrorism, Terrorism, Terrorism Studies, Threat, Risk, Survey, Questionnaire.

Introduction

This article presents original findings from a recent research project focusing on understandings of cyberterrorism amongst the global research community. Its objective is to build upon and complement earlier studies that were integral to mapping the contours of academic research on terrorism. Foremost amongst these, of course, was Schmid and Jongman's *Political Terrorism*,[1] which included the use of a questionnaire, "…mailed to some two hundred members of the research community in the field of political terrorism in 1985".[2] Silke's edited *Research on Terrorism* offers a more recent, but related, review of the state of terrorism research, including of the major methodological techniques employed in this field,[3] and dominant research trends and interests.[4] More recently still, Magnus Ranstorp and Silke published post-9/11 accounts of the primary concerns and limitations of contemporary

terrorism research.[5] Studies such as these were important in consolidating what was known and understood about terrorism by the research community at particular moments in time. The research underpinning this article seeks to do something similar for one of the newest incarnations or constructions of this form of political violence: cyberterrorism.

The article draws on responses to a survey completed by 118 researchers working in 24 different countries across six continents. It focuses on their views on three sets of issues: first, whether cyberterrorism constitutes a significant threat and, if so, against what referent; second, whether a cyberterrorism attack has ever taken place; and, third, the most effective countermeasures against cyberterrorism and whether these differ significantly from more traditional forms of counterterrorism. The article proceeds in four sections. It begins with a review of the relevant academic literature. As a comparatively recent addition to the rubric of terrorism, scholarship on the specific threat posed by cyberterrorism remains relatively limited. Despite this, a spectrum of perspectives on this threat's severity and imminence are identifiable, with the debate becoming increasingly polarised since the coining of this then-neologism in the 1980s. The second section details the methodology of the research, reflecting in particular on the sampling strategy employed and distribution of respondents. The third section describes and analyses the research findings. It outlines the diversity of responses received, arguing that these are the product of conceptual, definitional and inferential disagreements. Finally, the article concludes by pointing to the importance of these findings for examining the relations between cyber- and other forms of terrorism.

The Cyberterrorism Threat: Academic Debate

The extent to which cyberterrorism poses a genuine security threat to any form of referent object (a state, a corporation, citizens, and so on) is amongst the most contested of topics within this research area. In part, this is a product of terminological dispute. More expansive

conceptions of cyberterrorism as any form of online terrorist activity unsurprisingly tend to be associated with a higher estimated probability of the threat's materialisation than do more restrictive accounts.[6] At the same time, as detailed further below, competing threat assessments remain even if we restrict our focus to narrower understandings of this concept (described, by some, as 'pure cyberterrorism'[7]), such as the following:

> 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. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[8]

This section sets out two contrasting perspectives within debate on the threat of cyberterrorism when approached in this relatively narrow way: First, a 'concerned' view that sees cyberterrorism as constitutive of a genuine security threat; and, second, a 'sceptical' view of cyberterrorism as little more than hyperbolic media construction. It goes on to explain that sceptical accounts which advance the latter perspective frequently contrast cyberterrorism *per se* with other terroristic usages of information technology, which are often seen as posing a significant threat and requiring, as such, greater attention.

Assessments of cyberterrorism as a significant, and pressing, security challenge were particularly prominent in early debate on this phenomenon, and remain so within media and political discourse today.[9] Amongst its better known advocates has been Barry Collin of the US Institute for Security and Intelligence - the individual responsible for coining the term in the 1980s. As Collin argued in 1997, "make no mistake, *the threats are real today*".[10] This, for Collin, is because cyber-attacks now pose similar destructive capacity to traditional physical

assaults, including the prospect of multiple casualties and considerable publicity. Potential threats he identifies include the contamination of food products through interference with manufacturing processes, and the interception of air traffic control systems to engender fatal collisions.[11]

Collin is not alone in hypothesising such scenarios. Dorothy Denning - perhaps the highest profile scholar in this field - suggests that while "cyberterrorism has been mainly theoretical to date; it is something to watch and take reasonable precautions against".[12] Cronin notes that globalisation has offered terrorist organisations access to the technologies required for cyberterrorism as well as the wider audiences and recruitment potentialities often attributed to this socio-political process.[13] Gabrielle Weimann identifies five factors that render cyber-attacks appealing to terrorists. These include comparatively lower financial costs; the prospect of anonymity; a wider selection of available targets; the ability to conduct attacks remotely; and, the potential for multiple casualties.[14] Furnell and Warren argue similarly that, "from the perspective of someone wishing to cause damage, there is now the capability to undermine and disable a society without a single shot being fired or missile being launched".[15] This, they add, "enables simultaneous attacks at multiple nodes worldwide without requiring a large terrorist infrastructure necessary to mount equivalent attacks using traditional methods"[16]. Related utility-maximisation arguments suggest it is inevitable terrorists will employ cyber-weaponry if benefits from so doing are likely,[17] and/or if an enemy employs computers and networks as security tools, or maintains dominance in this area.[18] Such thinking is integral to the 'electronic pearl harbour'[19] scenarios which dominate much of the non-academic attention cyberterrorism receives.

Within these discussions of the threat posed by cyberterrorism, two issues in particular are frequently invoked: the vulnerability of Critical Information Infrastructures (CIIs), and contemporary dependences on information technologies.[20] Although inconsistently understood,

CIIs refer to those services that would have a debilitating impact on national security and economic and social welfare if destroyed.[21] The vulnerability of CII's is linked, *inter alia*, to their connection to the Internet, the infrequency and high cost of software updates, and the sporadic implementation of attack detection and prevention systems which can slow services down.[22] One of the main challenges involved in CII protection is the problem of attribution, and the challenge of locating responsibility for attacks. It is difficult, for example, to be certain whether a system's failure is accidental or due to a malicious attack.[23] Unlike a physical attack in which action and effect are often near-simultaneous, the consequences of a cyber-attack may not be noticeable for a considerable amount of time. That it is also possible to disguise one's identity on the Internet, using such means as 'botnets',[24] further complicates the ability to identify from where an intrusion has derived. These challenges become more acute still when we recognise the constant increase in the complexity of information systems, and the gap that has opened with capabilities for mitigating emergent problems.[25]

Although concerns such as the above dominated early debate in this area, more recent scholarship has witnessed the arrival of dissenting voices. Amongst these, the cyberterrorism threat is viewed as little more than a speculative (typically, media) fantasy; an outgrowth, for some, of the need to replace newly-redundant Cold War security imaginaries in the 1980s and 1990s. As an aggregate of terrorism, technology and the unknown, constructions of cyberterrorism - and related risks - are viewed here as parasitic upon - and multipliers of - fears over contemporary dependences on information systems.[26] Thus, authors such as Hansen and Nissenbaum deploy securitization theory in an effort to analyse and unravel cyber-security discourses.[27] Doing so is crucial, they argue, as a means of contesting security claims in this area which appear either self-evident or unchallengeable due to their framing in technical, specialised language. As they put it, "cyber securitizations are particularly powerful precisely

because they involve a double move out of the political realm: from the politicized to the securitized, and from the political to the technified"[28].

One of the most sustained deconstructions of the cyberterrorist threat is provided by Maura Conway.[29] Terrorists, she notes, are routinely dehumanised, while technology is associated with a lack of control over the world. The combination of these spectres is, therefore, ripe for the establishment of worst case scenarios in which entire societies are 'cut off' and thus rendered vulnerable by the 'evil' of terrorists.[30] Conway suggests that this construction of worst-case scenarios is a product of media as much as political discourse:

> The media plays a key role in the shaping of these assumptions, constructing these scenarios, and generally informing us as to what is "out there". It is thus a prime mover in the process of defining security […] with the aid of the mass media, cyberterrorism came to be viewed as the 'new' security threat *par excellence.*[31]

Critics of the constructions of threat that surround cyberterrorism forward two further arguments. First, these discourses are not necessarily driven by - and do not necessarily correspond with - empirical realities. Bendrath, for example, has mapped dramatic changes in US perceptions of the cyber world and the oscillation between cyberterrorism and cyberwarfare as the bogeymen *du jour* irrespective of concrete, 'real world', developments.[32] Conway points similarly to the impact of intangibly related events - such as 9/11 - to public policy on cybersecurity, where, for example, "the Council of Europe rushed through its Convention on Cybercrime in response to the attack".[33] Second, these authors also highlight the internalisation of these discourses by publics or users of ICT. For instance, "75% of global internet users believe 'cyberterrorists' may, soon inflict massive casualties on innocent lives by attacking corporate and governmental computer networks" while 45% of users agreed completely that "computer terrorism will be a growing problem".[34] Whether accurate or

otherwise, in other words, these discourses have real world impacts across different social strata.

One of the reasons offered for the argument that 'pure' cyberterrorism constitutes a relatively less significant risk is that cyber-attacks are comparatively unattractive to terrorists. In addition to the fact that they lack theatricality,[35] Giacomello, for example, offers a cost/benefit analysis of cyberterrorism to argue that traditional methods of terrorism and weapons remain more effective at killing people, and thereby growing the desired political capital.[36] These accounts frequently contrast the possibility of cyber-attack with other terrorist uses of information technology which are regarded as a pressing and largely overlooked threat. Attention, then, should be given to the wider use of the Internet by terrorists, including for "recruitment, financing, networking information gathering [and] sharing information"[37] all of which enhance the efficiency and reach of terrorist groups.[38] On this view, the nightmare scenarios associated with cyberterrorism should be replaced by a focus on this broad range of activities, with a range of political, policing and civil society stakeholders having a role in countering them.[39]

Within this debate on the level of threat posed by cyberterrorism, issues of spatiality and jurisdictional responsibility are also prominent, not least over whether the issue is better understood in national or international terms. Yould, for example, argues that the borderless nature of cyber-security challenges, and the globally connected nature of networks and infrastructure, "undermine – or, at the very least, render contingent – the sovereignty and significance of the nation-state"[40]. Similarly, Cavelty argues that "the vulnerabilities of modern societies – caused by their dependence on a spectrum of highly interdependent information systems – have global origins and implications"[41]. Other studies go further still, questioning whether security frameworks and organisations are at all appropriate to tackle threats in cyberspace[42]. Hardy identifies a number of problems in responding to cyberterrorism from a

national security perspective arguing that differences in the understanding and legal definition of terrorism have caused vast inconsistencies of prosecution across Western democracies. For Hardy, this is rooted in the fact that each country has applied its own understanding to this threat[43] and that state-led approaches "fail to recognise the nature of the globally interdependent network environment and the leading role of the private sector in this domain"[44].

Research Methodology

The above overview demonstrates two things, in particular, about the current state of scholarship on the threat posed by cyberterrorism. First, and most obviously, there is considerable diversity of perspective amongst contributors to debate in this area. As with debate on the extent to which terrorism more widely poses a current threat, it is difficult to identify any consensus here.[45] Second, and in spite of these disagreements, it is possible to point to changes of emphasis and perspective in the time that has passed since the term 'cyberterrorism' was first coined. This should, perhaps, be expected given the dramatic geopolitical and technological developments that have taken place across the globe since the early 1980s.

As noted earlier, one of the aims of the research underpinning this article was to capture as fully as possible the current state of academic opinion - and debate - on the threat posed by cyberterrorism by use of a survey methodology. Employing a combination of closed and open-ended questions, the survey was distributed to over six hundred academics and researchers working on terrorism or cyberterrorism. The survey was distributed between June and November 2012, and employed a purposive sampling strategy to identify potential respondents. This strategy made use of four primary methods.

First, a targeted literature review was undertaken to identify researchers with a record of publishing on cyberterrorism within peer-reviewed journals, monographs, edited books, or other relevant literature. This task was completed using the main catalogue of the British Library and a total of 47 other online databases (including JSTOR, Oxford Journals online, SAGE journals online, Wiley Interscience, Springer Link, IEEE Xplore, Lecture Notes in Computer Science and Zetoc).[46] The search was limited to publications on or since January 1st 2004. To this was added a second set of potential respondents identified by their standing in the wider terrorism research community. Whilst these individuals may not directly have published on cyberterrorism, their expertise and knowledge of definitional, causal, and related debates on terrorism rendered their opinions relevant to this research. To this end, individuals that had authored an article in any of the following four major journals on terrorism since January 1st 2009 were added to the sample: *Studies in Conflict and Terrorism*, *Terrorism and Political Violence*, *Critical Studies on Terrorism*, and, *Perspectives on Terrorism*. Members of the editorial boards of these journals (as of August 1st 2012) were also added. The first two journals are widely recognised as the most prominent specialist outlets for publishing peer-reviewed research on terrorist violence.[47] As Silke argued in 2004, "Taken together - and bearing in mind their different publishers, separate editorial teams and largely separate editorial boards (though there is some overlap on this last) - the two journals can be regarded as providing a reasonably balanced impression of research activity in the field".[48] The latter two journals were included to take account of the extent to which terrorism research has expanded dramatically across the last ten years,[49] and become more hotly contested in the process.[50]

The third sampling technique was a 'snowball method' that included respondents identified to us by individuals who had already completed and returned the survey. And, finally, we employed targeted requests for respondents disseminated via the mailing lists of

two UK-based academic organisations: the Terrorism and Political Violence Association,[51] and the British International Studies Association Critical Terrorism Studies Working Group.[52]

This use of a purposive, non-probabilistic, sampling strategy was appropriate to the survey's aims.[53] Although the method cannot claim any statistical representativeness in relation to the terrorism research community, such a claim would be difficult to sustain whatever the sample given the contestable, fluid and porous nature of this population.[54] Researchers enter and leave this community according to the evolving nature of their research interests, and any effort to capture opinion therein can offer only a static snapshot of a dynamic phenomenon. In this sense, the sacrifice of representativeness in our study is justified given that no discernible, definitive, population can meaningfully be said to exist.

A second potential limitation derives from the nature of the academic process and its extended temporalities. By sampling, in part, according to authorship in this area (however contemporary the published work), this research may provide an already-dated snapshot of this community. Published work only reports on projects, and perhaps even research interests, that are now completed. Much of the newest research - in PhD theses, for instance - will not have entered print yet. By using multiple sampling methods - and especially the mailing lists of current research communities – this research attempted to mitigate these concerns. The possibility remains, however, that junior researchers, newcomers to the field and other groups may be underrepresented in our study.

With these caveats in mind, our survey generated a total of 118 responses from 24 countries spanning six continents. 41 (35%) of the 117 respondents who provided geographical information worked in the United States of America, and 31 (27%) in the United Kingdom. Australia accounted for 7 of our respondents (6%), and Canada 4 (3%). This weighting toward Anglophonic countries is unfortunate, but to be expected given that this replicates the geographical trends of terrorism research.[55] In terms of employment status, our sample was

divided as follows: Academic Staff (Permanent): 75 (64%); Academic Staff (Temporary): 16 (14%); Research Student: 9 (8%); Independent Researcher: 11 (9%); Retired: 2 (2%); and, None of the Above: 5 (4%). In relation to disciplinary background, finally, our sample broke down thus: Political Science/International Relations: 69 (50%); Psychology/Anthropology: 20 (15%); Engineering/Computer Science/Cyber 17 (12%); Law/Criminology: 15 (11%); Literature/Arts/History: 9 (7%); Independent Researchers/Analysts: 5 (4%); and, Economics/Business: 2 (1%).[56] That half of our sample were Political Scientists or International Relations scholars again resonates with earlier empirical studies of contributors to terrorism research.[57]

The survey's substantive questions focused on four broad categories of question. First, definitional issues in relation to cyberterrorism and terrorism more widely. Second, the threat posed by cyberterrorism. Third, issues of response and deterrence. And, fourth, respondent views of current research in this area, including the challenges facing scholars. This focus reflected the survey's overall ambition to investigate prominent contemporary concerns of the relevant academic community, and to chart parallels with related, earlier, studies of (non-) cyberterrorism research. In the following, this article turns to the findings of the survey and their importance in relation to the cyberterrorism threat.

Findings and Analysis[58]

Three questions in the survey were specifically designed to assess researcher perceptions on the threat posed by cyberterrorism. These provide the focus for the following discussion, and were articulated thus:

Question 10: In your view, does cyberterrorism constitute a significant threat? If so, against whom or what is the threat focused?

Question 11: With reference to your previous responses, do you consider that a cyberterrorism attack has ever taken place?

Question 12: In your view what are the most effective countermeasures against cyberterrorism? Are there significant differences to more traditional forms of anti- or counter-terrorism?

Each question provided a 'free text' boxes for respondents (alongside, in the case of question 11, a dropdown menu), in order to capture the widest and fullest range of responses. As demonstrated below, these responses have been used to generate qualitative and quantitative findings.

Question 10 - on the threat posed by cyberterrorism - was answered by 110 respondents to our survey (response rate: 93%). These responses were coded by a quinquepartite scale, the findings from which are contained in Chart 1:

[*Insert chart 1 here*]

In line with the academic literature detailed above, this question generated a diversity of responses. The majority of respondents - 58% - answered in the affirmative, although these identified a diverse range of referents (see Table 1). Most common were states or governments, especially, "certain high profile countries".[59] One respondent, for instance, identified "powerful states"[60]; another mentioned the US, Russia and China as targets.[61] The second most common answer was critical infrastructures: financial institutions;[62] transportation networks;[63] intelligence networks;[64] energy grids;[65] water systems;[66] agriculture;[67] and, emergency services.[68] Ten respondents stated that the threat is focussed on civilians and

individuals, and the same number stated that the threat is focussed on organizations, the private sector, corporations and/or the economy.

[*Insert table 1 here*]

That respondents were divided on both aspects of this question - the extent of threat posed, and the referent object - was a product of four factors. The first was the importance of particular understandings of 'threat'. This was especially so amongst those identifying critical infrastructures and computer networks as the focus of potential attacks. Thus, some respondents referred to entire economies, transport networks or energy systems being "at risk"[69], of society's capacity to function being crippled[70] and organisations being paralyzed,[71] and of daily life being seriously disrupted.[72] Others, in contrast, described this risk in terms of "disruption",[73] interruption,[74] and 'significant ramifications'.[75] A second factor was the logic by which such threats were articulated. Some respondents referred to the possible emulation of recent events - such as the Stuxnet attack in Iran - by terrorists.[76] Others, in contrast, framed this threat in the abstract, discussing, for example, the possibility of violence against people or property.[77] Third, part of this diversity was a product of competing conceptions of cyberterrorism. Replicating the trend noted in the literature review section, those willing to countenance a wider conception of cyberterrorism identified a range of possible threat scenarios extending beyond attacks on people, property or critical infrastructures and essential services. Four respondents referred to cyberterrorists threatening national security by obtaining sensitive intelligence and classified information.[78] Others referred to terrorists committing cybercrime, including obtaining individuals' bank details and accessing financial and other information from both public and private sector institutions.[79] One respondent understood

cyberterrorism to include online harassment[80] and another warned of cyberattacks being perpetrated to influence elections.[81]

Fourth, respondents' answers to this question also raised temporal issues. Thus, some negative responses were qualified with phrasing such as, "at the moment"[82] or "at present".[83] Others, meanwhile, were more equivocal, warning that cyberterrorism has the potential to become a significant threat, if it is not one at present. One respondent, for example, stated: "Cyberterrorism is a potential threat and a potentially significant one … [A]t the moment, cyberterrorism is not a threat but a risk".[84] Others still, stated that cyberterrorism is currently a significant threat because of what terrorists might do *in the future*:

> Yes. What has been done against the Iranian government recently could potentially be done against any government by any actors, and that is probably just the beginning.[85]

> Yes, but one that is not yet manifest because terrorists lack the skills to mount an effective attack.[86]

> It does. However, it is the future of the threat that truly counts and, I think, is really worrisome.[87]

The respondents that stated cyberterrorism does not constitute a significant threat offered three reasons to support their position. First, three respondents pointed to the fact that cyberterrorism (as they conceptualised this phenomenon) has never occurred.[88] One stated that we have "no precedent and few metrics" to assess the cyberterrorist threat.[89] Another said that "empirical evidence is almost non-existent", adding that hypothesised scenarios are often, "blue sky thinking".[90] Second, six respondents stated that terrorist organisations lack the capability to attack critical infrastructures and essential services.[91] Of these, two doubted whether terrorists will ever acquire this level of expertise,[92] while three others suggested that things might change in the future.[93] As one commented, "Non-state actors don't seem to have the know-how

(yet)".[94] Third, two respondents opined that terrorists lack any motivation to perpetrate cyberterrorist attacks.[95] As one explained:

> [C]yberterrorism lacks the heroic quality of e.g. a suicide bombing and thus has less appeal to potential terrorists. I think the self-image can be a very important factor in a radicalisation process, and in this sense cyberterrorist attacks do not fulfil this need to the extent that other forms of terrorism do.[96]

The other went on to suggest that what is significant is not the cyberterrorist threat itself, but the manner in which this threat has been articulated: "At present, it is not a significant threat. The hyperbolic inflation of its threat in public discourse and the potential ramifications for civil liberties is far more significant, in my view".[97] Other respondents expressed similar sentiments. One stated that cyberterrorism is a significant threat "because 'we' (officials, emergency and military personnel, media again, in the US) act and talk as though it is".[98] Another commented that cyberterrorism "is a threat if it is constituted as such by security discourse".[99] Views such as these clearly reflect the broadly constructivist position held by many of the sceptical scholars explored in the above literature review section.

Responses to question 11 - on whether a cyberterrorist attack had ever taken place - raised similar issues. Respondents were invited to select either "Yes" or "No" from a dropdown menu, with an additional free text box allowing further explanation. 113 respondents answered this question (response rate: 96%). Three of these selected neither "Yes" nor "No", explaining that they were unsure. As Chart 2 shows, of the remaining 110 respondents, remarkably 55 selected "Yes" and 55 selected "No".

[*Insert chart 2 here*]

When findings for this question are restricted to those respondents who had earlier stated that cyberterrorism *does* constitute a significant threat, only 42 of this sample of 63 (67%) believed an attack had yet taken place. This indicates the importance of deductive reasoning as well as inductive inferences in conceptions of current and future risks. As might be expected given the comparative novelty of cybersecurity threats, the past is not necessarily seen as a reliable guide to understanding the present or future.

Respondents who stated that cyberterrorist attacks had taken place offered a number of examples, listed in Table 2 below. The table uses the wording provided by respondents, with the authors' interpretation of the events contained in the footnotes.

[*Insert table 2 here*]

Some other respondents gave more general - and quite diverse - examples. These included: theft of monies to fund terrorist organisations;[100] the preparation of terrorist attacks;[101] calls for home-grown terrorism;[102] attacks against individuals that governments perceive as dissidents[103]; and, cyber espionage.[104]

The respondents that stated a cyberterrorist attack had not yet taken place did not explicitly dispute that any of the events in Table 2 had occurred. Rather, they typically provided reasons for doubting attacks such as these could constitute cyberterrorism. First, eight respondents invoked an actor-specific definition of cyberterrorsm, arguing that some of the highest profile cyberattacks to have taken place, such as Stuxnet and upon Estonia, were not terrorist because they were not perpetrated by non-state groups.[105] Some of these respondents explicated further, suggesting that attacks carried out by state actors are better understood as cyber warfare. Second, seven respondents said that high profile cyberattacks could not qualify as (cyber)terrorist because they had not resulted in violence against people or property.[106] As

one respondent explained: "no person has ever been killed or injured as the result of an attack executed by using weaponised computer code".[107] Third, four respondents argued that there is a distinction between cyberterrorism and cybercrime.[108] One of these argued that, whilst terrorists might commit cybercrime in order to facilitate terrorist activity, this does not render the criminal activity terrorist. On this view, there is a difference between: (a) cyberterrorism; and, (b) cybercrime committed for terrorist purposes (such as to raise funds)[109]. Another respondent argued that hacktivism must be distinguished from cyberterrorism[110], though two other respondents suggested that the activities of Anonymous render this distinction more problematic.[111] Fourth, four respondents stated that the cyberattacks that have occurred did not instil fear in a wider audience and/or were not carried out with an intention to generate such fear.[112] Absent this element of intimidation or coercion, these respondents said that cyberattacks do not constitute cyberterrorism. Lastly, three respondents said that those who have perpetrated attacks to date lacked the political or ideological motive necessary for the attack to qualify as (cyber)terrorist.[113]

As stated previously, the fact that a respondent believed that no cyberterrorist attack has ever occurred did not necessarily mean that cyberterrorism was not viewed as a significant threat. Chart 3 shows the responses to question 10 of those respondents that answered no to question 11. Interestingly, in spite of the perceived absence of any cyberterrorist attacks to date, a greater proportion of these respondents stated that cyberterrorism poses a significant threat than stated it does not (35% compared to 29%). Moreover, an additional 15% of these respondents stated that cyberterrorism may potentially or possibly become a significant threat.

[*Insert chart 3 here*]

The final question to be explored focused more explicitly on issues of vulnerability and response than of capability and intention. Here, respondents were asked to name the most effective countermeasures against cyberterrorism, and then to detail whether there are significant differences to more traditional forms of anti- or counter-terrorism. 93 responses were received (response rate: 79%), although some respondents only answered part of the question.

In response to the first part of the question, twelve countermeasures were identified by at least two respondents (see Chart 4). One - target-hardening - dominated our responses, with 35 respondents mentioning this mechanism. Some of these framed their comments quite generally, for example: "Enhanced IT security"[114] or "Technical security measures".[115] Others, in contrast, gave more specific suggestions including "Redundancies in various civilian and critical online systems"[116], "Firewalls",[117] "Closed secure networks",[118] "Keeping sensitive data in encrypted format"[119] and "Increases in biometric security systems".[120]

[*Insert chart 4 here*]

A number of other countermeasures were mentioned by only one respondent. These included: refraining from starting illegal wars;[121] switching our focus from non-state to state actors;[122] and, education and humanitarian aid.[123]

The four most common responses to the second part of this question - on the peculiarities of countering cyberterrorism - are detailed in Chart 5. 17 respondents (18%) argued that, whilst the methods employed might be different, countering cyberterrorism involves the same underlying strategies as other forms of terrorism. By contrast, 16 respondents (17%) believed there to be a significant difference with other forms of terrorism in that greater technical expertise is required to counter cyberterrorism. These two viewpoints are

not necessarily incompatible. Whilst one focuses on the underlying principles (prevention, protection, resilience, etc), the other focuses on what the application of these principles looks like in practice. This was summed up neatly by one respondent, who said "Yes, from technological point of view, not from ideological point of view".[124]

[*Insert chart 5 here*]

The 12 countermeasures listed in chart 4 were identified by a total of 60 respondents.[125] Of these, it is worth noting that 14 had said (in response to question 10) that cyberterrorism does not constitute a significant threat.[126] So, the majority of the respondents that did not regard cyberterrorism as a significant threat nonetheless identified countermeasures. There were two reasons for this. First, five of these respondents explained that, whilst cyberterrorism does not constitute a significant threat, cyberwarfare and cybercrime do.[127] Measures taken in response to these other threats will also improve security against cyberterrorism. In the words of one respondent, "defensive measures taken against cybercrime and cyberwarfare will also work against cyberterrorism".[128] Second, five of these respondents explained that, whilst cyberterrorism does not constitute a significant threat, other forms of terrorism do.[129] For these researchers, measures taken to combat other forms of terrorism will also improve security against cyberterrorism. In fact, one respondent went further and argued that seeking specifically to tackle cyberterrorism could prove ultimately counterproductive:

> If we develop specific 'counter-terrorism' strategies for 'cyberterrorism', then we risk overlooking the motivations that underlie this impulse towards violence. Whether an act of terrorism is digitally or physically realised is but a particular manifestation of these motivations. It is important, therefore, that this basic rudiment of understanding 'terrorism' does not get lost in the 'cyberterrorism' hyperbole.[130]

Tables 3 and 4 complete this section of the article by detailing responses to questions 11 and 12 by the disciplinary backgrounds of respondents.

[*Insert table 3 here*]

Table 3 compares the disciplinary backgrounds of those respondents that opined that a cyberterrorist attack has, and hasn't, taken place with the backgrounds of the general pool of respondents. It is worth noting, first, that there were respondents from all seven groups that believed a cyberterrorist attack has taken place. In contrast, whilst there were respondents from five of the disciplinary groups that stated that a cyberterrorist attack has never taken place, there were no respondents from the other two groups (B and C) that held this view. This was particularly striking for disciplinary group B (Law, Criminology, et al), given that this group accounted for 11% of the general pool of respondents. Also striking was the fact that respondents from Group A (Political Science, International Relations, et al) accounted for 34% of those that stated that a cyberterrorist attack has taken place but 69% of those that said that such an attack has never occurred.

[*Insert table 4 here*]

Table 4 shows the disciplinary backgrounds of the respondents that proposed each of the identified countermeasures. Although the number of respondents is small for many of them, two interesting findings nonetheless emerge. First, some countermeasures seemed to be more closely linked to respondents from a particular disciplinary background. For example, while 42% of respondents who identified one of these 12 countermeasures were from Political Science and International Relations backgrounds (Group A), this group accounted for 67% of

those warning against exaggerating the threat, and 80% of those promoting counter-radicalization. In similar vein, 57% of the respondents that argued for enhanced international co-operation were from group D (Engineering, Computer Science, Cyber, et al) even though this group only accounted for 17% of all respondents, and 67% of those that suggested employing hackers were from group E (Psychology, Anthropology, et al) even though this group only accounted for 16% of all respondents. Second, the twelve countermeasures listed in the table were mentioned by respondents from across all seven disciplinary groups: none were restricted to any one background. As detailed further below, these two findings point to the importance of a multidisciplinary approach to responding to cyberterrorism.

Conclusion

As the preceding discussion has shown, there is considerable disagreement within the academic research community around cyberterrorism. According to the findings of this project's survey, no meaningful consensus exists around the extent to which this phenomenon poses a security threat; the potential targets of cyberterrorist attacks; indeed, whether cyberterrorism has even yet occurred. The roots of this disagreement are, in part, conceptual. As detailed above, different interpretations of 'threat' and 'significance' as well as different assessments of imminence were evident throughout the qualitative findings generated in this research. It was also, however, partly a product of competing logics for assessing and predicting threat: not least, divergent views on the past's reliability for inferential reasoning on the future. Definitional issues were important here too. Although fifteen different attacks were identified by our respondents as cyberterrorism - attacks stretching, incidentally, across Australia, Estonia, India, Iran, Israel, the US and beyond - others disqualified these for a number of reasons. Thus, the lack of physical violence or death from attacks launched in cyberspace to date was, for some, reason not to describe these as cyberterrorism. For others, the lack of fear

generated by cyberattacks (especially, vis-à-vis their physical equivalents) was of relevance. For others still, an actor-specific conception of cyberterrorism was needed to differentiate this phenomenon from state-based cyber-war attacks. Some respondents, moreover, emphasised the importance of differentiating cyberterrorism from cybercrime or cyberactivism.

The extent of this disagreement has two obvious parallels. The first, detailed at the start of this article, is that within the academic literature on the threat of cyberterrorism specifically. As argued there, this literature has gradually witnessed the emergence of competing perspectives to counter-balance the earliest - and in some senses most hyperbolic - of predictions around the likelihood and scale of future attacks. Many of the respondents raised issues explored in this literature - CII vulnerabilities, the preferences of terrorist actors, issues of global interconnectivity, and so forth - with a small number of others speaking instead to the construction of 'cyberterrorism' as a present/future threat. The second obvious parallel is existing academic debate on terrorism more widely, which has long been characterised by competing views of how best to calculate risk in this area.[131] In some senses, at least, current academic perspectives on cyberterrorism may therefore simply represent an extension of the positions held in relation to its parent concept.

In addition to these contiguities, however, it is also important to note two findings from the survey that point to the potential distinctiveness of cyberterrorism. First, a number of the respondents identified the need for specific types of expertise for the countering of cyberterrorism vis-à-vis other terrorisms. While some of these were environment-specific (for example, air walling), others invoked the need for new types of partnership between sectors and actors across the socio-political spectrum. Whilst the countering of terrorism has always evolved over time, and new types of actors have been brought into this public policy area,[132] these findings do speak to a debate over the distinctiveness of preventive and responsive activities in this particular context.

The second respect in which the research findings suggest cyberterrorism is distinct is the level of contestability surrounding the term. Its parent concept terrorism is, of course, the subject of longstanding – and well-worn – definitional controversies. Whether particular attacks or uses of violence warrant this terminology is hotly debated: not least in relation to 'state terrorism'. There is also debate over the objective or subjective status of the labelling of an act as 'terrorist' and over the likelihood of future attacks.[133] Yet, in spite of this, one would be hard-pressed to find a researcher willing to argue it has never occurred. In stark contrast, half of respondents to this survey believed cyberterrorism has already occurred, while the other half believed it has not. This demonstrates a level of contestability - conceptual and otherwise - that stretches far beyond debate on offline or non-cyberterrorism.

Chart 1: Cyberterrorism: A Significant Threat?

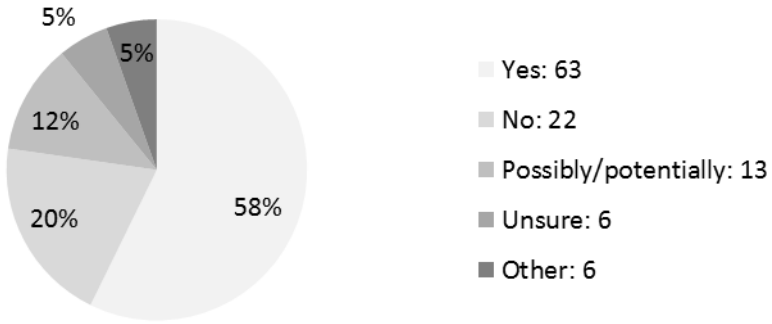

Table 1: Referent Objects of the Cyberterrorism Threat

Government/state	23 respondents
Critical infrastructure/computer networks	19 respondents
Civilians/individuals	10 respondents
Organizations/private sector/corporations/economy	10 respondents
Society	3 respondents
Anyone/everyone	3 respondents
Groups	2 respondents
Political elections	1 respondent

[Some respondents identified more than one referent]

Chart 2: Has a cyberterrorist attack ever taken place? (All respondents)

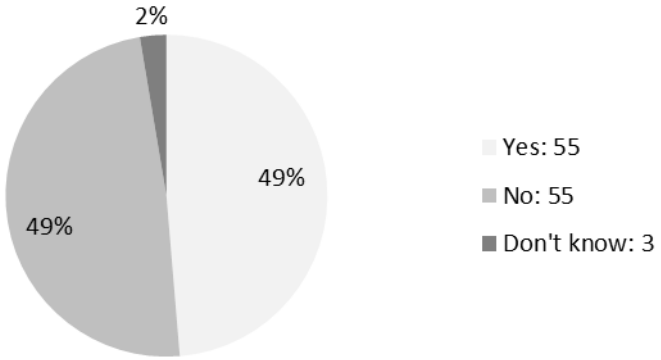

Table 2: Examples of cyberterrorist attacks offered by respondents

Attacks on Estonia[134]	11 respondents
Stuxnet, Iran[135]	6 respondents
Attacks on Georgia[136]	3 respondents
India-Pakistan[137]	2 respondents
Anonymous[138]	2 respondents
Turkey PKK collapsed Govt network[139]	1 respondent
Zapatista spamming[140]	1 respondent
Wikileaks	1 respondent
Israel-Gaza[141]	1 respondent
India (social networking)[142]	1 respondent
Dalai Lama[143]	1 respondent
Tariq bin Ziyad Brigades[144]	1 respondent
Aerospace[145]	1 respondent
Australian sewage leak[146]	1 respondent
Kyrgyzstan[147]	1 respondent

Chart 3: Does cyberterrorism constitute a significant threat? (Those respondents that stated that no cyberterrorist attack has ever taken place)

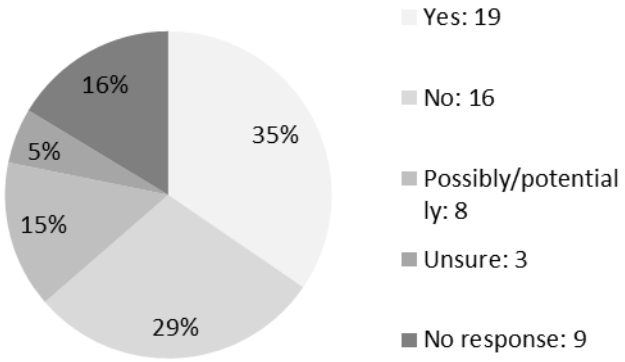

Chart 4: The most effective countermeasures against cyberterrorism

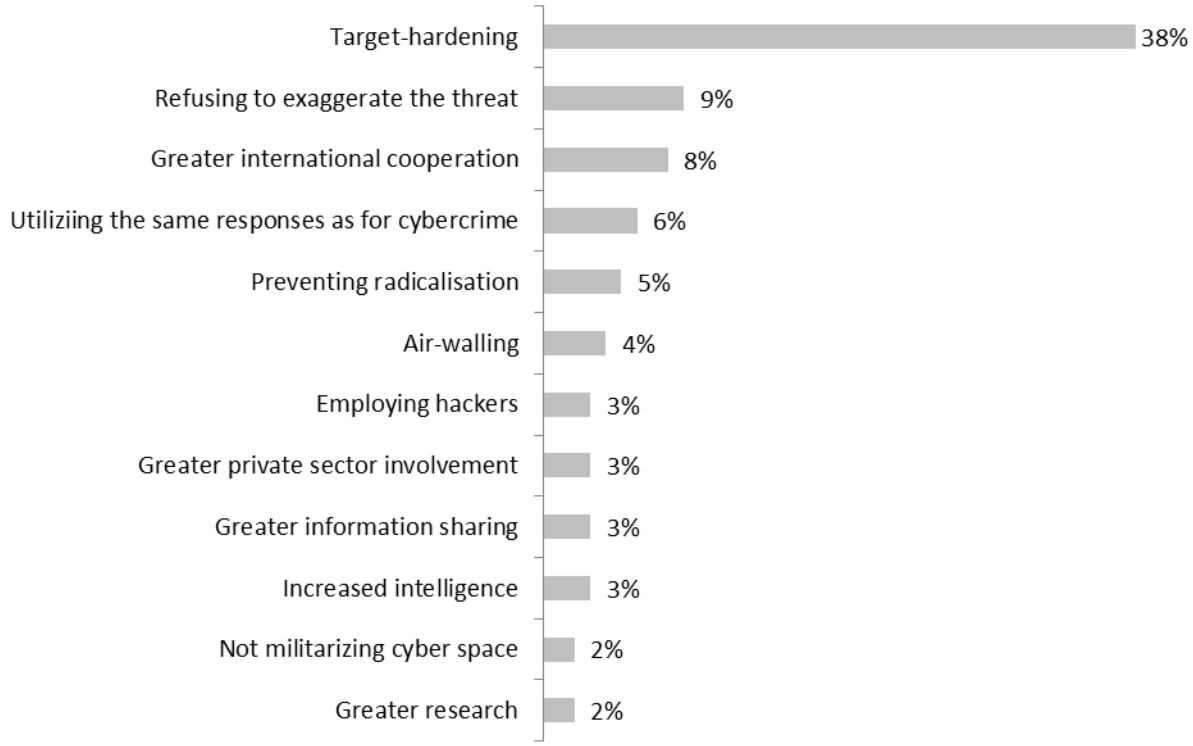

Chart 5: Differences to other forms of anti- or counter-terrorism

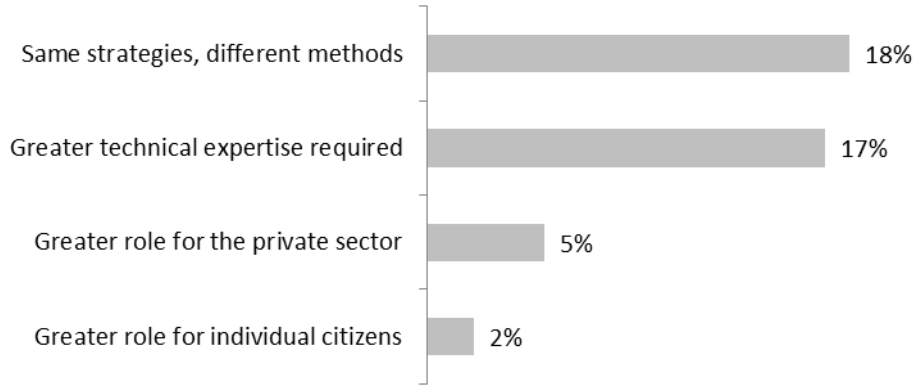

Table 3: Has a cyberterrorist attack ever taken place? (By disciplinary background)

	All respondents	Those respondents that said a cyberterrorist attack has taken	Those respondents that said a cyberterrorist attack has not

		place	taken place
Group A (Political Science, International Relations, et al)	50%	34%	69%
Group B (Law, Criminology, et al)	11%	20%	0%
Group C (Economics, Business, et al)	1%	3%	0%
Group D (Engineering, Computer Science, Cyber, et al)	12%	15%	10%
Group E (Psychology, Anthropology, et al)	15%	16%	12%
Group F (Literature, Arts, History, et al)	7%	5%	7%
Group G (Independent Researchers, Analysts, et al)	4%	7%	2%

Table 4: Countermeasures against cyberterrorism by disciplinary background

	Total	Group A (Political Science, International Relations, et al)	Group B (Law, Criminology, et al)	Group C (Economics, Business, et al)	Group D (Engineering, Computer Science, Cyber, et al)	Group E (Psychology, Anthropology, et al)	Group F (Literature, Arts, History, et al)	Group G (Independent Researchers, Analysts, et al)
Respondents that identified one of the following 12 measures	60	29 (42%)	7 (10%)	1 (1%)	12 (17%)	11 (16%)	5 (7%)	4 (6%)
Target-hardening	35	17 (41%)	5 (12%)	1 (2%)	7 (17%)	6 (15%)	4 (10%)	1 (2%)
Refusing to exaggerate the threat	8	6 (67%)	-	-	1 (11%)	2 (22%)	-	-
Greater international co-operation	7	2 (29%)	-	-	4 (57%)	-	1 (14%)	-
Utilizing the same responses as for cybercrime	6	2 (33%)	-	-	2 (33%)	1 (17%)	1 (17%)	-
Preventing radicalization	5	4	-	-	-	1	-	-

		(80%)				(20%)		
Air-walling	4	3 (75%)	-	-	-	1 (25%)	-	-
Employing hackers	3	-	1 (33%)	-	-	2 (67%)	-	-
Greater private sector involvement	3	2 (67%)	-	-	-	-	-	1 (33%)
Greater information-sharing	3	-	-	-	1 (33%)	-	1 (33%)	1 (33%)
Increased intelligence	3	2 (66%)	-	-	-	1 (33%)	-	-
Not militarizing cyberspace	2	1 (50%)	1 (50%)	-	-	-	-	-
Greater research	2	1 (50%)	-	-	-	-	-	1 (50%)

[1] Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature* Updated Edition (New Burnswick, NJ: Transaction, 2008).

[2] Schmid and Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature*, 2.

[3] Andrew Silke, "The Devil You Know: Continuing Problems with Research on Terrorism", in *Research on Terrorism: Trends, Achievements and Failures,* ed. Andrew Silke (Abingdon: Routledge, 2004), 57-71. See also, John Horgan, (2004) "The Case for Firsthand Research", in *Research on Terrorism: Trends, Achievements and Failures*, ed. Andrew Silke (Abingdon: Routledge, 2004), 30-56.

[4] Andrew Silke, "The Road Less Travelled: Recent Trends in Terrorism Research", in *Research on Terrorism: Trends, Achievements and Failures*, ed. Andrew Silke (Abingdon: Routledge, 2004), 186-213.

[5] Magnus Ranstorp, "Mapping terrorism studies after 9/11: An academic field of old problems and new prospects", in *Critical Terrorism Studies: A New Research Agenda*, eds. Richard Jackson et al (Abingdon: Routledge, 2009), 13-33; See also, Andrew Silke, "Contemporary terrorism studies: Issues in Research", in *Critical Terrorism Studies: A New Research Agenda* Jackson, eds. Richard Jackson et al (Abingdon: Routledge, 2009), 34-48.

[6] Stuart Macdonald, Lee Jarvis, Tom Chen and Simon Lavis, *Cyberterrorism: A Survey of Researchers*, Cyberterrorism Project Research Report No. 1 (Swansea University, 2013), accessed June 28, 2013, http://www.cyberterrorism-project.org.

[7] Sarah Gordon and Richard Ford, "Cyberterrorism?" *Computers and Security* 21 (7) (2002): 637. For an overview of conceptual debate on terrorism more broadly, see: Leonard Weinberg, Ami Pedahzur and Sivan Hirsch-Hoefler, "The Challenges of Conceptualizing Terrorism," *Terrorism and Political Violence* 16 (4) (2004), 777-794; Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* 7 (11) (2002), accessed May 15, 2013, doi: 10.5210%2Ffm.v7i11.1001; George K. Kostopoulos, "Cyberterrorism: The Next Arena of Confrontation," *Communications of the IBIMA*, 6 (1) (2008), 165-169; Peter Neumann, *Old and New Terrorism* (Cambridge: Polity Press, 2009).

[8] Dorothy Denning, "Cyberterrorism," (Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000), accessed May 15 2013, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[9] See, for example: UK Government, "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review (2010)", accessed May 15, 2013, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191 6 4.pdf?CID=PDF&PLA=furl&CRE=sdsr; Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, "Cyber Security and the UK's Critical National Infrastructure (2011)", accessed May 15, 2013, http://www.chathamhouse.org/publications/papers/view/178171.

[10] Barry Collin, "The Future of Cyberterrorism", *Crime and Justice International* 13 (2) (1997), 17.

[11] Barry Collin, "The Future of Cyberterrorism", 17.

[12]Dorothy Denning, "Cyberterrorism".

[13] Audrey Kurth Cronin, "Behind the Curve Globalisation and International Terrorism," *International Security* 27 (3) (2002/03), 47.

[14] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" *United States Institute of Peace Special Report* 119 (2004), accessed May 15, 2013, http://www.usip.org/publications/cyberterrorism-how-real-threat: 6.

[15] S. M. Furnell and M. J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?" *Computers and Security* 18 (1999), 28.

[16] Jerrold M. Post, Kevin G. Ruby and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence* 12 (2) (2000), 102.

[17] Simon, Steven and Daniel Benjamin, "America and the New Terrorism," *Survival* 42 (1) 2000, 59-75.

[18] Jerrold M. Post, Kevin G. Ruby and Eric D. Shaw, "From Car Bombs to Logic Bombs", 103.

[19] Matthew G. Devost, Brian K. Houghton and Neal Allen Pollard, "Information Terrorism: Political Violence in the Information Age," *Terrorism and Political Violence* 9 (1) (1997), 78.

[20] For a discussion of the resilience of CII's to attack that is at odds with most of the following references, please see: James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies*, accessed May 16, 2013, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf: 27.

[21] Myriam Dunn Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses", 16.

[22] Clay Wilson, "Cyber Threats to Critical Information Infrastructure" (Forthcoming) *Cyber Terrorism: A Multi-disciplinary Approach* eds. Lee Jarvis, Stuart Macdonald and Tom Chen (New York, Springer, 2014).

[23] Myriam Dunn Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses", 17.

[24] "Networks of comprised computers that are controlled remotely to perform large-scale disrupted denial of service (DDoS) attacks, send spam, trojan and phishing emails, distribute pirated media or conduct other usually illegitimate activities" - Anestis Karasaridis, Brian Rexroad and David Hoeflin, "Wide-Scale Botnet Detection and Characterisation" (paper presented at First Workshop on Hot Topics in Understanding Botnets, 2007) accessed May 16, 2013 http://dl.acm.org/citation.cfm?id=1323135.

[25] Myriam Dunn, "Securing the Information Age: The Challenges of Complexity for Critical Information Infrastructure Protection and IR Theory", in *International Relations and Security in the Digital Age* eds. Johan Eriksson and Giampiero Giacomello (Abingdon: Routledge, 2007), 97.

[26] Myriam Dunn Cavelty, "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology and Politics* 4 (1) (2007), accessed May 13, 2013, doi: 0.1300/J516v04n01_03; Maura Conway, "The Media and Cyberterrorism: A Study in the Construction of 'Reality'," (2008), accessed May 15, 2013, http://doras.dcu.ie/2142/1/2008-5.pdf.

[27] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School," *International Studies Quarterly* 53 (4) (2009): 1155-1175. For further examples, see: Maura Conway, "The Media and Cyberterrorism"; Myriam Dunn Cavelty, "Cyber-Terror – Looming Threat or Phantom Menace?".

[28] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", 1168.

[29] Maura Conway, "The Media and Cyberterrorism", 11.

[30] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict and Terrorism* 28 (2005), 129-49.

[31] Maura Conway, "The Media and Cyberterrorism: A Study in the Construction of 'Reality'", 43-44.

[32] Ralf Bendrath, "The American Cyber-Angst and the Real World – Any Link?" in *Bombs and Bandwidth: The Emerging Relationship Between Information and Technology and Security*, ed. Robert Latham. (London: The New Press, 2003), 49-73.

[33] See, for example: Maura Conway, "The Media and Cyberterrorism", 43; Arash Barfar, Kiyana Zolfaghar and Shahriar Mohammadi, "A Framework for Cyber War against International Terrorism," *International Journal of Internet Technology and Secured Transactions* 3 (1) (2011), accessed May 13, 2013 doi: 10.1504/IJITST.2011.039677, 30.

[34] Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet", 13.

[35] Maura Conway, "Against Cyberterrorism," *Communications of the ACM* 54 (2) (2011), accessed May 13, 2013, doi: 10.1145/1897816.1897829; Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?" *Crime Law and Social Change* 46 (2006), accessed May 13, 2013, doi: 10.1007/s10611-007-9061-9.

[36] Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism* 27 (2004), 387-388.

[37] Maura Conway, "Terrorism and New Media: The Cyber-Battlespace" in *Countering Terrorism and Insurgency in the 21st Century: International Perspectives* Volume 2, ed. James J. Forest, (Westport: Praeger Security International, 2007), 365- 371.

[38] See, for example: Maura Conway, "Terrorism and (Mass) Communication: From Nitro to the Net," *World Today* 60 (8/9) (2004), 19-22; Audrey Kurth Cronin, "Behind the Curve Globalisation and International Terrorism", 30-58. A related, but distinct, argument is also made within the relevant literature that identifies advancements in technology and the processes of globalisation as a driver of changes in the hierarchies and structures of terrorist organisations. For a comprehensive discussion of these issues see: David Ronfeldt and John Arquila, "What Next for Networks and Netwars," in *Networks and Netwars: The Future of Terror, Crime and Militancy,* eds. David Ronfeldt and John Arquila (Santa Monica: RAND, 2001), 311–368.

[39] Manuel R. Torres Soriano, "The Vulnerabilities of Online Terrorism," *Studies in Conflict and Terrorism* 35 (4) (2012), 275.

[40] Rachel E. Yould, "Beyond the American Fortress: Understanding Homeland Security in the Information Age," in *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security,* ed. Robert Latham, (New York: Social Science Council, 2003), 79.

[41] Myriam Dunn Cavelty, "Critical Information Infrastructures: Vulnerabilities, Threats and Responses," *Disarmament Forum* (2007), accessed May 16 2013, http://www.unidir.org/pdf/articles/pdf-art2643.pdf, 19.

[42] See, for example: Rex Hughes, "Towards a Global Regime for Cyber Warfare," in *The Virtual Battlefield: Perspectives on Cyber Warfare,* eds. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press), 106-117; Donald J. Reed, "Beyond the War on Terror: Into the Fifth Generation of War and Conflict," *Studies in Conflict and Terrorism* 31 (8) (2008), 684-722.

[43] Keiran Hardy, "WWWMDs: Cyber-Attacks Against Infrastructure in Domestic Anti-Terror Laws," *Computer Law and Security Review* 27 (2011), 161.

[44] Andrew Rathmell, "Controlling Computer Network Operations" *Studies in Conflict and Terrorism* 26 (3) (2003), 218.

[45] See Jackson, R. et al (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, 124-149.

[46] The complete list is as follows: ACM Digital Library; Anthropoligical Index Online; Applied Social Sciences Index and Abstracts; Bibliography of British & Irish History; BioMed Central Journals; British Humanities Index (CSA); British Periodicals (XML); Business Source Complete (EBSCO); CINAHL Plus (EBSCO); Cochrane Database of Systematic Reviews (Wiley); Education Resources Information Centre; Emerald; HeinOnline; HMIC (Ovid); IEEE Xplore; INSPEC (Ovid); International Bibliography of the Social Sciences; IOP Journals Z39; JISC Journals Archives; JSTOR; Kluwer Law Journals; Lecture Notes in Computer Science (Springer Link); Lexis Library; MathSciNet (AMS); Medline (EBSCO); MLA International Bibliography; Oxford Journals; Periodicals Archive online; Philosopher's Index (Ovid); Project Muse; Proquest Business Collection; PsycARTICLES (Ovid); PsycINFO (Ovid); PubMed; Royal Society Journals; SAGE Journals Online; Scopus (Elsevier); Social Care Online (SCIE); Springer Link (Metapress); Taylor & Francis Online; Web of Knowledge (Cross Search); Web of Knowledge (ISI); Web of Science (Cross Search); Web of Science (ISI); Westlaw; Wiley Interscience; and, Zetoc.

[47] At the time of writing, *Terrorism & Political Violence* was ranked 27/78 in International Relations and 59/141 in Political Science, with an impact factor of 0.814. *Studies in Conflict and Terrorism* was ranked 42/78 in International Relations and 78/141 in Political Science, with an impact factor of 0.588.

[48] Andrew Silke, 'The Devil You Know: Continuing Problems with Research on Terrorism', in *Research on Terrorism: Trends, Achievements and Failures* ed. Andrew Silke (Abingdon: Routledge, 2004), 61.

[49] See, amongst many others, Jeroen Gunning, "A Case for Critical Terrorism Studies?", *Government & Opposition* 42(3) (2007), 363-393.

[50] The most obvious example is in the emergence of debates around 'Critical Terrorism Studies' (CTS). Although diverse, proponents of CTS argue for a revisiting of the fundamental ontological, epistemological, normative and methodological assumptions of terrorism research, as well as the purposes of scholarship in this field. For overviews, see, Jeroen Gunning, "A Case for Critical Terrorism Studies?"; Richard Jackson et al*, Critical Terrorism Studies: A New Research Agenda*; Richard Jackson et al, *Terrorism: A Critical Introduction* (Basingstoke: Palgrave, 2011); Lee Jarvis, "The Spaces and Faces of Critical Terrorism Studies", *Security Dialogue* 40(1) 2009, 5-27. For criticism, see, John Horgan and Michael J. Boyle, Michael J, 'A Case against 'Critical Terrorism Studies'', *Critical Studies on Terrorism* 1(1) (2008), 51-64; David M. Jones and M.L. R, 'We're All Terrorists Now: Critical - or Hypocritical - Studies "on" Terrorism', *Studies in Conflict & Terrorism* 32(4) (2009), 292-302.

[51] For further information on this association, please see: TAPVA, accessed February 26, 2013, http://tapva.com.

[52] Please see the following webpage for more information on this working group: BISA, accessed February 26, 2013, http://www.bisa.ac.uk/index.php?option=com_content&view=article&id=93&catid=37&Itemid=68.

[53] See, Sandra Halperin, and Oliver Heath, *Political Research: Methods and Practical Skills* (Oxford: Oxford University Press, 2012), 245-246.

[54] On the transitory nature of terrorism studies as an academic field, see, Magnus Ranstorp, "Mapping terrorism studies after 9/11: An academic field of old problems and new prospects", in *Critical Terrorism Studies: A New Research Agenda* eds. Richard Jackson et al (Abingdon: Routledge, 2009), 14-15.

[55] Jacob L. Stump and Priya Dixit, *Critical Terrorism Studies: An Introduction to Research Methods* (Abingdon: Routledge, 2013), 37.

[56] Several of our researchers self-identified according to more than one disciplinary background.

[57] Silke, for instance, points to the dominant and growing hold of political scientists over terrorism research throughout the 1990s. See, Andrew Silke, "The Road Less Travelled: Recent Trends in Terrorism Research", in *Research on Terrorism: Trends, Achievements and Failures* ed. Andrew Silke (Abingdon: Routledge, 2004), 193-194.

[58]Responses to the survey have been anonymised and arranged numerically from R1 to R118. Responses have been edited as sparingly as possible to ensure fidelity to our findings.

[59] R93

[60] R61

[61] R53

[62] R31, R39, R80, R85, R99

[63] R85, R93 and R99 all referred to transport in general. R25 referred specifically to aviation.

[64] R25, R43, R94.

[65] R16 and R85 referred to energy grids in general. R31 and R39 referred specifically to electric grids

[66] R16, R31.

[67] R93.

[68] R93.

[69] R85

[70] R47

[71] R57

[72] R16

[73] R1, R9, R68, R86.

[74] R2

[75] R39

[76] R82

[77] R20, R68, R70.

[78] R39, R43, R65, R94. One of these (R65) specifically referred to cyberterrorism including cyber espionage.

[79] R1, R65, R80, R94.

[80] R80

[81] R22

[82] R95

[83] R45

[84] R90

[85] R82

[86] R4

[87] R9

[88] R34, R45, R73.

[89] R34

[90] R73

[91] R11, R21, R45, R52, R63, R73.

[92] R21, R73.

[93] R11, R45, R52.

[94] R11

[95] R45, R63.

[96] R63

[97] R45

[98] R30

[99] R36

[100] R76

[101] R56

[102] R107

[103] R50

[104] R104

[105] R1, R4, R10, R53, R55, R64, R78, R106.

[106] R5, R21, R26, R28, R35, R64, R95.

[107] R95

[108] R1, R8, R33, R54.

[109] R1

[110] R33

[111] R1, R21.

[112] R21, R34, R58, R65.

[113] R21, R26, R63.

[114] R60

[115] R90

[116] R9

[117] R80

[118] R97

[119] R57

[120] R85

[121] R102

[122] R86

[123] R93

[124] R81

[125] The other 33 respondents that answered this question either: identified a countermeasure that was not mentioned by any other respondents; or, only answered the second part of question 12.

[126] R11, R15, R21, R27, R45, R52, R54, R63, R64, R73, R74, R103, R108, R110.

[127] R21, R54, R63, R103, R108.

[128] R108

[129] R21, R27, R45, R63, R110.

[130] R45

[131] See, for example, John Mueller's 'Six Rather Unusual Propositions' article and the responses to it within the same issue: John Mueller, "Six Rather Unusual Propositions About Terrorism", *Terrorism and Political Violence* 17(4) (2005), 487-505.

[132] Lee Jarvis and Michael Lister, "Stakeholder Security: The New Western Way of Counter-Terrorism?", *Contemporary Politics* 16(2) (2010), 173-188.

[133] Richard Jackson et al, *Terrorism: A Critical Introduction*.

[134] The Russian cyberattacks on Estonia in 2007.

[135] See further: James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*. 53(1) (2011), 23-40.

[136] The Russian cyberattack on a Georgian government website in 2008.

[137] In 2010 the Indian Cyber Army hacked into the website of the Pakistani Army, and the Pakistan Cyber Army hacked into the website of the Indian Central Bureau of Investigation.

[138] One respondent referred specifically to Anonymous hacking into the websites of the Boston and Salt Lake City Police Departments and threatening to release the names and addresses of police officers (R39). The other referred simply to the group (R101).

[139] The Turkish Ministry of Finance's website was hacked by the Kurdistan Workers' Party (PKK) (2011).

[140] The Mexican Zapatista group has shut down Mexican police and other websites.

[141] Following its air strikes on the Gaza Strip Israel experienced more than 44 million hacking attempts on government and other finance websites (2012).

[142] During the Assam riots threatening messages and pictures were sent to migrant workers using social networking sites (2012).

[143] A Chinese cyber espionage organisation targeted the office of the Dalai Lama (2009).

[144] The respondent stated that this group are mentioned in the UK's CONTEST strategy. The relevant paragraph reads: "We continue to see no evidence of systematic cyber terrorism (i.e. terrorist attack on IT systems). But the first recorded incident of a terrorist 'cyber' attack on corporate computer systems took place in 2010.33 The so called 'here you have' virus, (the responsibility for which was claimed by the Tariq bin Ziyad Brigades for Electronic Jihad) was relatively unsophisticated but a likely indicator of a future trend. Since the death of Usama bin Laden, Al Qa'ida has explicitly called not only for acts of lone or individual terrorism (see para 2.22) but also for 'cyber jihad'." (*CONTEST: The United Kingdom's Strategy for Countering Terrorism* Cm 8123 (2011), para 2.47)

[145] US defence firm Lockheed Martin said it came under a significant cyberattack in 2011.

[146] The Maroochy Shire cyberattack (2000).

[147] The sustained cyberattack reported in 2009.