Terrorism and Political Violence

ISSN: 0954-6553 (Print) 1556-1836 (Online) Journal homepage: http://www.tandfonline.com/loi/ftpv20

What Is Cyberterrorism? Findings From a Survey of Researchers

Lee Jarvis & Stuart Macdonald

To cite this article: Lee Jarvis & Stuart Macdonald (2015) What Is Cyberterrorism? Findings From a Survey of Researchers, Terrorism and Political Violence, 27:4, 657-678, DOI: 10.1080/09546553.2013.847827

To link to this article: http://dx.doi.org/10.1080/09546553.2013.847827

Published online: 08 May 2014.

Submit your article to this journal

Article views: 1281

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=ftpv20

Download by: [University of Saskatchewan Library] **Date:** 14 February 2016, At: 10:12

Terrorism and Political Violence, 27:657–678, 2015
Copyright © Taylor & Francis Group, LLC
ISSN: 0954-6553 print/1556-1836 online
DOI: 10.1080/09546553.2013.847827

Routledge
Taylor & Francis Group

What Is Cyberterrorism? Findings From a Survey of Researchers

LEE JARVIS

School of Political, Social and International Studies, Faculty of Arts and Humanities, University of East Anglia, Norwich, UK

STUART MACDONALD

College of Law, Swansea University, Swansea, UK

This article reports on a recent survey designed to capture understandings of cyberterrorism across the global research community. Specifically, it explores competing views, and the importance thereof, amongst 118 respondents on three definitional issues: (a) the need for a specific definition of cyberterrorism for either policymakers or researchers; (b) the core characteristics or constituent parts of this concept; and (c) the value of applying the term "cyberterrorism" to a range of actual or potential scenarios. The article concludes by arguing that while a majority of researchers believe a specific definition of cyberterrorism is necessary for academics and policymakers, disagreement around what this might look like has additional potential to stimulate a rethinking of terrorism more widely.

Keywords cyberterrorism, definition, survey, terrorism, terrorism research, terrorism studies

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Introduction

This article reports original findings from a recent project on definitions and understandings of the concept of "cyberterrorism" within the global research community. This "state of the discipline" exercise employed a survey which was completed by 118 researchers working in 24 countries across six continents. The survey was designed with three principal ambitions. The first was to map areas of consensus, disagreement, and ambiguity on core definitional questions around the term cyberterrorism.

Lee Jarvis is a Senior Lecturer in the School of Political, Social and International Studies, Faculty of Arts and Humanities, University of East Anglia. His publications include *Times of Terror: Discourse, Temporality and the War on Terror* (Palgrave, 2009) and *Terrorism: A Critical Introduction* (Palgrave, 2011). His research is in print or forthcoming in journals including *International Relations, Political Studies, Security Dialogue, Citizenship Studies, Critical Studies on Terrorism*, and *Contemporary Politics*. Stuart Macdonald is an Associate Professor in the College of Law at Swansea University. He has published articles on anti-terrorism policy and legislation in a number of leading international journals, including the *Sydney Law Review* and the *Cornell Journal of Law and Public Policy*. His recent research on security and liberty was funded by the British Academy.

Address correspondence to Lee Jarvis, School of Political, Social and International Studies, Faculty of Arts and Humanities, University of East Anglia, Norwich Research Park, Norwich NR4 7TJ, UK. E-mail: l.jarvis@uea.ac.uk

The second was to explore whether agreement or otherwise on these definitional questions had implications for derivative debates including on the causes and threat of cyberterrorism. The third was to map current academic activity in this area, including the extent to which researchers are currently teaching courses on cyberterrorism, or planning to do so.[1]

The discussion in this article focuses on findings relating to three issues of definition in particular: (a) whether the academic community deems a specific definition of cyberterrorism necessary for either policymakers or researchers; (b) the core characteristics or constitutive elements of cyberterrorism; and (c) the appropriateness and value of applying the term "cyberterrorism" to a range of actual and potential scenarios. By presenting and discussing these findings, this article aims to take stock of what is known or thought about cyberterrorism within the research community today. This is important, we argue, because the increasing prevalence of this term across political, media, and academic debate since its coinage in the 1980s[2] has engendered nothing like a consistency of usage. The academic backdrop to our exploration is a series of precedent studies that were integral to mapping the contours of academic research on terrorism more broadly. Schmid and Jongman's pioneering *Political Terrorism*[3] made similar use of a questionnaire, "mailed to some two hundred members of the research community in the field of political terrorism in 1985."[4] Silke's edited *Research on Terrorism* offers a related review of dominant methodological techniques and research trends within terrorism research.[5] More recent still are contributions by Ranstorp and Silke on the interests and limitations of terrorism research in the post-9/11 period.[6] Where all of these outputs helped consolidate knowledge of, and identify tensions within, terrorism research at particular junctures, we attempt here to do likewise for the concept of cyberterrorism.

The article proceeds in four stages. We begin with a review of current academic literature on the concept of cyberterrorism. Drawing attention to the diversity of definitions of this term we distinguish, first, between narrow and broad conceptions and, second, between different approaches to the distinctiveness of cyberterrorism. The second section outlines our methodology, following which we turn to analysing our findings. The article concludes by arguing that while a majority of researchers believe a specific definition of cyberterrorism is necessary for academics and policymakers, disagreements and debates around what this might look like also have potential to encourage a rethinking of terrorism more widely.

Cyberterrorism: Concepts and Controversies

The extent and the longevity of definitional debate on the concept of terrorism have been well documented. Despite its far briefer existence, it is perhaps unsurprising that cyberterrorism presents an equally contested concept.[7] With its emergence tied, in part, to late twentieth century insecurities and zeitgeists in which "the rapid growth in Internet use and the debate on the emerging 'information society' sparked several studies on the potential risks faced by the highly networked, high-tech dependent United States,"[8] the continuing popularity of cyberterrorism as a concept—and fear—has been underpinned by established economic and political interests, as much as by psychological fears of its occurrence.[9] Despite this continued resonance, however, two definitional issues in particular divide researchers working in this area. The first is referential: to what does, or should, the term cyberterrorism refer? The second is relational: how is cyberterrorism similar to, and different from, other forms

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

of violence or behaviour? Is it, for instance, a distinctive phenomenon with its own characteristics? Or is it a sub-species of terrorism which comprises a broad and diverse spectrum of violence?

To begin with the former question, discussions of cyberterrorism's appropriate referent frequently invoke a distinction between narrow and broad conceptions of this term. Where the former concentrate on terrorist attacks conducted via or against information infrastructures, more expansive understandings are willing to incorporate a far more diverse range of online activities associated with terrorism under this heading. Thus, as Brunst notes:

> A more narrow view is often worded close to common terrorism definitions and might include only politically motivated attacks against information systems and only if they result in violence against noncombatant targets.... Broader approaches often include other forms of terrorist use of the Internet and therefore might define cyberterrorism as almost any use of information technology by terrorists.[10]

Talihärm invokes a similar distinction, differentiating between target-oriented (narrow) and tool-oriented (broad) understandings:

> The first identifies as cyberterrorism all politically or socially motivated attacks against computers, networks and information, whether conducted through other computers or physically, when causing injuries, bloodshed or serious damage, or fear (hereafter "target-oriented cyberterrorism"). The second labels all actions using the Internet or computers to organize and complete terrorist actions as cyberterrorism (hereafter "tool-oriented cyberterrorism").[11]

Under this latter approach, activities as diverse as fundraising, reconnaissance, communications, and propagandising all potentially qualify as cyberterrorism if conducted online for the purposes of terrorism.

Perhaps the most familiar example of a narrower approach is found within Dorothy Denning's 2000 Testimony before the U.S. House of Representatives. As the following demonstrates, the remit of her definition is circumscribed in two unrelated ways:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. 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.[12]

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

The first restriction introduced by Denning is a focus on information technologies as the immediate target of an attack. As her subsequent elaboration makes clear, these technologies serve also as the instruments of cyberterrorism:

> Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies. These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of Web sites on the Internet.[13]

Second, Denning's account also includes the condition of material or corporeal harm. To qualify as cyberterrorism, in this understanding, an attack must have offline or ''real world'' consequences that extend beyond damage to information technologies or data.

Narrow understandings of cyberterrorism such as Denning's remain far more prevalent in the literature than their more expansive counterparts. Weimann, for example, limits the term to ''the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations).''[14] Hua and Bapna define the term similarly, as ''an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies.''[15] Conway follows each of Denning's requirements by distinguishing cyberterrorism from terrorist usage of computers and by introducing a requirement that offline damage is caused.[16] An early contribution by Pollitt, moreover, added a further actor-specific qualification: ''Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.''[17] In his view, ''For cyberterrorism to have any meaning, we must be able to differentiate it from other kinds of computer abuse such as computer crime, economic espionage, or information warfare.''[18] Discussions of the utility of broader understandings of cyberterrorism, on the other hand, include Gordon and Ford's exploration of the Internet's penetration into all aspects of ''the terrorism matrix.''[19] In their view, the dominant focus on ''pure cyberterrorism'' (terrorist activities carried out entirely or primarily in the virtual world) is a potentially costly one given the potential of this to obscure other terrorism-related online activities.

If denotative breadth offers one major source of definitional disagreement, a second revolves around divergent understandings on the relationship between cyberterrorism and other types of terrorist activity. At least four different views are apparent here. The first is to approach cyberterrorism as an unlikely or purely hypothetical counterpart to the reality of other, more conventional, types of terrorism. Here, specificity in defining the former is important only for focusing the attention of analysts upon the latter. Consider, for example, James A. Lewis' argument:

> Explosions are dramatic, strike fear into the hearts of opponents and do lasting damage. Cyber attacks would not have the same dramatic and political effect that terrorists seek. A cyber attack, which might not even

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

> be noticed by its victims, or attributed to routine delays or outages, will not be their preferred weapon.[20]

Similarly, Maura Conway advances four arguments for why no act of cyberterrorism has ever yet occurred and is unlikely to at any time in the near future.[21] These are that: cyber attacks are vastly more expensive than physical ones; terrorists lack technical capability and are unlikely to outsource; the destructive potential of non-cyber attacks is more readily materialised; and cyber attacks are less attractive to terrorists because they lack the theatricality of physical attacks. On this perspective, exemplified by Joshua Green in the following, since cyberterrorism has never occurred, and remains unlikely to do so, it simply does not exist:

> There's just one problem: There is no such thing as cyberterrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity.... Which is not to say that cybersecurity isn't a serious problem—it's just not one that involves terrorists.[22]

As this illustrates, commentators that have taken this approach tend toward narrow understandings of cyberterrorism. Their rationale for engaging in questions of definition is to divert attention away from cyberterrorism—understood restrictively—and toward other types of terrorism, or other terrorist uses of the Internet. Although alternative online terrorist activities are potentially prevalent, they have—according to this view—"been largely ignored... in favour of the more headline-grabbing 'cyberterrorism.'"[23] Thus, as Denning warns, "Too much emphasis on cyberterror, especially if it is not a serious threat, could detract from other counterterrorist efforts in the cyber domain."[24]

A second view treats cyberterrorism as a reality, but one that is distinct from other forms of terrorism and therefore requiring of its own definition. Thomas J. Holt has argued that:

> 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.[25]

This approach is similar to the first in that it emphasises terrorist uses of the Internet other than cyberattacks. Unlike the previous view, however, it embraces a broader definition of cyberterrorism which allows the identification of qualitative differences to traditional understandings of terrorism. For example, Holt illustrates his argument using a definition offered by Bryan Foltz.[26] Whilst Foltz's definition includes some features commonly associated with traditional terrorism—a political motivation and an attack (or threat of attack)—it does not require physical harm or an intention to generate fear. According to Foltz, attacks may qualify as cyberterrorist without meeting these criteria if they are intended to "interfere with the political, social or economic functioning of a group, organization or country," or to "induce either

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

physical violence or the unjust use of power.'' Holt explains that these differences recognise the fact that ''extremist groups utilize the Internet in ways that more closely resemble the characteristics of cybercrimes including the dissemination of information to incite violence and harm.''[27]

A third view collapses any qualitative distinction between cyberterrorism and more traditional forms of terrorism. It regards cyberterrorism simply as a subset of this broader category, and so states that an attack only qualifies as cyberterrorist if all components of the definition of terrorism have been satisfied. Michael Stohl, for example, has argued that we should ''restrict cyber terrorism to activities which in addition to their cyber component have the commonly agreed upon components of terrorism.''[28] This, he explains, preserves the distinction between cybercrime and cyberterrorism. On this approach (exemplified also by Pollitt's definition quoted above), for an attack to qualify as cyberterrorist it must result in violence (or the threat thereof). So if an extremist group were to interfere with a nation's Stock Exchange via digital technologies and cause severe economic damage this would not constitute cyberterrorism. In contrast, if the same group interfered with an air traffic control system and caused two passenger aircraft to collide in mid-air this would. As Collin succinctly puts it, cyberterrorism is ''hacking with a body count.''[29] From this, it follows that a definition of cyberterrorism is not strictly necessary. Cyberterrorist attacks already fall within the definition of terrorism, and the cyber prefix denotes nothing more than the means employed. We do not specify the means used in other forms of terrorism (no one employs such terms as pyro-terrorism, aero-terrorism, or hydro-terrorism), and so there is no need for a separate subcategory of cyberterrorism. As Gordon and Ford explain:

> We do not use the term ''ice pick terrorism'' to define bombings of ice-pick factories, nor would we use it to define terrorism carried out with ice picks. Thus, we question the use of the term cyberterrorism to describe just any sort of threat or crime carried out with or against computers in general.[30]

A fourth view is an amalgam of the second and third. This insists that cyberterrorism is a subset of the broader category of terrorism, but that there are important qualitative differences between the two. An example is Dorothy Denning's 2007 definition of cyberterrorism:

> Cyberterrorism is generally understood to refer to highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property.[31]

In contrast to the third approach, Denning goes on to explain that an attack against critical infrastructure which is motivated by political or social objectives and which causes a billion dollar banking loss would constitute cyberterrorism. This is also the approach taken by the UK's statutory definition of cyberterrorism.[32] An attack qualifies as terrorist under section 1 of the Terrorism Act 2000 if: (i) it was carried out with an intention to influence the government or an international governmental

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

organisation or intimidate the public or a section of the public; (ii) the purpose was to advance a political, religious, racial or ideological cause; and (iii) the attack falls within one of the five actions listed in subsection (2). Paragraphs (a)–(d) of subsection (2) focus on acts which endanger life, cause serious violence or serious property damage or create a serious risk to public health and safety. By contrast, paragraph (e) applies whether or not human life or property was endangered. It encompasses acts which are designed seriously to interfere with or seriously to disrupt an electronic system. This would include cyber-attacks on Internet service providers, financial exchanges computer systems, and controls of national power and water.[33] In other words, there exists a lower threshold for including cyber-attacks within the broad category of terrorism than there does for non-cyber-attacks.

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Methodology

As the above discussion suggests, the concept of cyberterrorism provokes considerable definitional disagreement. Our own effort to contribute to these discussions involved the distribution of a survey to over 600 members of the global research community between June and November 2012. Respondents were identified using a purposive strategy that made use of four primary sampling methods. First: a targeted literature review search to identify researchers who have published specifically on cyberterrorism within peer-reviewed journals, monographs, edited books, or other literature. This 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).[34] The search was limited to publications on or since January 1, 2004.

The second strategy was to target active researchers within the terrorism research community more widely. Whilst these individuals may not have published on cyberterrorism specifically, their knowledge of definitional and related debates around terrorism more widely meant they would be well positioned to contribute to this research. To this end, individuals that had published an article in any of the following four journals since January 1, 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 1, 2012) were also added for their academic standing in terrorism research. The first two journals selected—*Terrorism and Political Violence* and *Studies in Conflict and Terrorism*—are widely recognised as the most established outlets for publishing peer-reviewed research on terrorist violence. As Andrew 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."[35] The continuing reputation of these journals today is confirmed by measures such as impact factor counts.[36] At the same time, however, the field of terrorism research has expanded dramatically in recent years, becoming far more contested in the process.[37] To take account of this, and to capture the plurality of contemporary approaches to terrorism, contributors to and editors of *Critical Studies on Terrorism* and the online, open access, *Perspectives on Terrorism* were added to our sample.

The third sampling strategy was a "snowball method" in which we contacted potential respondents identified by individuals who had already completed the

survey. The fourth was via two academic mailing lists maintained by the Terrorism and Political Violence Association,[38] and the British International Studies Association Critical Terrorism Studies Working Group.[39] Although there was, of course, overlap in the individuals identified in our four strategies, these latter two methods engendered far fewer respondents than did our initial literature review searches.

The use of a purposive, non-probabilistic sampling strategy was, we argue, appropriate to the survey's ambitions.[40] Whilst it involves sacrificing any strict claim to statistical representativeness, this may be defended given the nature of the population in whom we were interested: the terrorism research community. Where the boundaries of this community lie, and who may be considered a legitimate inhabitant therein, are, of course eminently contestable. Does it, for instance, extend to research students, non-affiliated researchers, or retired academics? Moreover, as with any epistemic community—indeed, perhaps more than many[41]—the field of terrorism research is, by its nature, fluid and porous. Individuals enter and leave this community according to their evolving research interests, and any effort to capture opinion therein can offer only a de-temporalised snapshot of a dynamic phenomenon. In this sense, this sacrifice of representativeness is justified given the lack of any objectively identifiable population here.

A total of 118 responses from researchers working in 24 countries across six continents were generated by our survey. Of the 117 responses providing geographical information, our sample had a majority of respondents working in the United States of America and United Kingdom: 41 (35% of the total) and 32 (27%) respectively. The next largest sites were Australia (7 respondents, 6%) and Canada (4 respondents, 3%). This weighting toward anglophonic countries is unfortunate, but unsurprising given the traditional anglocentricism of terrorism research.[42] In terms of professional status, the distribution was 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 terms of disciplinary background, finally, our sample described themselves 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%).[43] This high proportion of researchers identifying with the disciplines of Political Science and International Relations again resonates with earlier empirical studies of terrorism research.[44]

Our survey employed a combination of open-ended and closed questions designed to generate quantitative and qualitative data. Twenty questions were included in total. These focused on: demographic information; definitional issues around terrorism and cyberterrorism; the cyberterrorism threat; countering cyberterrorism; and views of current research on this phenomenon, including the major challenges facing contemporary scholars. To encourage as high a completion rate as possible, the questionnaire was made available via an online survey and a word processing document.

Findings and Analysis

The remainder of our article explores our research findings in relation to six questions from our survey:[45]

- *Question 2:* On a scale of 1 to 5—where 1 is "not at all" and 5 is "entirely"—to what extent have the definitional issues around terrorism in general been satisfactorily resolved: (a) for policymakers; (b) for researchers?

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

- *Question 3:* On a scale of 1 to 5—where 1 is "not at all" and 5 is "very important"—how important is/was their resolution: (a) for policymakers; (b) for researchers?
- *Question 4:* On a scale of 1 to 5—where 1 is "of no use" and 5 is "essential"—how necessary do you believe a specific definition of cyberterrorism to be: (a) for policymakers; (b) for researchers?
- *Question 5*: In your view, which of these are important elements of cyberterrorism?: A political or ideological motive; civilian targets; criminality or illegality; fear as an outcome; random or indiscriminate attack; a theatrical or performative dimension; conducted by an organization or group; digital means or target; non-state perpetrators; violence against people or property.
- *Question 6:* In your view are there any important elements of cyberterrorism missing from this list [above]?
- *Question 7:* The following diagram distinguishes terrorist acts by the site of their preparation, means and target. In your view, which of the following scenarios constitutes an act of cyberterrorism?[46]

Defining (Cyber) Terrorism

One of the main aims of our survey was to explore whether the "cyber" prefix has any discernible impact on definitional issues around the wider concept of terrorism. In other words, do views of the necessity—or existence—of an adequate definition of "cyberterrorism" simply reproduce researcher stances on definitional debates in this area more generally? Or, alternatively, does a shift in focus from terrorism to cyberterrorism lead to a shift in perspective on the value of definitional work? To explore this, we began our survey by seeking respondents' views on two related themes: (a) The importance of resolving the definitional issues around terrorism in general, and (b) Whether these issues have already been satisfactorily resolved. Respondents were provided with a five point Likert scale to record their answers for policymakers and researchers, with an optional free text box for further reflection. Tables 1 and 2 summarise the response to these questions:

As Table 1 demonstrates, the definitional issues surrounding terrorism have not been satisfactorily resolved for many respondents to our survey. In relation to policymakers, the mean score was 2.41. For researchers, it was slightly higher, at 2.82. Just over one-third of respondents (34%) entered a score of either 1 or 2 in respect of researchers, rising to just over one half (52%) for policymakers. Importantly, as Table 2 illustrates, the majority of respondents also believe that the resolution of

Table 1. The resolution of terrorism's definitional issues

	To what extent have the definitional issues around terrorism in general been satisfactorily resolved? (where 1 = *not at all* and 5 = *entirely*)				
Discipline	1	2	3	4	5
For policymakers? ($n = 114$, response rate: 97%)	29	31	35	16	3
For researchers? ($n = 118$, response rate: 100%)	15	25	48	26	4

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

these definitional issues has importance. A majority of all respondents entered a score of either 4 or 5 for policymakers (61%) and researchers (57%) alike; the mean scores being 3.71 (policymakers) and 3.61 (researchers).

A number of respondents explained why they believe a satisfactory definition of terrorism is important. Some emphasised the importance of clarity for researchers for setting the parameters of a research project (*R29*), communicating findings to others (*R87*), and in ensuring consistency across different projects (for example, in databases of terrorist events) (*R87*). Others focussed on the implementation of policy and legislation. They explained that a clear definition of terrorism is needed to delineate the scope of terrorism-related criminal offences (*R33*), to distinguish terrorism from crime (*R70*), and to facilitate cooperation across jurisdictional boundaries (*R1*). As one respondent suggested: "If we do not know exactly what terrorism is, how can we study or stop it?" (*R80*).

Whilst the majority of respondents approached terrorism's definitional issues as both important and unsatisfactorily resolved, it is important to note that this view was far from unanimous. In Table 2, roughly one-fifth of respondents entered a score of either 1 or 2 out of 5 on the importance of a definition of terrorism (20% in respect of researchers, 18% in respect of policymakers). A similar number also felt that the definitional issues had already been satisfactorily resolved. In Table 1, 19 respondents (17%) entered a score of either 4 or 5 in respect of policymakers. This figure rose to 30 respondents (25%) in respect of researchers.

As Table 3 demonstrates, a related trend was apparent in responses to question 4, which sought respondents' views on the necessity of a specific definition of cyberterrorism.

Here, the majority of our respondents believed a specific definition of cyberterrorism to be necessary for each audience: policymakers and researchers. The mean scores for this question were 3.73 (for policymakers) and 3.51 (for researchers). Almost two-thirds of respondents entered a score of either 4 or 5 in respect of policymakers (66%) and although the total was slightly lower in respect of researchers it was still a majority (56%). Roughly one-fifth doubted the necessity of such an enterprise, entering a score of either 1 or 2 (18% in respect of policymakers, 23% in respect of researchers).

Justifications for, and objections to, a specific definition of cyberterrorism largely mirrored those given for terrorism more broadly. One respondent pointed out that jurisdictional problems are likely to be especially acute in cases involving

Table 2. The importance of a definition of terrorism

	How important is, or was, the resolution of the definitional issues around terrorism? (where 1 = *not at all* and 5 = *very important*)				
Discipline	1	2	3	4	5
For policymakers? ($n = 111$, response rate: 94%)	9	11	23	28	40
For researchers? ($n = 115$, response rate: 97%)	5	18	27	32	33

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Table 3. The need for a specific definition of cyberterrorism

	How necessary do you believe a specific definition of cyberterrorism to be? (where 1 = *of no use* and 5 = *essential*)				
Discipline	1	2	3	4	5
For policymakers? ($n = 114$, response rate: 97%)	7	13	19	40	35
For researchers? ($n = 118$, response rate: 100%)	7	20	25	38	28

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

cyberterrorism, increasing the importance of a clear definition here (*R1*). Others, in contrast, questioned the value of definitional work at all:

> Security practice does not require definition of threat. It is performative—it constructs its own threats and its reasons for being. Cyberterrorism, or "terrorism," performs an oppositional construct that doesn't require specific definition. (*R36*)

Others still argued that, since the cyber realm is relatively young and rapidly developing, it would be premature and counterproductive to attempt to define cyberterrorism. One respondent, for example, argued, "rigid definitions fix artificial meanings on social phenomena that are perennially shifting, thus foreclosing certain parameters for adaptation of 'new' or 'alternative' conceptions of cyberterrorism" (*R45*). In the words of another: "cyber is in a state of flux at the moment, so some uncertainty is helpful. We don't know what a cyber world looks like, so defining terrorism within that context is a bit early" (*R20*).

There were also contrasting views on the relative importance to policymakers and researchers of resolving these issues. As Figure 1 illustrates, the overall view was that

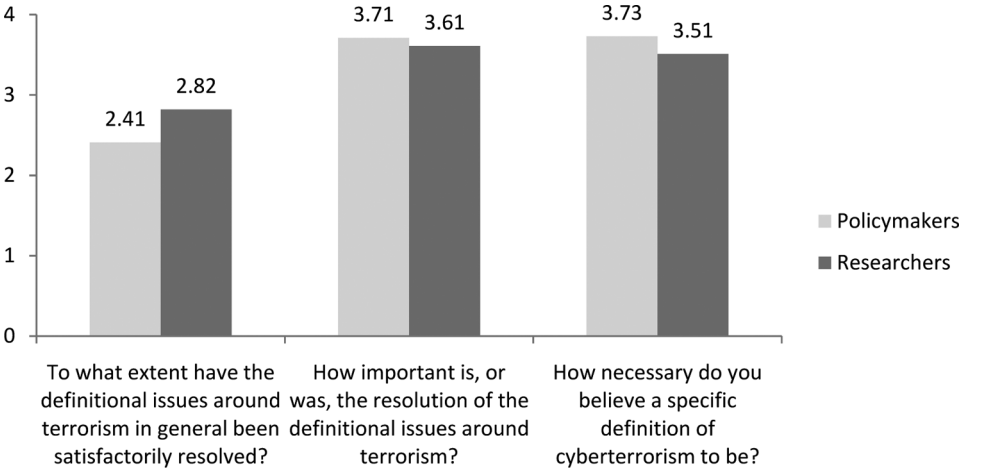


Figure 1. Mean scores in respect of policymakers and researchers.

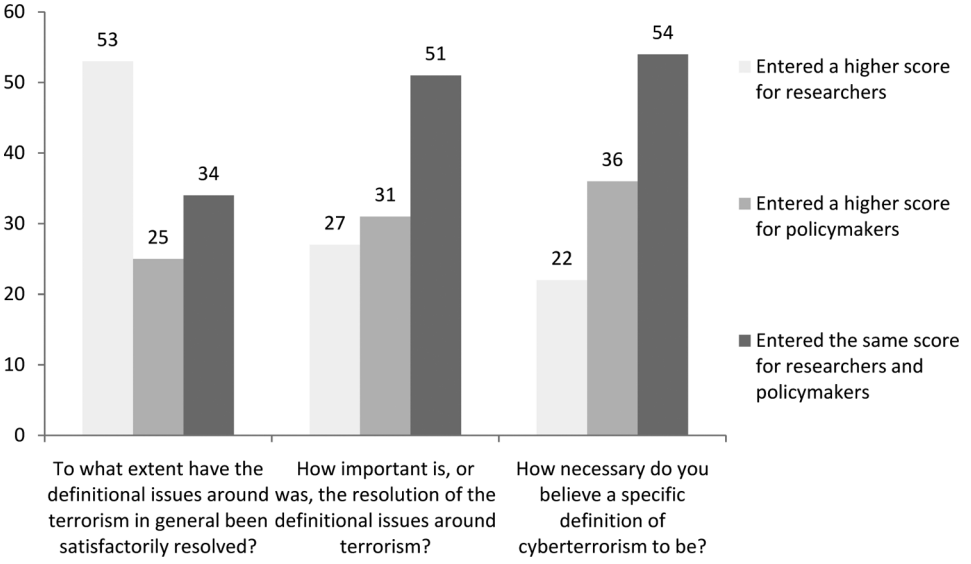


Figure 2. Differences between policymakers and researchers.

not only are these definitional issues more important for policymakers than for researchers, but also that they have been less satisfactorily resolved for the former.

A number of reasons were provided for the greater importance of definitional issues to policymakers. Some focussed on the formulation of laws and policies, and the prior need to identify the targeted phenomenon (*R43, R54*). Others focussed on the application of laws and policies and the need to stop the misapplication (*R46, R72, R82, R104*) or deliberate misuse (*R101*) of statutory or other powers. At the same time, as Figure 2 demonstrates, 27 respondents (25%) believed the resolution of terrorism's definitional issues to be of greater significance to researchers. As one respondent put it:

> Having worked in a policy-making environment as well as an academic one on this issue, it seems to me that policymakers' definitions of such phenomena tend to flow from legislative sources and are significant only inasmuch as they affect decisions about prosecutions (i.e., who should be charged with "terrorist" hacking vs. computer mischief) or jurisdiction (i.e., an incident is a law enforcement problem or an intelligence service problem). They are far more problematic and vital for researchers, who wish to understand the phenomena in question in objective, holistic terms. (*R21*)

It is also worth noting that, when the question focussed on cyberterrorism specifically, rather than terrorism in general, the number of respondents entering a higher score for policymakers increased to 36 respondents (32%) from 31 respondents (28%). At the same time, the number entering a higher score for researchers decreased from 27 respondents (25%) to 22 respondents (20%). Coupled with the mean scores from Figure 1, this clearly suggests that the definitional issues surrounding terrorism in general are of greater importance to researchers than the ones surrounding cyberterrorism, as viewed by our respondents.

Finally, on this theme, Table 4 presents respondents' answers to these questions by disciplinary background. Several respondents' additional comments emphasised

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Table 4. Defining terrorism and cyberterrorism by academic discipline (mean scores)

Question	Discipline	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, et al.)	Group E (psychology, anthropology, et al.)	Group F (literature, arts, history, et al.)	Group G (independent researchers, analysts, et al.)	Overall average
Question 2	For policymakers	2.37	2.54	2	2.75	2.39	2	2.4	2.41
	For researchers	2.76	2.79	2	3.125	2.74	3.25	2.6	2.82
Question 3	For policymakers	3.57	3.54	5	4	4.28	3.875	3.6	3.71
	For researchers	3.44	3.57	5	4.06	3.95	3.625	3.6	3.61
Question 4	For policymakers	3.52	3.85	4	4.125	3.94	4.125	3.6	3.73
	For researchers	3.26	3.71	3.5	4.19	3.74	3.75	3.6	3.51

Questions were as follows: *Question 2*: To what extent have the definitional issues around terrorism in general been satisfactorily resolved? (where 1 = *not at all* and 5 = *entirely*). *Question 3*: How important is, or was, the resolution of the definitional issues around terrorism? (where 1 = *not at all important* and 5 = *very important*). *Question 4*: How necessary do you believe a specific definition of cyberterrorism to be? (where 1 = *of no use* and 5 = *essential*).

the especial importance of definitions in the legal realm, offering statements such as, "Definitions matter most with respect to law" (*R67*) and "A specific definition would be most useful for lawmakers" (*R99*). It is striking, therefore, that when asked how important the definitional issues around terrorism are for policymakers the mean score for the respondents from Group B of our sample—Law, Criminology, et al.—was lower than for any of the other six groups:

Understanding Cyberterrorism

Question 5 of our survey asked respondents to identify important elements of cyberterrorism from a list of ten items drawn from the literature reviewed in the above section. 115 respondents in total answered this question (response rate: 97%). As Figure 3 illustrates, the three features regarded as the most important were: (a) motive; (b) digital means or target; and (c) fear as an outcome. Given the survey's focus on cyberterrorism, it is interesting to note that a greater number of respondents selected the need for a political or ideological motive than a digital means or target. The fact that fewer than half of our respondents selected violence against people or property is also noteworthy, not least for its contrast to Schmid and Jongman's review of definitions of terrorism which identified "violence, force" as the most prevalent of word categories, appearing in 83.5% of the definitions discussed.[47]

Question 6 then asked respondents to identify important elements of cyberterrorism missing from our list, with 50 respondents replying with one or more suggestions (see Table 5). The most common response was harm or disruption to infrastructure. One respondent, for example, commented that cyberterrorism is "about the disruption of ICT systems. The effects will spill over to non-digital social processes, but the immediate target is something digital" (*R63*). The next two most common responses were the possibility of state perpetration, and coercion or terror in a wider audience.

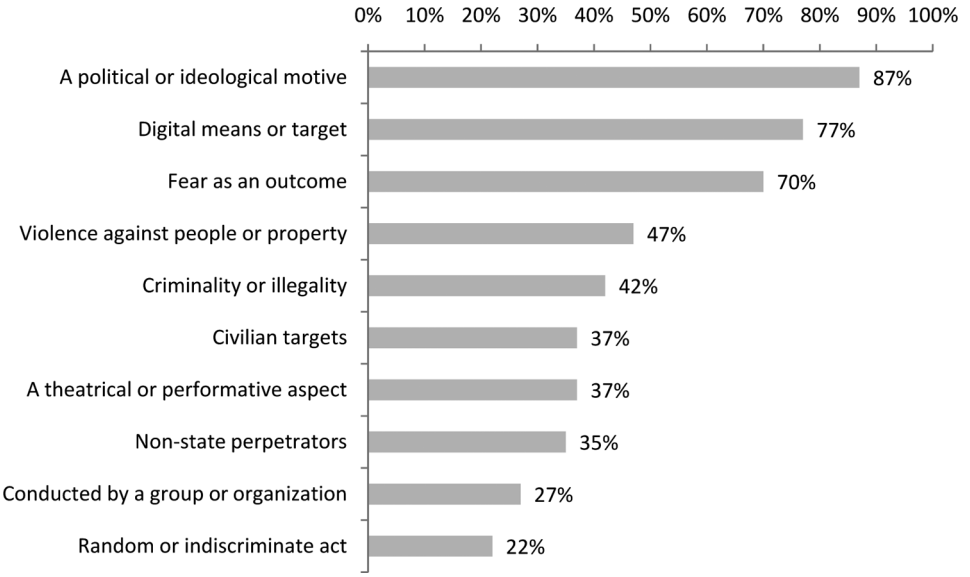


Figure 3. Important elements of cyberterrorism.

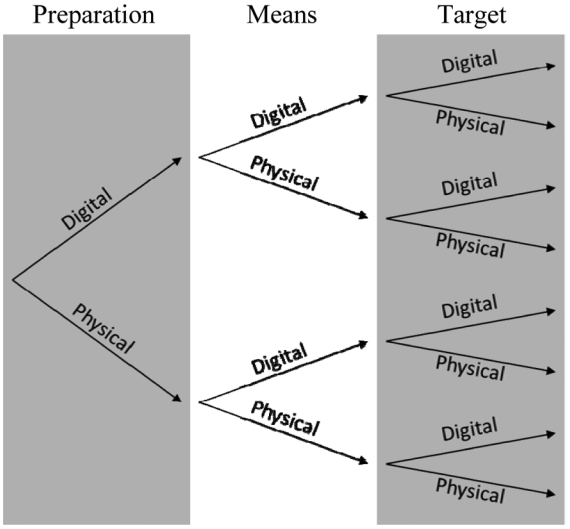
Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Table 5. Additional elements of cyberterrorism

Item	Number of respondents
Harm/disruption to infrastructure	7 respondents
Possibility of state perpetration	6 respondents
Coercion or terror in a wider audience	6 respondents
Demonstration of perpetrator skill/capability	3 respondents
Causes harm/damage	2 respondents
Low cost	2 respondents
Other motives:	
Social or economic motives	1 respondent
Religious motives	1 respondent
Threat to national security	1 respondent
Large scale	1 respondent
Violation of international law	1 respondent
Brainwashing	1 respondent
Entertainment	1 respondent

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

To generate a fuller understanding of the applicability of the label cyberterrorism to particular activities, Question 7 of the survey provided a tree diagram reproduced in Figure 4 below. This derived from Devost et al.'s suggestion that "pure" information terrorism (which involves digital tools and a digital target) may be distinguished from information terrorism (which involves either digital tools or a digital target, but not both).[48] The tree diagram set out a total of eight scenarios—or types of event—involving different combinations of digital/physical preparation, means, and targets. Respondents were asked to decide which scenarios would constitute acts of cyberterrorism. The three possible answers were: yes; potentially; or no. Respondents were also able to enter additional comments in a free text box.



	Yes	Potentially	No
A	77%	20%	3%
B	60%	30%	10%
C	50%	24%	27%
D	20%	19%	61%
E	70%	24%	6%
F	38%	43%	18%
G	33%	36%	32%
H	9%	13%	78%

Figure 4. Which of the following scenarios constitutes an act of cyberterrorism?

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Nine respondents stated in the text box that the diagram was unclear or lacked sufficient explanation. To an extent, this was a product of our decision not to provide further clarification or examples in an effort to avoid leading respondents. One of the other most common concerns was the diagram's lack of reference to a protagonist's motives. This query appeared to be based on a misunderstanding of the difference between necessary and sufficient conditions. The aim of the question was to ascertain respondents' views on whether digital preparation, means, and target are necessary conditions for an attack to be classified as cyberterrorism, not whether they are sufficient conditions. The claim that digital preparation, means, and/or target are necessary conditions does not automatically entail the claim that they are also sufficient. So any reference to the motives of the attacker was unnecessary, just as it is possible to state that a dead body is a necessary prerequisite for a murder conviction without knowing anything about the intentions of the attacker.

In total, 92 respondents completed this question in full (response rate: 80%). A further 13 completed it in part. The figures in each row of Figure 4 are the proportion of respondents who responded to that particular scenario. The data suggests, first, that digital preparatory activities were generally regarded as insufficient for an attack to qualify as cyberterrorism. Whilst 61% of respondents stated that scenario D—which involved digital preparation but physical means and target—did not constitute cyberterrorism, only 20% stated that it did. So, whilst some researchers might classify an attack such as 9/11 as cyberterrorism on the basis that the Internet was used for planning and to purchase tickets,[49] it seems the majority would not.

As Figure 4 indicates, the means and target of an attack were of far greater significance to our respondents than its preparation. Of these, digital means were regarded as the most important. On scenario F, in which the only digital component was the means employed, 38% of respondents believed this constituted cyberterrorism, with only 18% selecting no. By contrast, in response to scenario G—where the only digital component was the target—33% stated this did constitute cyberterrorism with 32% claiming not. A similar comparison can be drawn between scenarios C (where the only physical component was the means employed) and B (where the only physical component was the target). In the absence of a digital target, 60% of respondents believed that the scenario nonetheless constituted cyberterrorism. This figure fell to 50% when it was digital means that were missing. Similarly, in the absence of a digital target only 10% of respondents stated that the scenario did not constitute cyberterrorism. This figure rose to 27% when it was digital means that were absent.

Although, as the responses to questions 5 and 7 indicate, the majority of respondents regarded digital means or target as an important element of cyberterrorism, this view was not unanimous. As shown in Figure 3 above, 23% of respondents did not select digital means or target as important elements of cyberterrorism. In Table 6, we therefore set out the responses to our tree diagram divided into two parts: the responses from those who did select digital means or target and the responses from those who did not. The figures in brackets are the difference from the percentage figure for all respondents (set out in Figure 4 above). As one would expect, those who did not select digital means or target in question 5 were less likely to state that the scenarios involving physical means do not constitute cyberterrorism. In this group's responses to each of the four scenarios involving physical means (C, D, G, and H), the proportion that selected no was significantly lower than the equivalent figure for those that had selected digital means or target in question 5. The same was not true, however, for the four scenarios involving a physical target (B, D, F,

Table 6. Digital means and target

	Those who selected "digital means or target" in question 5			Those who did not select "digital means or target" in question 5		
Scenario	Yes	Potentially	No	Yes	Potentially	No
Scenario A	79% (+2%)	18% (−2%)	2% (−1%)	68% (−9%)	27% (+7%)	5% (+2%)
Scenario B	63% (+3%)	31% (+1%)	6% (−4%)	50% (−10%)	27% (−3%)	23% (+13%)
Scenario C	51% (+1%)	19% (−5%)	30% (+3%)	43% (−7%)	43% (+19%)	14% (−13%)
Scenario D	17% (−3%)	21% (+2%)	63% (+2%)	33% (+13%)	14% (−5%)	52% (−9%)
Scenario E	71% (+1%)	23% (−1%)	6% (=)	67% (−3%)	29% (+5%)	5% (−1%)
Scenario F	41% (+3%)	44% (−1%)	15% (−3%)	29% (−9%)	43% (=)	29% (+11%)
Scenario G	35% (+2%)	31% (−5%)	35% (+3%)	25% (−8%)	55% (+19%)	20% (−12%)
Scenario H	8% (−1%)	11% (−2%)	81% (+3%)	14% (+5%)	19% (+6%)	67% (−11%)

and H). Perhaps surprisingly, for two of these scenarios (B and F) a greater proportion of those that had *not* selected digital means or target as an important element of cyberterrorism said that these scenarios do *not* constitute cyberterrorism. This again suggests that, for those who regarded digital means or target as an important element of cyberterrorism, it is digital means that is the most important.

Table 7 focuses on another divisive issue: the relevance of violence against people or property. We saw above that in question 5, 47% of respondents selected this as an important element of cyberterrorism. Table 7 breaks down the responses to question 7 into two categories: the responses from those that selected violence against people or property in question 5 and the responses from those that did not.

Table 7 shows that those respondents that did select violence against people or property in question 5 were more likely to opine that scenarios involving a physical target were cyberterrorism. The proportion of this group that stated that the four scenarios involving a physical target (B, D, F, and H) constitute cyberterrorism was significantly higher than the equivalent figure for the group that did not select violence against people or property in question 5. As one respondent explained, if violence against people or property is an important element of a cyberterrorist attack it follows that the target of the attack is physical:

> The question of how you define the target is very important. If a terrorist group attacks an ICT system (digital) that controls people's drinking water supply (physical), the immediate target is digital, but the goal of the attack is to harm people physically. In my view, disrupting an ICT system is rarely, if ever, a goal in itself in a cyber terrorist attack. (*R63*)

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

Table 7. Violence and cyberterrorism

	Those who selected "violence against people or property" in question 5			Those who did not select "violence against people or property" in question 5		
Scenario	Yes	Potentially	No	Yes	Potentially	No
Scenario A	73% (−4%)	21% (+1%)	6% (+3%)	80% (+3%)	20% (=)	0% (−3%)
Scenario B	71% (+11%)	23% (−7%)	6% (−4%)	51% (−9%)	36% (+6%)	13% (+3%)
Scenario C	54% (+4%)	15% (−9%)	30% (+3%)	45% (−5%)	31% (+7%)	24% (−3%)
Scenario D	35% (+15%)	17% (−2%)	48% (−13%)	8% (−12%)	21% (+2%)	72% (+11%)
Scenario E	67% (−3%)	24% (=)	9% (+3%)	73% (+3%)	24% (=)	4% (−2%)
Scenario F	46% (+8%)	37% (−6%)	17% (−1%)	32% (−6%)	49% (+6%)	19% (+1%)
Scenario G	32% (−1%)	34% (−2%)	34% (+2%)	33% (=)	37% (+1%)	30% (−2%)
Scenario H	19% (+10%)	12% (−1%)	70% (−8%)	2% (−7%)	13% (=)	85% (+7%)

This is further supported by the fact that the group who selected violence against people or property in question 5 were significantly less likely to state that scenarios D and H (which involved physical means and a physical target) did not constitute cyberterrorism.

Conclusion

This article has explored a diversity of views amongst the terrorism research community on a number of fundamental conceptual and definitional questions around cyberterrorism. These include: whether the definitional issues surrounding terrorism in general have been satisfactorily resolved; how important it is to resolve these definitional issues; whether a specific definition of cyberterrorism is necessary; whether the resolution of these definitional issues is more important for researchers or policymakers; which constitute the most important elements in identifying cyberterrorism; and the relative importance of digital preparation, means, and target in identifying whether an attack may be described as cyberterrorism. Whilst our findings did not reveal unanimity or consensus on any of these issues, in some cases it was possible to identify dominant views. Specifically, as demonstrated above, the majority of respondents to our survey argued that: the definitional issues surrounding terrorism in general are important but have not been satisfactorily resolved for either policymakers or researchers; a specific definition of cyberterrorism is needed by both policymakers and researchers; political/ideological motives, digital means/targets and the production of fear constitute important elements of cyberterrorism; and digital means is more important than digital target or digital preparation in identifying

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

whether an attack may be described as cyberterrorism. The fact that a majority of respondents believed that a definition of cyberterrorism is needed is in keeping with the existing literature on the concept reviewed at this article's outset. For, as explained previously, even those arguing that cyberterrorism does not exist have tended to engage in, and urged the importance of, these definitional questions.

Our findings also demonstrate researchers' different views on the referential and relational questions that were highlighted in our literature review. In terms of the referential question—to what does, or should, the term cyberterrorism refer?—contrasting conceptions of cyberterrorism were particularly apparent in the responses to question 7. Whilst some respondents adopted a broad understanding of the term (with, for example, 20% stating that a scenario involving digital preparation but physical means and target constitutes cyberterrorism), many others applied a far narrower understanding emphasising the importance of using digital means to launch an attack.

In terms of the relational question—is cyberterrorism a distinctive phenomenon with its own characteristics, or a sub-species of terrorism as a broad and diverse category of violence?—different approaches were also identifiable. Some of our respondents appeared to regard cyberterrorism as a subset of terrorism, with an attack only qualifying as cyberterrorist once all of the components of the definition of terrorism had been properly satisfied. These respondents therefore regarded physical violence against people or property as an important element of cyberterrorism. Importantly, however, this was not a majority view. That there is, as such, a contrast here with understandings of terrorism *per se* raises the question of whether there exist qualitative differences between terrorism and cyberterrorism. In his discussion of state terrorism, Andrew Silke suggested: "I cannot help but feel that state terrorism is actually a rhinoceros which has strayed close to our terrorism elephant. So while there are similarities between the two, they are ultimately two different creatures."[50] Our findings suggest that, for many researchers, whilst terrorism and cyberterrorism share some common features, they might ultimately also be different creatures.

It is highly significant, then, that several national legislatures (including the UK) have adopted the fourth of the approaches to the relational question explored at this article's outset. This view treats cyberterrorism as a subset of the broader category of terrorism, but simultaneously recognises that there are qualitative differences between the two. Adding a qualitatively distinct subcategory to an already existing concept has the potential to have important knock-on effects. For, as Collier and Mahon explain, "when scholars take a category developed from one set of cases and extend it to additional cases, the new cases may be sufficiently different that the category is no longer appropriate in its additional form."[51] In this sense, our findings suggest that disagreement over the concept of cyberterrorism is important not only in assessing and responding to this particular threat. But, in addition, because this disagreement also encourages scholars to reconsider, perhaps even change, their understandings of terrorism itself.

Acknowledgments

We are very grateful to all the respondents for taking the time to respond to our survey. We particularly thank Simon Lavis for his excellent research assistance throughout this project, and Thomas Chen, Joanna Halbert, David Mair, Lella Nouri, and Andrew Whiting for their comments on, and help with, earlier drafts. Our gratitude goes also to the editors and anonymous reviewers for their engagement with

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

this article, and to Swansea Academy of Learning and Teaching for their support for this research. Any errors remain ours alone.

Notes

1. For an overview of the findings, see: S. Macdonald, L. Jarvis, T. Chen, and S. Lavis, *Cyberterrorism: A Survey of Researchers* (Swansea, UK: Cyberterrorism Project Research Report [No. 1], Swansea University, 2013), www.cyberterrorism-project.org. For analysis of findings not explored in this article please also see: L. Jarvis, S. Macdonald and L. Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers," *Studies in Conflict & Terrorism* 37, no. 1 (2014): 68–90; and L. Jarvis and S. Macdonald, "Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon," *Perspectives on Terrorism* (forthcoming, 2014).
2. Barry Collin, "The Future of Cyberterrorism," *Crime and Justice International* 13, no. 2 (1997): 15–18.
3. Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature,* updated ed. (New Brunswick, NJ: Transaction, 2008).
4. Schmid and Jongman, *Political Terrorism* (see note 3 above), 2.
5. Andrew Silke, ed., *Research on Terrorism: Trends, Achievements and Failures* (Abingdon: Routledge, 2003).
6. Magnus Ranstorp, "Mapping Terrorism Studies After 9/11: An Academic Field of Old Problems and New Prospects," in Richard Jackson, Marie Breen Smyth, and Jeroen Gunning, eds., *Critical Terrorism Studies: A New Research Agenda* (Abingdon: Routledge, 2009), 13–33; Andrew Silke, "Contemporary Terrorism Studies: Issues in Research," in Richard Jackson, Marie Breen Smyth, and Jeroen Gunning, eds., *Critical Terrorism Studies: A New Research Agenda* (Abingdon: Routledge, 2009), 34–48.
7. On the contestability of the term "cyberterrorism," see Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* 7, no. 11 (2002), http://firstmonday.org/ojs/index.php/fm/article/view/1001/922. Amongst many references to the contestability of the concept "terrorism," see Martha Crenshaw, "The Psychology of Terrorism: An Agenda for the 21st Century," *Political Psychology* 21, no. 2 (2000): 405–420.
8. Gabriel Weimann, "Cyberterrorism: The Sum of all Fears?," *Studies in Conflict & Terrorism* 28, no. 2 (2005): 129–149, 131.
9. Ibid., 131–134.
10. Phillip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in Marianne Wade and Almir Maljević, eds., *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications* (New York: Springer, 2010), 51–78, 51.
11. Anna-Maria Talihärm, "Cyberterrorism: In Theory or in Practice?," *Defense Against Terrorism Review* 3, no. 2 (2010): 59–74, 63–64.
12. Dorothy Denning, *Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives,* 2000, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.
13. Ibid.
14. Weimann, "Cyberterrorism" (see note 8 above), 130.
15. Jian Hua and Sanjay Bapna, "How Can We Deter Cyberterrorism?," *Information Security Journal: A Global Perspective* 21, no. 2 (2012): 102–114, 104.
16. Conway, "Reality Bytes" (see note 7 above).
17. Mark M. Pollitt, "Cyberterrorism: Fact or Fancy," *Computer Fraud & Security* 2 (1998): 8–10, 9.
18. Ibid.
19. Sarah Gordon and Richard Ford, "Cyberterrorism?," *Computers & Security* 21, no. 7 (2002): 636–647.
20. James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Centre for Strategic and International Studies, December 2002), http://www.mafhoum.com/press4/128T41.pdf.

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

21. Maura Conway, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism," in Tom Chen, Lee Jarvis, and Stuart Macdonald, eds., *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer, forthcoming).

22. Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly,* November 2002, http://www.washingtonmonthly.com/features/2001/0211.green.html.

23. Maura Conway, "Cyberterrorism: Hype and Reality," in Leigh Armistead, ed., *Information Warfare: Separating Hype From Reality* (Dulles, VA: Potomac, 2007), 73–93.

24. Dorothy Denning, "A View of Cyberterrorism Five Years Later," in Kenneth Himma, ed., *Internet Security: Hacking, Counterhacking, and Society* (London: Jones and Bartlett, 2007), 123–140, 125.

25. Thomas J. Holt, "Exploring the Intersections of Technology, Crime, and Terror," *Terrorism and Political Violence* 24, no. 2 (2012): 337–354, 341.

26. C. Bryan Foltz, "Cyberterrorism, Computer Crime, and Reality," *Information Management & Computer Security* 12, no. 2 (2004): 154–166.

27. Holt, "Exploring the Interactions of Technology, Crime, and Terror" (see note 25 above), 341.

28. Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law & Social Change* 46, nos. 4–5 (2006): 223–238, 229. The commonly agreed upon components which Stohl refers to are "some form of intimidate, coerce, influence as well as violence or its threat."

29. Barry Collin, quoted in James D. Ballard, Joseph G. Hornik, and Douglas McKenzie, "Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues," *American Behavioral Scientist* 45, no. 6 (2002): 989–1016, 992.

30. Gordon and Ford, "Cyberterrorism?" (see note 19 above), 645.

31. Dorothy Denning, "A View of Cyberterrorism Five Years Later," in K. Himma, ed., *Internet Security: Hacking, Counterhacking, and Society* (London: Jones and Bartlett, 2007), 123–140, 124.

32. The statutory definitions in Canada and Australia are similar: see further Keiran Hardy and George Williams, "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism," in Tom Chen, Lee Jarvis, and Stuart Macdonald, eds. *Cyberterrorism: Understanding, Assessment and Response* (New York, NY: Springer, forthcoming).

33. *The Definition of Terrorism: A Report by Lord Carlile of Berriew Q.C. Independent Reviewer of Terrorism Legislation* Cm 7052 (2007), para. 71.

34. The complete list is as follows: ACM Digital Library; Anthropological 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.

35. Andrew Silke, "The Devil You Know: Continuing Problems with Research on Terrorism," in Andrew Silke, ed., *Research on Terrorism: Trends, Achievements and Failures* (Abingdon: Routledge 2004), 57–71, 61.

36. At the time of writing, *Terrorism and 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.

37. 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,

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016

as well as the purposes of scholarship in this field. For overviews, see, Jeroen Gunning, "A Case for Critical Terrorism Studies?," *Government & Opposition* 42, no. 3 (2007): 363–393; Richard Jackson, Lee Jarvis, Jeroen Gunning, and Marie Breen Smyth, *Terrorism: A Critical Introduction* (Basingstoke: Palgrave, 2011); Lee Jarvis, "The Spaces and Faces of Critical Terrorism Studies," *Security Dialogue* 40, no. 1 (2009): 5–27. For criticism, see John Horgan and Michael J. Boyle, "A Case against 'Critical Terrorism Studies,'" *Critical Studies on Terrorism* 1, no. 1 (2008): 51–64; David M. Jones and M. L. R. Smith, "We're All Terrorists Now: Critical—or Hypocritical—Studies 'on' Terrorism," *Studies in Conflict & Terrorism* 32, no. 4 (2009): 292–302.

38. For further information on the association, please see: http://tapva.com/.

39. For further information on this working group, see: http://www.bisa.ac.uk/index.php?option=com_content&view=article&id=93&catid=37&Itemid=68.

40. See Sandra Halperin and Oliver Heath, *Political Research: Methods and Practical Skills* (Oxford: Oxford University Press, 2012), 245–246.

41. On the transitory nature of terrorism studies as an academic field, see Ranstorp, "Mapping Terrorism Studies After 9/11" (see note 6 above), 14–15.

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

43. Several of our researchers self-identified according to more than one disciplinary background.

44. Andrew Silke, "The Road Less Travelled: Recent Trends in Terrorism Research," in Andrew Silke, ed., *Research on Terrorism: Trends, Achievements and Failures* (Abingdon: Routledge, 2004), 186–213, 193–194.

45. Respondents have been anonymised and numbered from R1 to R118.

46. The diagram is reproduced in Chart 4 below alongside responses to the eight scenarios provided.

47. Schmid and Jongman, *Political Terrorism* (see note 3 above), 5.

48. Matthew G. Devost, Brian K. Houghton, and Neal Allen Pollard, "Information Terrorism: Political Violence in the Information Age," *Terrorism and Political Violence* 9, no. 1 (1997): 72–83, 72.

49. Cf. Gordon and Ford, "Cyberterrorism?" (see note 19 above) in which the authors warn that narrow conceptions of cyberterrorism "[pose] a significant barrier to our ability to protect ourselves" (641), stating that "computers and, in particular, the Internet, played a key role in the execution of the September 11th attacks" (637).

50. Cited in Michael Stohl, "State Terror: The Theoretical and Practical Utilities and Implications of a Contested Concept," in Richard Jackson and Justin Sinclair, eds., *Contemporary Debates on Terrorism* (Abingdon: Routledge, 2012), 43–49.

51. Cited in Leonard Weinberg, Ami Pedahzur, and Sivan Hirsch-Hoefler, "The Challenges of Conceptualizing Terrorism," *Terrorism and Political Violence* 16, no. 4 (2004): 777–794.

Downloaded by [University of Saskatchewan Library] at 10:12 14 February 2016