View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Cronfa at Swansea University

Cronfa - Swansea University Open Access Repository

This is an author produced version of a paper published in :
Perspectives on Terrorism

Cronfa URL for this paper:
http://cronfa.swan.ac.uk/Record/cronfa17899

Paper:
Macdonald, S. & Jarvis, L. (2014). Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon. *Perspectives on Terrorism, 8*(2), 52-65.

This article is brought to you by Swansea University. Any person downloading material is agreeing to abide by the terms of the repository licence. Authors are personally responsible for adhering to publisher restrictions or conditions. When uploading content they are required to comply with their publisher agreement and the SHERPA RoMEO database to judge whether or not it is copyright safe to add this version of the paper to this repository.
http://www.swansea.ac.uk/iss/researchsupport/cronfa-support/

Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon

by Lee Jarvis and Stuart Macdonald

Abstract

This article reports on findings from a survey on the concept of cyberterrorism from researchers working in twenty-four countries across six continents. Our aim is to contribute to the definitional debate in this area by exploring the boundaries between cyberterrorism and potentially related terms. Focusing on two questions from our survey in particular, we ask: First, how does cyberterrorism relate to adjacent concepts such as hacktivism, cybercrime and cyberwar? And, second, how familiar, frequently used, and useful are these concepts amongst the global research community? Our findings include: First, high levels of familiarity with the terms cyberwarfare, information warfare and cybercrime. And, second, concerns over, and widespread avoidance of, other terms including cyber jihad and pure cyberterrorism. The article concludes by exploring the importance of these findings for definitional debates around cyberterrorism and terrorism more broadly, before outlining a number of suggestions for future research.

Keywords: *cyberterrorism, terrorism, terrorism studies, definition, cybercrime, cyberwar, hacktivism, survey*

Introduction

Arriving at a satisfactory definition of terrorism has proved a notorious and longstanding challenge for academics, policymakers and other potentially interested parties. There are multiple reasons for this elusiveness [1]. *Inter alia*, these include, first, the term's pejorative connotations and the difficulties this creates for attempts to apply it objectively [2]. Terrorism is a word, as Richard English notes, that "is almost always used to express something of one's revulsion at the acts one is describing or the people involved in them" [3]. A second reason concerns embedded political interests and the temptation to define or use the language of terrorism in flexible or misleading ways in order to condemn (or refuse to condemn) the violence of others. As Shanahan puts it: "Defining socially important concepts is seldom a disinterested activity. …It hardly needs pointing out that governments have a strong interest in promulgating definitions of 'terrorism' that emphasise its unlawful, anti-social, and morally illegitimate nature" [4]. A third issue relates to historical transformations in the meaning of terrorism, not least its original formulation to describe violence 'from above' rather than 'below' or beyond the state [5]. Fourth is the challenge of capturing the diversity of types of terrorism under one overarching label. And, fifth, is the term's propensity to 'travel' such that it is readily stretched to incorporate new behaviours and prefixes, as, for instance, in the case of 'narco-terrorism', 'eco-terrorism' and 'cyberterrorism' [6].

This article engages with an additional, and particularly significant, factor within this problem of definition: the issue of terrorism's terminological boundaries. Specifically, this is the challenge of attempting to distinguish or isolate terrorism from other types of violence (such as war), other forms of political communication (such as propaganda), or other potentially related activities [7]. As one recent contribution put it, "the label is all too often used without any real rigour as to what terrorism is and what its parameters are" [8]. Perhaps the best illustration of this boundary problem can be found in debates over whether it is ever appropriate, useful or desirable to describe state violence of any sort as terrorist. For many authors, there exists a fundamental ontological distinction between terrorism and state violence of any sort precisely because they are conducted by different actors. Additional reasons for such a distinction include the

pragmatic challenges of researching such a diversity of violent behaviour [9], and a desire for analytical clarity in the usage of terminology relating to terrorism [10]. Other authors, in contrast, argue that the boundary is far less clear than this, and that state violence – including acts of war – may justifiably be deemed terrorist should it fulfil specific criteria [11]. The point is that part of the challenge of determining what is included 'inside' a definition of terrorism involves being able somehow to distinguish this 'inside' from that which is excluded.

As with terrorism, cyberterrorism has also proved to be an equally elusive concept. This neologism offers one of the most recent additions to our already burgeoning terrorist lexicon, having become increasingly prominent within political and media discourse since it was first coined in the 1980s [12]. The meaning of cyberterrorism has proved as troublesome as its 'parent' concept in part because the definitional challenges surrounding terrorism have simply migrated along with its application in the digital realm. This is compounded, however, because the digital realm is itself a site of constant change which is often, as a consequence, poorly understood by researchers and analysts. An outcome of this, as Weimann notes, is a profusion of ill-specified and ill-understood vocabulary such that it has become:

> *especially common when dealing with computers to coin new words simply by placing the words "cyber," "computer," or "information" before another word. Thus, an entire arsenal of words – cyber-crime, cyberwar, infowar, netwar, cyberterrorism, cyber harassment, virtual-warfare, digital terrorism, cybertactics, computer warfare, information warfare, cyberattack, cyberwar, and cyber break-ins – is used to describe what some military and political strategists describe as the "new terrorism" of these times [13].*

This profusion of new terminologies throws up considerable challenges for clarifying terms such as cyberterrorism. Not least amongst these is the inconsistent and interchangeable use of such terms whereby, as Weimann illustrates: "…the mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter" [14]. Thus, while authors such as Stohl argue that it, "continues to be very important to distinguish between cyber crime and cyber terror and that we restrict cyber terrorism to activities which in addition to their cyber component have the commonly agreed upon components of terrorism" [15], doing so is far from straightforward.

This article seeks to contribute to these ongoing discussions by reporting on a recent research project which attempted to capture current understandings of cyberterrorism within the global research community. The project employed a survey methodology, which was designed, first, to explore how academics, research students and others conceptualise and understand cyberterrorism, and second, to chart the prominence and rationale of perspectives on derivative debates around the threat and appropriate responses to this phenomenon, amongst others. The exercise as a whole represented an effort to build on earlier projects which had captured the state of knowledge within terrorism research [16]. Where those earlier publications sought to consolidate and portrait terrorism research at a particular historical moment, this article attempts to do likewise for the concept of cyberterrorism.

Following a brief discussion of our research methodology, this article explores responses we received to two questions asked in our survey. As detailed further below, the first of these questions sought to gauge the level of experience different academics had with twelve terms that occur within academic and policy discussions of cyberterrorism. The second question asked whether respondents to our survey purposefully avoid any of these twelve terms, and if there were particular reasons for doing so. Together, the two questions were designed to explore the terminological boundaries of cyberterrorism, and to investigate what sort of role these 'adjacent' or 'supporting' concepts perform in attempts to make sense of cyberterrorism [17]. Thus,

following Buzan and Hansen, do terms such as 'hacktivism', 'pure cyberterrorism' and 'cyber jihad' function as complementary concepts that work to narrow down the meaning of cyberterrorism by pointing to specific aspects of this phenomenon? Alternatively, are these better thought of as parallel concepts that are used in place of cyberterrorism but in different discussions? Or, are they oppositional concepts: preferred alternatives to, or potential replacements for, cyberterrorism perhaps because of this concept's own complexities? Underpinning all of this was an effort to explore two overarching research questions. First, for contemporary researchers, how does cyberterrorism relate to other concepts? And, second, how familiar, frequently used, and useful are particular terms within the cyber lexicon?

Methodology

The project on which this article reports employed a survey that was distributed to over six hundred terrorism researchers between June and November 2012. A purposive sampling strategy was used to identify potential respondents, a list of which was generated via four methods. The first of these was a targeted literature review, which was employed to identify authors who have published specifically on cyberterrorism on, or since, 1 January 2004 within peer-reviewed journals, monographs, or other scholarly literature. This search was completed using the main catalogue of the British Library and 47 online databases of research [18].

Second, we added to our sample individuals who had published within the four most prominent journals in terrorism research since 1 January 2009, or who were members of the editorial boards thereof: *Terrorism and Political Violence*, *Studies in Conflict & Terrorism*, *Perspectives on Terrorism*, and *Critical Studies on Terrorism*. Although these authors may not have published on cyberterrorism specifically, their standing within the terrorism research community made it reasonable to assume a familiarity with definitional debates around terrorism more widely. Third, we used a 'snowball' method to contact potential respondents identified by researchers who had already returned our survey. And, fourth, we employed targeted advertisements distributed via academic mailing lists maintained by the Terrorism and Political Violence Association, and the British International Studies Association Critical Terrorism Studies Working Group.

Our use of a purposive sampling strategy was, we argue, appropriate to the survey's ambitions given the fluid boundaries of this (and, indeed, any) research community. Although this involves sacrificing any claim to statistical representativeness, it is unclear that such a claim could ever be justified given that research communities constantly change and evolve [19]. In total, our survey generated 118 responses from researchers working in 24 countries across six continents. 117 of these provided geographical information about their working lives, of whom 41 (35% of the total) worked in the United States of America; 32 (27%) in the United Kingdom; 7 (6%) in Australia; and, 4 (3%) in Canada. This weighting toward Anglophone countries is unfortunate but to be expected given the dominance of US – and UK – based researchers within terrorism research. In terms of professional status, 75 (64%) of our respondents were permanent academic staff, with a further 16 (14%) temporary academic staff, and 9 (8%) research students. The remainder of our sample was made up of independent researchers, retired academics and individuals fitting none of the above criteria. In terms of disciplinary background, our sample described themselves in the following way: 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%). This high proportion of researchers identifying with the disciplines of Political Science and International Relations resonates with earlier studies of terrorism research [20].

The survey included a total of twenty questions designed to generate quantitative and qualitative data. These focused on: demographic information; definitional issues around terrorism and cyberterrorism; the cyberterrorism threat; perspectives on countering cyberterrorism; and, assessments of the state of current research in this area. Responses to the survey were anonymised and ordered numerically from R1 to R118.

Findings and Analysis

The two questions explored in this article were numbered eight and nine of our survey. Question eight listed the following twelve cyber-related terms: cracktivism; cybercrime; cyber dissidence; cyber espionage; cyber jihad; cyber militarism; cyber sabotage; cyber vandalism; cyberwarfare; hacktivism; information warfare; and pure cyberterrorism. For each of these terms, respondents were asked to indicate whether they agreed with any of the following four statements: 'This term is one I am familiar with'; 'This term is one I use personally'; 'This term is one that I think is useful'; and, 'This term overlaps with cyberterrorism'. Question nine then asked respondents whether they purposefully avoid using any of the twelve listed terms – and, if so, why – providing a free text box for responses. The following discussion draws on completed responses to each of these questions – responses totalling 89 (response rate 75%) and 73 (62%) respectively. Importantly, 50 respondents indicated that they *purposefully* avoid using one or more of the 12 terms.

As Chart 1 demonstrates, the three terms most familiar to our respondents were also those most likely to be used. These were cyberwarfare, information warfare and cybercrime. By contrast, four terms included in our survey were familiar to less than 30% of respondents: cyber dissidence; cyber militarism; cracktivism; and pure cyberterrorism. Cyber militarism and cracktivism also emerged as rarely used terms, and were the least likely of all of the twelve options to be employed by those familiar with them. As demonstrated in Chart 2, only 22% of those familiar with the term cracktivism reported using it, whilst the figure for cyber militarism was a mere 5%.

The lack of usage of the terms cracktivism and cyber militarism by those familiar with them can be explained, in part, by their deliberate avoidance (as opposed to, for example, having no occasion to use them). As Chart 3 shows, 13 respondents stated they purposefully avoid the term cyber militarism, describing it as ambiguous [21], vague [22] and ill-defined [23]. Whilst some respondents also described cracktivism as vague and ambiguous [24], further reasons were given for avoiding this term. One respondent explained that the term's focus upon one particular technique – cracking (or criminal hacking) – is unhelpful, arguing it is preferable to situate such techniques within broader frameworks of political activism. Others stated that the term adds nothing to existing terminology [25] and risks trivialising this phenomenon [26].

Chart 1: With reference to your own work, what is your experience with the following terms?

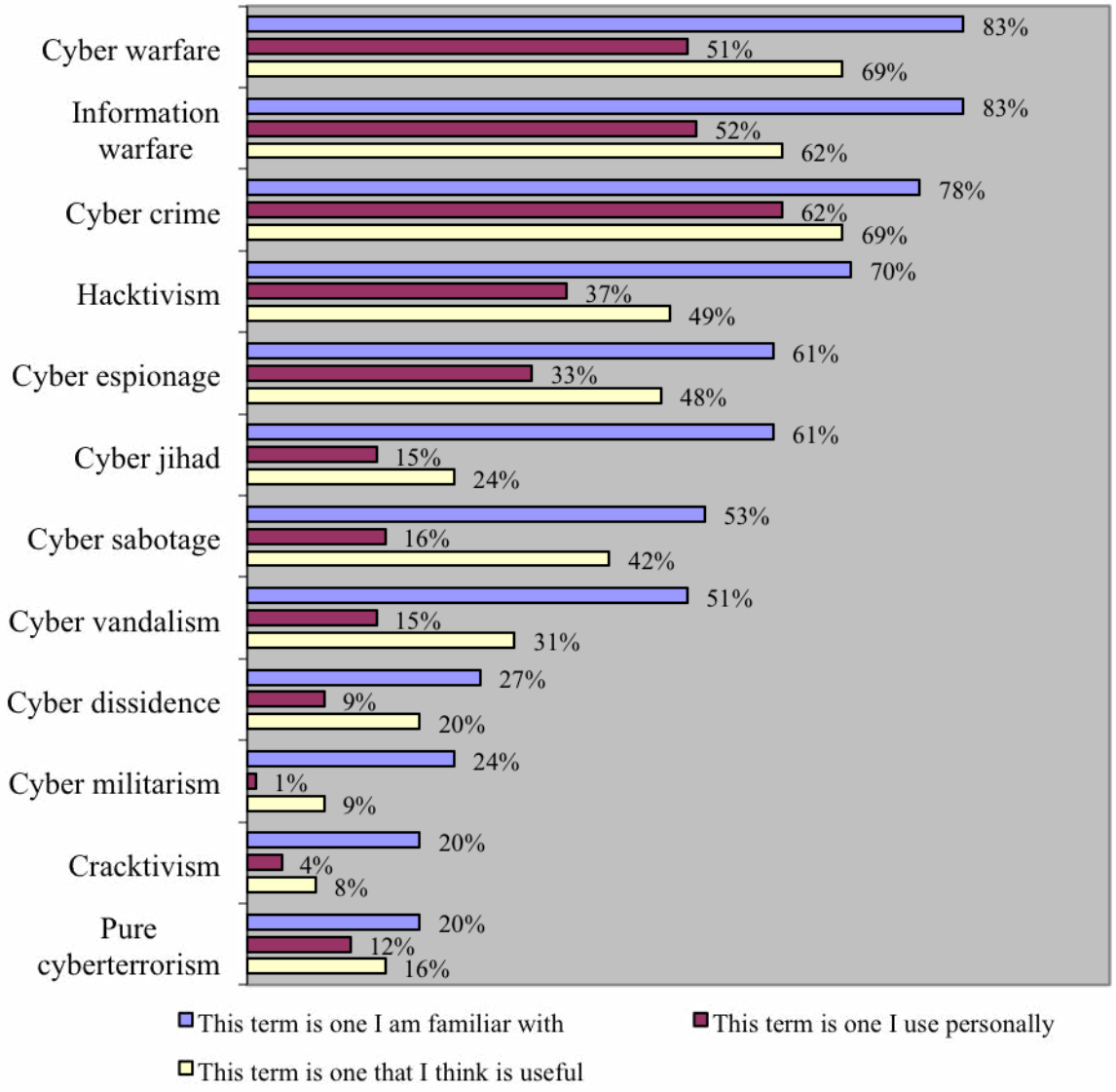
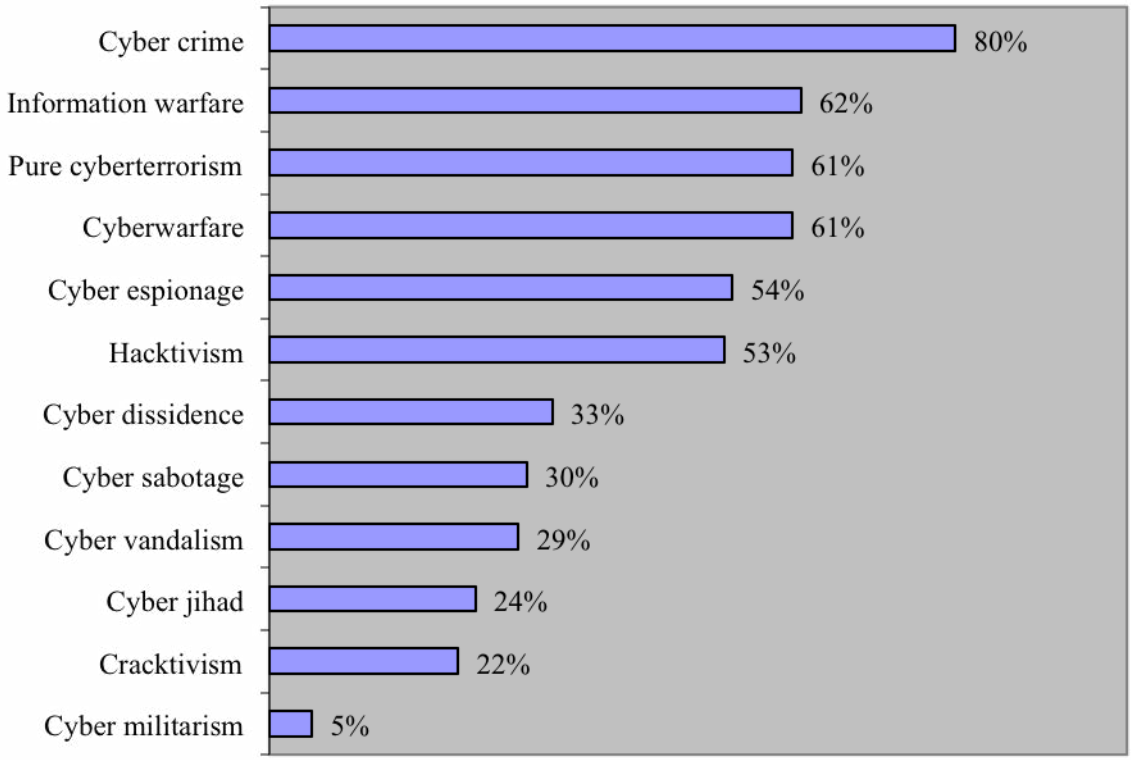
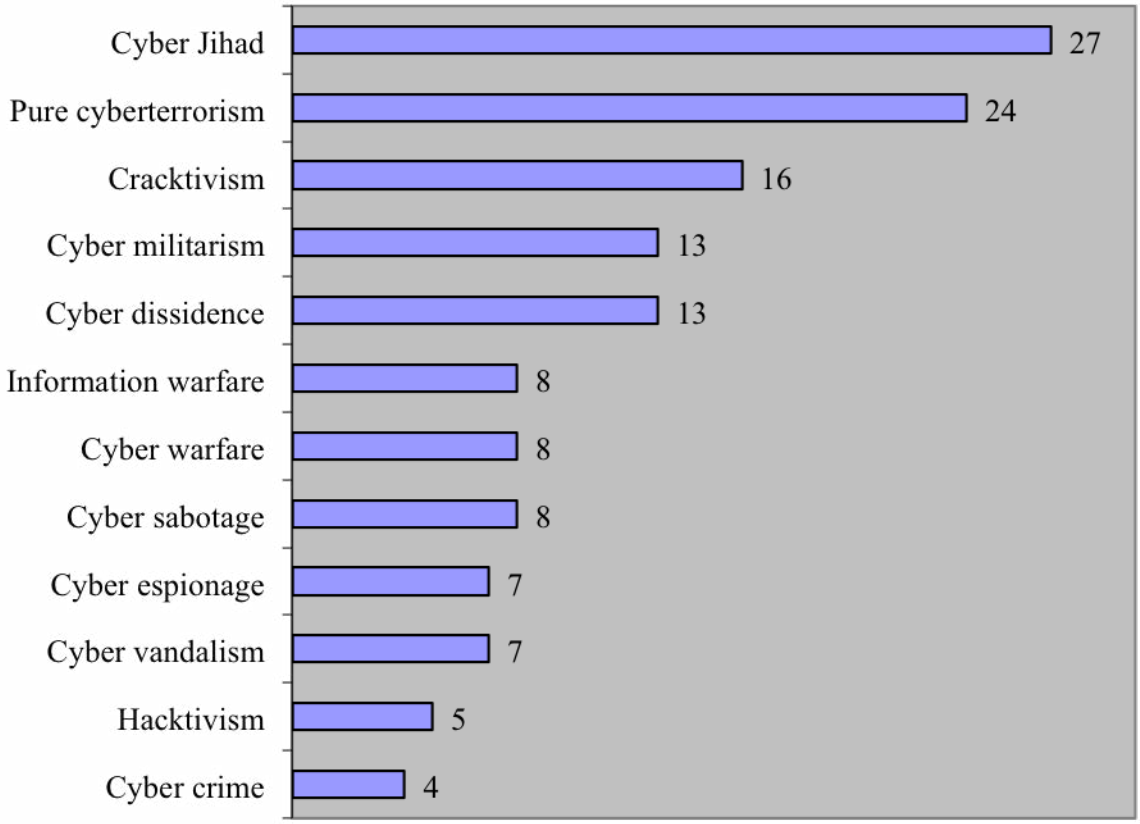


Chart 2: Percentage of respondents familiar with each term that reported using it



The two terms which respondents were most likely to purposefully avoid were cyber jihad (27 respondents) and pure cyberterrorism (24 respondents). The most common reasons given for avoiding cyber jihad were that it is a distortion of the term jihad [27] and that it has damaging social and political consequences [28]. Respondents stated that the term is "unnecessarily loaded except in very specific situations" [29], and that it is, "dangerous because it increases the moral panic already associated with the term Jihad" [30]. Others criticised the term's emphasis upon one particular religion, describing this as "misleading and nonsensical" [31] and "possibly racist" [32], pointing out that non-Muslim groups and states may commit acts of cyberterrorism [33]. Two respondents stated that the term is also unnecessary. One described it as "unjustified" since "there haven't been any acts of cyberterrorism committed by Jihadists" [34]. The other questioned the need to create subcategories of Jihad, asking "Where do we stop? Bus Jihad, Knife Jihad, Shoe Jihad?" [35]. Others still stated that they avoid this term because of how loosely it is used by the media [36] and due to its association with "the problematic concept of new terrorism" [37]. Lastly, one respondent noted avoiding it because it "can be a positive term to many" [38] whilst another said they prefer the term electronic Jihad because this is the term Jihadists "tend to use" [39].

Chart 3: Of the terms listed, are there any which you purposefully avoid? (n.)



The second most avoided term – pure cyberterrorism – was coined by Gordon and Ford in a much-cited contribution to the literature on cyberterrorism [40]. In their view, a narrow focus on pure cyberterrorism – digital attacks against "computers, networks, and the information storied therein" [41] – has the potential to obscure the "true impact" of the convergence of terrorism and cyberspace. Accordingly, they put forward a case for a broad conception of cyberterrorism which encompasses the full range of terrorists' online activities and so recognises the "true threat posed by the addition of acts in the virtual world to the terrorists' playbook" [42]. Narrower understandings of cyberterrorism nonetheless remain far more prevalent in the academic literature [43], and so it is perhaps unsurprising that many respondents avoided using the term pure cyberterrorism. Several stated that the word 'pure' serves no obvious purpose in this context [44], whilst others suggested that its meaning is unclear [45]. Others still argued that the term merely generates additional complexity and uncertainty [46], with one remarking that "it creates more confusion than it seeks to resolve" [47]. At the same time, however, it was apparent that some researchers do find the term useful. Of all twelve terms included in our survey, it was the third most likely to be used by a respondent who was familiar with it.

A number of respondents also used our survey as an opportunity to caution against overly expansive uses of the term cyberterrorism. One commented that terms like cyberterrorism are "problematic" when they are used to "cover all sorts of activity that may not be accurately described as terroristic in nature" [48]. Similarly, another respondent stated:

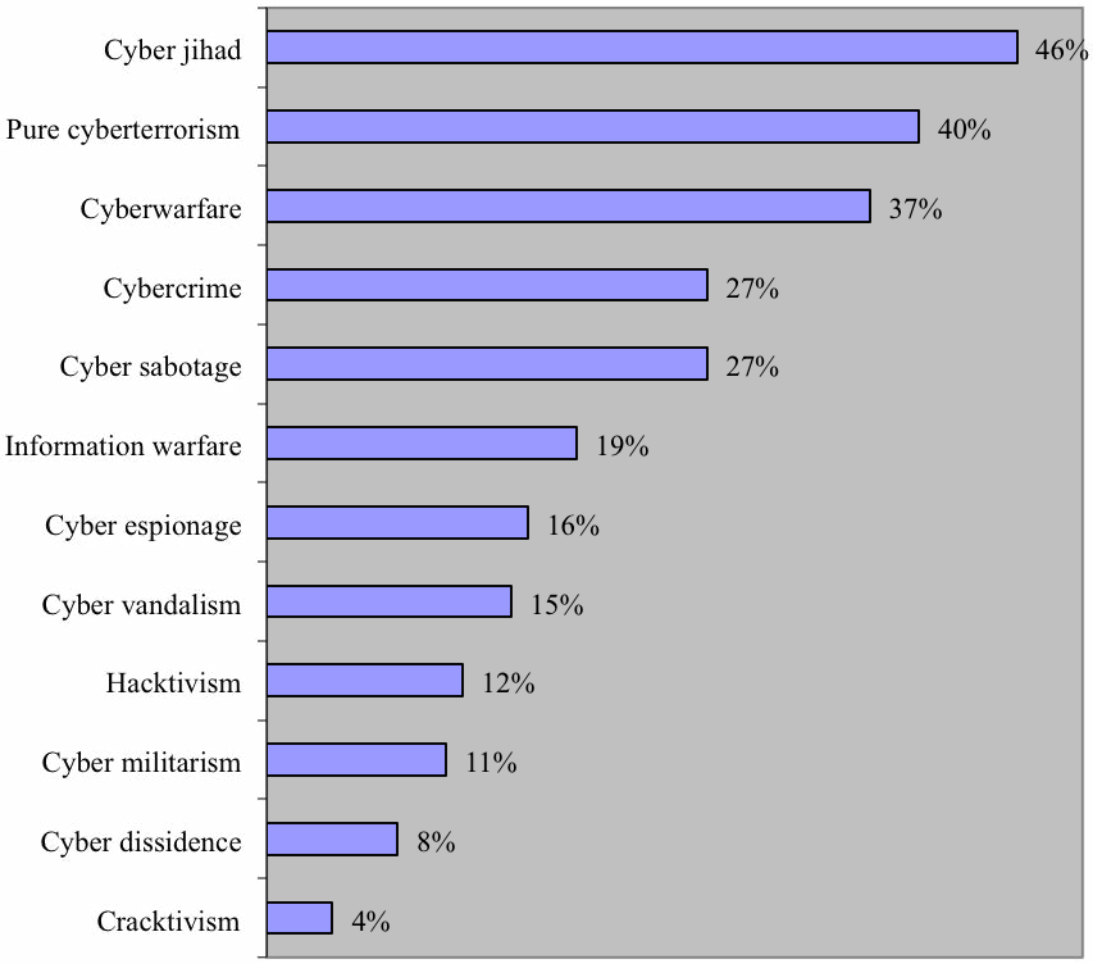
> *Terrorism is normally understood as a political strategy involving violence or its threat. Therefore, the idea of cyberterrorism would seem to be an oxymoron, as it involves no direct violence against individuals. I take the term cyberterrorism to be a state propaganda tactic of demonising certain kinds of*

online criminal behaviour by tarring it with the brush of 'terrorism' [49].

This was echoed by another respondent, who warned against "labelling cybercrime and cyber activism as terrorism" since to do so would "permit a much wider cross section of society to be brought under the terrorism label" [50]. This respondent also warned against using the term cyber dissidence, arguing that it is "loaded". Another respondent criticised the term cyber sabotage for similar reasons, saying that it allows the state to "designate acts of sub-state 'dissidence' or 'resistance' as 'sabotage', resulting in the exaggerated vilification of groups such as "Anonymous" [51].

The final part of question 8 asked respondents to indicate which terms they believed overlap with cyberterrorism. As Chart 4 shows, the highest scores were for cyber Jihad (46%) and pure cyberterrorism (40%). This sense of synonymy, again, may help to further explain the avoidance of these terms by researchers, in that cyberterrorism may be seen as a preferable alternative to these potential 'parallel' concepts.

Chart 4: Which of these terms overlap with cyberterrorism?



There was a similar divergence of opinion regarding the relationship between cyberterrorism and cybercrime. Whilst 27% of respondents stated that these two terms overlap, there were others who emphasised the importance of distinguishing clearly between the two. Various reasons were given for this, including the importance of delineating the scope of special terrorism-related investigative powers and offences [55] and the need to distinguish between law enforcement and intelligence [56]. However, one respondent doubted

whether it will continue to be possible to draw a sharp distinction between cybercrime and cyberterrorism, asking "When terrorists pay criminal organizations to launch an attack, is that crime or terrorism?" [57]. This respondent went on to suggest that "The term 'cyber-disruption' may be more useful for the future". A similar suggestion was advanced by another respondent, who said that the term cyber security is a useful one since it "combats all forms of threats to cyber space" [58].

It is also worth noting that several respondents stated that they avoid using terms within the cyber lexicon altogether. One commented that the "cyber prefix often gets in the way" [59] whilst another stated that trying to distinguish between the cyber and physical realms "usually obscures rather than illuminates the subject" [60]. Others regarded the cyber terminology as sensationalist, describing it as "over-dramatic" and "ambiguous" [61], "overused" [62], jargonistic [63] and "overly contentious and invented for purpose" [64]. In the opinion of one respondent, indeed, the terms "belong to the media rather than academic research" [65].

Finally, Table 1 shows the disciplinary backgrounds of the respondents who stated that they purposefully avoid using one or more of the twelve specified terms.

Table 1: Disciplinary backgrounds and the purposeful avoidance of cyber terminology

	Number of respondents to the survey: n (%)	Number of respondents who stated that they purposefully avoid using one or more of the 12 terms
Political Science/International Relations	69 (50%)	27 (48%)
Law/Criminology	15 (11%)	3 (5%)
Economics/Business	2 (1%)	2 (4%)
Engineering/Computer Science/Cyber	17 (12%)	10 (18%)
Psychology/Anthropology	20 (15%)	8 (14%)
Literature/Arts/History	9 (7%)	2 (4%)
Independent Researchers/ Analysts	5 (4%)	4 (7%)
Total	137 (Note that some respondents selected more than one disciplinary background)	56 (Six of these respondents selected more than one disciplinary background)

Three interesting points emerge from this data. First, whilst 11% of the respondents to the survey came from the Law/Criminology disciplinary group, only 5% of those who stated that they purposefully avoid using one or more of the 12 terms came from this group. Similarly, whilst nine of the respondents to the survey were from a Literature/Arts/History background, only two of these (i.e., 22% of this disciplinary group) stated that they purposefully avoid using one or more of the twelve terms. This is significantly lower than the corresponding figure of 42% for the overall group of respondents (50 out of 118). Second, the fact that slightly less than half of the overall group of respondents stated that they purposefully avoid using one or more of the twelve terms may be contrasted with the findings for three of the disciplinary groups: ten out of seventeen respondents (59%) for those from an Engineering/Computer Science/Cyber background; four out of five (80%) for Independent Researchers/Analysts; and both of the respondents from an Economics/ Business background. Third, researchers from all disciplines – spanning both the social and the physical

sciences – demonstrated an appreciation of, and sensitivity to, the terminological issues that have been described above. This was evidenced, amongst other ways, in the depth and sophistication of the qualitative answers we received in response to these questions, some of which are included in the above discussion.

Conclusion

Given the amount of attention that definitional debates have attracted within terrorism research, it is perhaps unsurprising that respondents to our survey engaged at length with questions designed to explore the connections between cyberterrorism and potentially adjacent concepts. To return to the first of our original research questions – how does cyberterrorism relate to other concepts – a number of our respondents noted that cyberterrorism overlaps with other, related terms especially cyber jihad, pure cyberterrorism, cyber warfare and cybercrime. For a number of researchers in this area, therefore, these terms appear to be adjacent to, or supporting of, the concept of cyberterrorism. Yet, as the qualitative responses discussed above suggest, the relationships between these are complex and open to contestation, with these concepts seen variously as complementary, oppositional, or parallel to cyberterrorism by different researchers.

In terms of our second research question, many of our respondents articulated clear – and frequently persuasive – reasons for the use or avoidance of specific terms in this lexicon. Some of these focused primarily on the terms' explanatory value. Our research encountered considerable overlap between familiarity with a term, its perceived usefulness, and its actual use. Thus, the more settled concepts of cyberwarfare, information warfare and cybercrime topped each of these tables. At the same time, as demonstrated in Chart 3, less familiar terms including pure cyberterrorism and cyber espionage were used by a majority of those familiar with these. This, perhaps, points to the potential future prominence of concepts that are not widely used at present.

Importantly, researchers from the full range of disciplinary backgrounds present in our survey reflected at length on the politics of specific choices of terminology. Here again we can see similarities with discussions on the definition of terrorism that have long combined analytical as well as policy-related justifications for engaging in this activity [66]. As demonstrated above, our respondents' choices of terminology were made on substantive grounds as much as for semantic or aesthetic reasons. These included a desire to avoid stigmatising or criminalising potentially legitimate protest activities (in the cases of 'cracking' and 'hacktivism'), as well as a desire to avoid adding further suspicion to minority communities (in the case of 'cyber jihad'). These concerns, we suggest, demonstrate a widespread sensitivity to the connotations of the cyber lexicon as much as to its denotative functions.

Although important in their own right, the above findings are further significant, we suggest, for two additional reasons. In the first instance, they both demonstrate and provide some empirical measure of contemporary debates around labelling and terminology within research on cyberterrorism. This matters not only because our findings therefore speak to, and allow comparison with, related research projects focusing on terrorism more generally [67] but also because the lexicon surrounding cyberterrorism is still in its infancy. There is, as such, a real opportunity for terrorism researchers to reflect on, engage with, and shape the ways in which activities associated with this terminology are discussed, debated and understood. Therefore, taking stock of researcher attitudes – as this article attempts to do – is a crucial first step toward this.

Second, the findings of our survey are also significant in their pointing to important future research agendas with potential to further contribute to our understanding of the ways in which researchers engage with this – and related – lexicons. To conclude our discussion, we point to three of these now. First, would be a temporal

research agenda. Where our survey presents a 'snapshot' of academic work in this area taken at a particular historical moment there is obvious scope for future work exploring the permanence of the attitudes and perspectives charted above. Such research would enable analysis of the changing political and normative assumptions within work on cyberterrorism, as well as the emergence and decline of new concepts. It could, as such, offer a genealogical, comparative static, or diachronic complement to the synchronic analysis of this research [68].

A second obvious future research agenda would be a comparative analysis of engagements with the cyber lexicon by constituencies away from the academic research community. Such an agenda would involve the exploration of attitudes to, and the use of, terms such as cyber jihad amongst journalists, contributors to social media, policy advisors, employees at cyber security corporations, police forces and so forth. The value here would include an assessment of whether terrorism researchers as an epistemic community (if they may be thought of as such) are particularly attuned to the importance and politics of labelling. Or, whether such concerns travel beyond their discussions in the pages of academic journals and books.

A third area requiring further research is the distinctiveness of the online realm here. For instance, do terrorism researchers encounter similar problems in differentiating espionage, sabotage and war from terrorism? And, do 'offline' equivalents of the twelve terms listed above – such as jihad, militarism, activism and vandalism – display similar levels of familiarity, use, and perceived value? Or, on the other hand, is the distinctiveness of cyberterrorism more blurred than 'terrorism' in general because of the newness of this term and its surrounding lexicon? Work of this sort, we suggest, would complement other on-going research – both by ourselves and by others – on the extent to which there exist differences in the dynamics of terrorists' activities in the online and offline realms.

About the authors: **Lee Jarvis** *is a Senior Lecturer in International Security at the University of East Anglia, UK. He is author of' Times of Terror: Discourse, Temporality and the War on Terror', and co-author (with Richard Jackson, Jeroen Gunning and Marie Breen Smyth) of 'Terrorism: A Critical Introduction'. His research has been published in journals including Security Dialogue, Political Studies, Millennium: Journal of International Studies, International Relations, Terrorism and Political Violence, and Studies in Conflict and Terrorism.* ***Stuart Macdonald*** *is 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. He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney. His recent research on security and liberty was funded by the British Academy.*

Support for this research was provided by the Swansea Academy of Learning and Teaching (SALT), based at Swansea University, UK. The authors wish to express their gratitude to Simon Lavis for his excellent research assistance in this project, and to Tom Chen, Joanna Halbert, Lella Nouri, Andrew Whiting and other members of The Cyberterrorism Project for their time, support and help throughout the research. We also express our thanks to all those who responded to our survey. Any errors remain the fault of the authors alone.

Notes

[1] See Weinberg, L., Pedahzur, A. & Hirsch-Hoefler, F. (2004) 'The Challenges of Conceptualizing Terrorism', *Terrorism & Political Violence* 16(4): 777-794; Schmid, A. P. 'The Definition of Terrorism', in A. P. Schmid (ed.) (2011) *The Routledge Handbook of Terrorism Research*. London: Routledge, pp.39-98, p.43-44.

[2] Hoffman, B. (2006) *Inside Terrorism (Revised and Expanded Edition)*. New York, NY: Columbia University Press, p.23.

[3] English, R. (2009) *Terrorism: How to Respond*. Oxford: Oxford University Press, p.18.

[4] Shanahan, T. (2010) 'Betraying a Certain Corruption of Mind: How (and how not) To Define 'Terrorism'', *Critical Studies on Terrorism* 3(2): 173-190, p.174.

[5] Jackson, R., Jarvis, L., Gunning, J. & Breen-Smyth, M. (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, pp.104-105.

[6] Weinberg, L., Pedahzur, A. & Hirsch-Hoefler, F. (2004) 'The Challenges of Conceptualizing Terrorism', *Terrorism & Political Violence* 16(4): 777-794, p.779

[7] Hoffman, B. (2006) *Inside Terrorism (Revised and Expanded Edition)*. New York, NY: Columbia University Press, p.26

[8] Richards, A. (2013) 'Conceptualizing Terrorism', Accepted Author Manuscript, *Studies in Conflict & Terrorism*. DOI: 10.1080/1057610X.2014.872023, p.3.

[9] See Jackson, R., Jarvis, L., Gunning, J. & Breen-Smyth, M. (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, p.181.

[10] Richardson, L., 2006. *What Terrorists Want: Understanding the Enemy, Containing the Threat*. New York, NY: Random House, p.5.

[11] Stohl, M. & Lopez, G. (1988) 'Introduction' in M. Stohl and G. Lopez (eds.) *Terrible Beyond Endurance?: The Foreign Policy of State Terrorism*. New York, NY: Greenwood Press, pp.1-9; Chomsky, N., 1991. International Terrorism: Image and Reality', in A. George (ed.), *Western State Terrorism*. Cambridge: Polity, pp. 12-38; Blakeley, R., 2007. Bringing the State Back Into Terrorism Studies. *European Political Science*, 6 (3), 228-235; Blakeley, R., 2009. *State Terrorism and Neoliberalism: The North in the South*. Abingdon: Routledge.

[12] Collin, B. (1997) "The Future of Cyberterrorism", *Crime and Justice International* 13, no. 2: 15-18.

[13] Weimann, G. (2005) Cyberterrorism: The Sum of All Fears?, *Studies in Conflict & Terrorism*, 28:2, 129-149, p.135.

[14] Idem, p.132.

[15] Stohl, Michael (2006) "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?." *Crime, law and social change* 46 (4-5): 223-238, p.229.

[16] Andrew Silke (ed.) (2003) *Research on Terrorism: Trends, Achievements and Failures* (Abingdon: Routledge); Schmid, A.P. & Jongmann, A. J. (2008) *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature (2005).* (New Brunswick, NJ: Transaction; Jackson, R., Gunning, J., and Breen-Smyth, M. (eds.) (2009) *Critical Terrorism Studies: A New Research Agenda* (Abingdon: Routledge; Schmid, A. P.(2011b) 'The Literature on Terrorism', in A. P. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. London: Routledge, pp. 457-474.

[17] See Buzan, B. & Hansen, L. (2009) *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, pp.14-15.

[18] The full list of these databases 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.

[19] See Schmid, A. P. (2011b) 'The Literature on Terrorism', in A.P. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. London: Routledge, pp. 457-474.

[20] 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), pp.186-213, p.193-194.

[21] Respondent 57 and Respondent 107, hereafter R57 and R107.

[22] R106.

[23] R19.

[24] R57 and R106.

[25] R7.

[26] R53.

[27] Seven respondents: R5, R12, R15, R19, R43, R77, R97.

[28] Seven respondents: R5, R15, R43, R45, R52, R79, R93.

[29] R79.

[30] R45.

[31] (R5)

[32] R15.

[33] R43.

[34] R45.

[35] R11.

[36] R74.

[37] R101.

[38] R107.

[39] R18.

[40] Gordon, S. and Ford, R. (2002) 'Cyberterrorism?' *Computers & Security*, 21(7): pp. 636-647.

[41] Idem, p. 637.

[42] Idem,, p. 645.

[43] See Jarvis, L. and Macdonald, S. (forthcoming, 2014) 'What is Cyberterrorism? Findings from a Survey of Researchers', *Terrorism & Political Violence*.

[44] R46, R67.

[45] R10, R19, R34, R52, R106, R107.

[46] R35, R100.

[47] R35.

[48] R65.

[49] R26.

[50] R97.

[51] R45.

[52] R64.

[53] R1.

[54] Macdonald, S., Jarvis, L., Chen, T. and Lavis, S. (2013) *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1), Swansea University. Available via: www.cyberterrorism-project.org

[55] R33.

[56] R21.

[57] R59.

[58] R42.

[59] R34.

[60] R21.

[61] R111.

[62] R59.

[63] R72.

[64] R36.

[65] R6.

[66] Jackson, R. *et al* (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, p.107.

[67] For example, Schmid, A. P. 'Introduction', in A. Schmid (ed.) (2011) *The Routledge Handbook of Terrorism Research*. London: Routledge, pp. 1-37.

[68] Hay, C. (2002) *Political Analysis: A Critical Introduction*. Basingstoke: Palgrave, pp.135-150.