Cyberterrorism Today?

Findings from a follow-on survey of researchers

Stuart Macdonald[a], Lee Jarvis[b], and Simon M. Lavis[c]

[a] *Hillary Rodham Clinton School of Law, Swansea University, Swansea, UK*

[b] *School of Politics, Philosophy, Language and Communication Studies, University of East Anglia, Norwich, UK*

[c] *School of Communication, The Ohio State University, Columbus, USA*

Corresponding author: Stuart Macdonald (s.macdonald@swansea.ac.uk)

Cyberterrorism Today?

Findings from a follow-on survey of researchers

This article reports on a survey of researchers designed to capture current perspectives on core questions around cyberterrorism. The survey – conducted in 2017 as a follow-on to an initial, 2012, exercise - focused on questions of definition, threat and response. By documenting our findings in each of these areas – and highlighting developments in the years between our surveys – we identify three particularly important trends. First, an increasing convergence around the core characteristics of cyberterrorism, albeit with continuing conceptual disagreements at the concept's penumbra. Second, increasing researcher concern with the threat posed by cyberterrorism, underpinned by a widespread view that this threat has increased, and a growing feeling that cyberterrorist attacks have now taken place. Third, support for a diversity of counter-measures to this threat, although perhaps counter-intuitively little suggestion that resort to exceptional or draconian measures is needed. In order to inform future research, the article concludes by detailing some of the major limitations, gaps and weaknesses within academic research to date as identified by our respondents.

Keywords: cyberterrorism; cyber terrorism; cybersecurity; terrorism; survey

Introduction

In March 2019, a coordinated attack on two mosques in Christchurch, New Zealand led to the deaths of fifty people. The shootings had a significant impact beyond their immediate victims – even as they unfolded – due to the attacker, Brenton Harrison Tarrant, having "live-streamed footage of his rampage to Facebook, filmed with a head-mounted camera."[1] This use of digital technologies for the live communication of an attack was not qualitatively new: assailants in an earlier, 2013, attack on the Westgate shopping mall in Nairobi, Kenya, for example, had done similar via the social media platform, Twitter.[2] Tarrant's actions, however, served to re-center media and public attention on the relationship between terrorism and cyber-technologies, in this instance as a mechanism for propagandizing one's violences. As one well-known journalist put it shortly afterwards: "Technology is terrorism's most effective ally. It delivers a global audience."[3] Such concerns around the use of cybertechnologies to produce, or augment, security threats, of course, continue to exercise policy communities too. On the very day that the Christchurch shootings were unfolding, no less, media sources in Britain and beyond were also reporting the UK National Audit Office's admonishment of the British government's failure to protect national critical infrastructure from future cyber-attacks.[4]

In 2012, members of the *Cyberterrorism Project* set out to explore the prominence or lack thereof of such concerns amongst academics and researchers working in this field. Drawing inspiration from important earlier efforts to snapshot the terrorism research community, a survey was conducted focusing on researcher understandings of the meaning of cyberterrorism, the threat that it poses, and the appropriate responses to this threat. Key findings from this survey – considered further detail below – included: the existence of widespread support for a specific, stand-alone definition of cyberterrorism – albeit with considerable disagreement on the appropriate content of such a definition;[5] researcher skepticism about the proliferation and value of adjacent terms – especially 'cyber jihad' or 'pure cyberterrorism' – in this context;[6] evidence of a pronounced and important divide between "skeptical" and "concerned" perspectives on the threat posed by cyberterrorism;[7] and, some sympathy for the validity of the proposition that states are capable of engaging in cyberterrorism.[8]

In the years that have now passed since that initial exercise, we have witnessed two developments of relevance to those interested in cyberterrorism. The first is a series of events that might be understood as instances of – or, more cautiously, evidence of the threat posed by – the phenomenon of cyberterrorism. Such events include the Wannacry ransomware attack, which was subsequently estimated to have disrupted 1 percent of all UK National Health Service care over the course of a full week, generating a financial cost of £92million.[9]

Other prominent examples have included Kaspersky's 2012 discovery of the 'Red October' virus, a 2015 attack on TV 5Monde by the 'Cybercaliphate', and the 2017 attacks on Ukrainian targets through the malware Petya. The second is a continuing growth in scholarship on 'cyberterrorism' and related threats, which is indicative of escalating research interest in this area. The importance of these developments encouraged the research team behind the initial survey to repeat our survey of researchers 'five years on'. Doing so, we demonstrate below, enables exploration of epistemic (dis)continuity across this eventful period: facilitating reflection on the impact, if any, of these events upon research perspectives, views and paradigms. This, in turn, provides opportunity for considering the first survey's reliability, and to capitalize on feedback received on our earlier effort by adding, removing or reframing specific questions as appropriate. Thus, as detailed further below, the 2017 survey included 12 repeated questions, 4 reformulated questions and 4 new questions. Finally, by attempting to survey the academic field as constituted in 2017 – rather than simply returning to our original respondents – the follow-up survey also takes account of this research community's fluidity, recognizing that topics such as cyberterrorism are characterized by the emergence of new researchers, research interests, questions and paradigms.

In this article we trace key findings from the 2017 survey based around three themes: definitions, threat assessments, and proposed solutions to cyberterrorism. We offer three arguments. First, although there are continuing – and important – conceptual disagreements around this term, there appears also to exist some convergence around cyberterrorism's core characteristics. Second, our surveys also indicate a growing scholarly concern that the threat posed by cyberterrorism is increasing over time. Third, we show– perhaps counter-intuitively – that this growing sense of threat is not accompanied by increasing support for exceptional or draconian responses. Our evaluation of continuity and change in these areas is, of course, limited to the comparison of two static moments separated by five years, and therefore unable to explore trends in the intervening period (much less predict the continuation of these trends into the future). It does, however, offer the fullest evaluation to date of perspectives within the global research community around these and related questions.

Recent developments in cyberterrorism research

In the period since our first survey of researchers, there has been a notable increase in scholarship around cyberterrorism and related cybersecurity issues. Much of this work continues the focus of earlier scholarship around three big questions: the definition of cyberterrorism, the threat of cyberterrorism, and the issue of how (or how not) to respond to this threat.[10]

To summarize briefly, discussion of definitional issues continues to demonstrate the contestability of this term, highlighting the confusion and disagreement that surrounds its usage.[11] Early reference points within this debate have become, if anything, more prominent with frequent mention made, first, of Barry Collin's purported coining of this term,[12] and, second, of Dorothy Denning's testimony to the House Armed Services Committee's Special Oversight Panel on Terrorism in 2000, from which the most widely-used understanding of this term emerges. Recent interventions, however, do include specific attempts at definition, with the following illustrative of these: "In contrast to conventional terrorism, cyberterrorism employs malicious computer technology rather than kinetic force. But like conventional terrorism, cyberterrorism aims to further political, religious, or ideological goals by harming civilians physically or psychologically"[13]; and, "Cyberterrorism is the ability of terrorists to conduct terrorist actions in cyberspace with the intent of creating violence and destruction on or even death of its target"[14]; and, "Cyberterrorism commonly implies prohibited assaults and hazards against computer systems, computer networks, and the Internet."[15]

Complementary interventions within the contemporary literature offer conceptual clarification by situating cyberterrorism within typologies of cybersecurity challenges,[16] or by focusing on specific instantiations of this phenomenon such as "lone actor cyberterrorism,"[17] or "ideologically motivated cyberattacks performed by far left groups."[18] There has also, importantly, been a growth of critical reflection around the language of cyberterrorism. This includes more pronounced attention to the politics of this terminology and its application to various forms of online activism,[19] and analyses of the lexicon's usage by various actors, especially political executives.[20] These reflections build on earlier reflections oncyberterrorism discourse,[21] while speaking also to contemporary debate on the utility of the 'cyber' prefix more broadly.[22]

Recent work on the threat of cyberterrorism is confronted by the two main challenges of earlier discussion: the conceptual confusion considered above, and a lack of uncontroversial instances of this threat's realization. Thus, while some case study work attempts to document examples of this phenomenon,[23] one remains as likely – in the recent literature – to find: assertions of threat via analogical reasoning, e.g. "The recent successes of hacktivists, however, do highlight the potential threat of cyberterrorism in that a few individuals with little to no moral restraint may use methods similar to hackers to wreak havoc, generate fear, and cause severe injury or death";[24] exercises simulating the consequences of cyberterrorism;[25] or, speculative projections of this threat's *future* severity, for instance:

> it can be assumed that in the offensive sphere, global jihad organizations are able to cause significant damage in a short period of time by receiving services or information from international criminal organizations and/or terror-supporting states. While developing cyber-attack capabilities may require some time in terms of developing malwares and training skilled hackers, purchasing these capabilities online can be done instantly; also, with the support of financial resources as well as manpower from terror-supporting states, cyber-terrorism attacks pose an imminent threat.[26]

Where some of this literature succumbs to the temptation of worst-case scenarios – "potential gains from a successful attack for terrorists could be substantial, ranging from stealing money to fund terrorist actions to crashing national, even global financial markets"[27] – more skeptical perspectives highlight significant governmental attention to cybersecurity,[28] and the risk of threat exaggeration in this relatively ill-understood domain.[29] Although a longstanding concern with the resilience of critical infrastructures remains a key focus of this scholarship on threat,[30] more expansive discussions of the terrorism/internet nexus concentrate upon the propagandistic uses of digital technologies by organizations such as al Qaeda and, especially, Daesh.[31]

A third prominent theme in contemporary scholarship is the viability of various measures for countering cyberterrorism. Legally-oriented work here explores the regulation of internet technologies, often with a focus on the challenges of divergent national jurisdictions and a limited framework of international law.[32] Related research complements this with an emphasis on the political challenges confronting the global governance of cybersecurity threats.[33] At a more micro-level, scholarship has also begun to explore the preparedness and resilience of individuals – either as citizens or as employees of significant institutions – to potential cyberattack.[34] Although, as Futter notes, enhancing individual computer hygiene might be more appropriate for high-frequency, low-level incidents[35] than for the more catastrophic scenarios to which discussion on cyberterrorism is often drawn. Discussion continues too, finally, on the feasibility of deterrence in a realm characterized by attribution difficulties, for instance with Klein arguing:

> Because there appears to be a persistent desire by some terrorist organizations to use any and all means, including cyberattacks, to achieve their desired goals, it is paramount for policy makers and military planners to take preparatory actions to prevent such acts and mitigate any effects should such an attack occur. These preparatory actions include deterrence efforts.[36]

Methodology

The findings discussed in this article draw from two surveys distributed electronically, in 2012 and 2017 respectively, with different purposive sampling approaches utilized in both instances as described below. The purposive approach was best placed to identify potential respondents from our population of interest – members of the global research community working in the area of cyberterrorism – but as a non-probability approach we cannot and do not make claims about the statistical representativeness of our findings. The research community around cyberterrorism is, of course, a dynamic and porous one for which no objective identification of membership is possible. It has also, of course, changed in the five years between our surveys. On top of this, our own backgrounds within specific social scientific disciplines (Political Science, Law and Communication Science), for instance, may have skewed our sample, as may other factors such as our residence in the UK and US.

2012 Sampling Approach

The initial survey was distributed to over 600 identified members of the global research community. Members of this community were identified via four key sampling strategies. First, via a targeted literature review to identify researchers who have published specifically on cyberterrorism within peer-reviewed journals, monographs, edited books, or other literature. The review focused upon the main catalogue of the British Library and 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).[37] The search was limited to publications since 2004.

This review was complemented, second, by active researchers working on terrorism more broadly – identified via recent publication of articles in, and the editorial boards of, the following journals: *Studies in Conflict and Terrorism*, *Terrorism and Political Violence*, *Perspectives on Terrorism*, and *Critical Studies on Terrorism*. These include the two most established journals for terrorism research and (in the latter two) two more recent additions. Taken together they represent the conceptual and methodological breadth within terrorism research today. The third sampling strategy was via a "snowball method" in which potential respondents were identified by individuals who completed the survey. And, finally, targeted requests for respondents were disseminated via the mailing lists of two UK-based academic organizations: the Terrorism and Political Violence Association and the British International Studies Association Critical Studies on Terrorism Working Group.

2017 Sampling Approach

For the 2017 survey we replicated the first three of the sampling strategies used in 2012: a targeted literature review; invitations to active researchers on terrorism, identified via publication of articles in, and the editorial boards of, the four identified journals; and, the snowball method. In respect of the fourth strategy, instead of using the mailing lists of the same organizations as in 2012 we used the mailing list of the *Cyberterrorism Project*. This mailing list included a number of the respondents to the 2012 survey as well as others familiar with our research in the intervening years.

Sample

The 2017 survey generated a total of 120 complete and 4 partial responses from researchers working in 30 countries across 5 continents: this represents a small increase from the 118 responses across 24 countries and 6 continents in 2012. And, as in 2012, our survey demonstrates a similar weighting towards the Anglosphere, with 43 respondents (34.7%) working in the United States (2012: n. 41; 35.0%); 21 (16.9%) in the United Kingdom (2012: n. 32; 27.4%), 8 in Australia (6.5%; 2012: n. 7; 6.0%) and 6 in Canada (4.8%; 2012: n. 4; 3.4%). Of our respondents, 89 identified as permanent members of academic staff (71.8%;

2012: n. 75; 63.6%); 15 as independent researchers (12.1 %; 2012: n. 11; 9.3%); and 5 as research students (4.0%; 2012: 9; 7.6%). On disciplinary background, finally, our sample described themselves thus: Political Science/International Relations: 52 (46.0%; 2012: n. 69; 50.4%); Engineering/Computer Science/Cyber: 18 (15.9%; 2012: n. 17; 12.4%); Psychology/Anthropology: 15 (13.3%; 2012: n. 20; 14.6%); Law/Criminology: 15 (13.3%; 2012: n. 15; 10.9%); Literature/Arts/History: 6 (5.3%; 2012: n. 9; 6.6%); Economics/Business: 1 (0.9%; 2012: n. 2; 1.5%); Other: 6 (5.3%; 2012: n. 5; 3.6%).

As indicated in our discussion of findings below, the 2017 survey maintained a combination of closed and open-ended questions in order to generate both quantitative and qualitative findings. Twelve questions remained the same as the 2012 survey; four questions were reformulated; and, four new questions were posed to reflect changes in academic debate and empirical events since the initial survey. The questions focused on demographic information; definitional issues around terrorism and cyberterrorism; the cyberterrorism threat; the appropriateness of particular forms of response to this threat; and 'state of the discipline' views of current research in this field. In the following, we document our findings around three key themes: definitional issues; threat assessments; and matters of response.

Defining cyberterrorism

Questions one to six of the 2017 survey focused on definitional issues. The first three of these used a five-point Likert scale, asking respondents the extent to which they believed the definitional issues around terrorism in general have been resolved (where 1 was "Not at all" and 5 was "Entirely"); how important they considered the resolution of the definitional issues around terrorism (where 1 was "Not at all" and 5 was "Very important") and how necessary they believed a specific definition of cyberterrorism (where 1 was "Of no use" and 5 was "Essential"). For each question, respondents were asked to enter two scores: one in respect of policymakers and another in respect of researchers. There was also a free text box for respondents to add any additional comments. The mean scores are shown in Table 1.

Table 1: the significance of the definitional issues surrounding terrorism and cyberterrorism, in respect of policymakers and researchers

	Mean scores (Scale responses: 1-5)			
	Policymakers		Researchers	
	2012	2017	2012	2017
To what extent have the definitional issues around terrorism in general been satisfactorily resolved?	2.41	2.36	2.82	2.58
How important is, or was, the resolution of the definitional issues around terrorism?	3.71	3.80	3.61	3.62
How necessary do you believe a specific definition of cyberterrorism to be?	3.73	3.88	3.51	3.83

(The response rates for the individual questions ranged from 97% to 98% in 2017, and from 94% to 100% in 2012)

As Table 1 demonstrates, for all three questions the mean scores in 2017 in respect of policymakers were similar to those in 2012. The slight decrease in respect of the first question (from 2.41 to 2.36) and slight increase in respect of the other two (from 3.71 and 3.79 to 3.81 and 3.88 respectively) are not statistically significant. According to our respondents, then, the definitional issues around terrorism in general and cyberterrorism in particular remain as important to policymakers as they were five years ago but are no closer to being resolved.

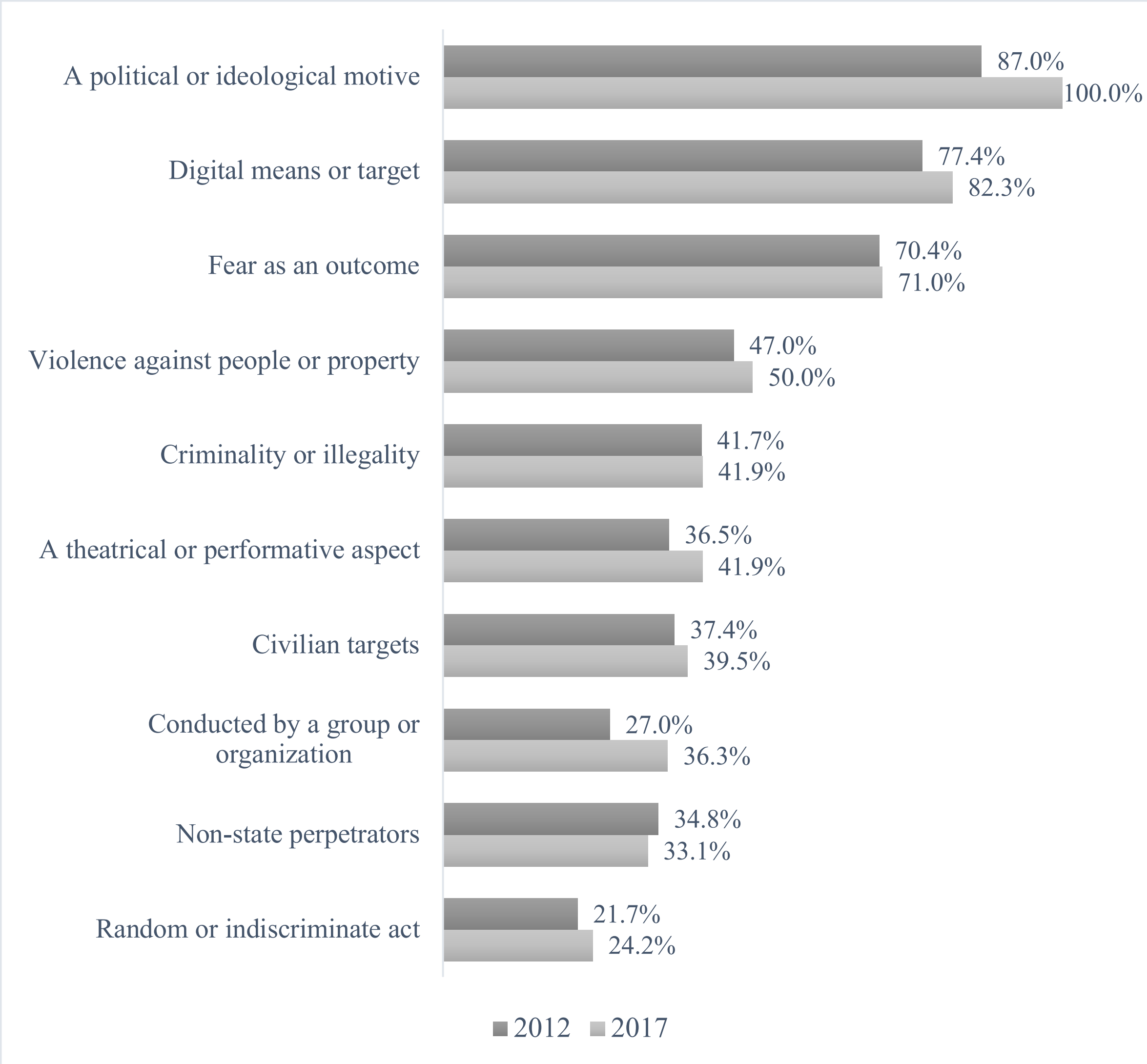
In terms of researchers, the mean score for the second question was almost identical to five years ago (3.615 compared to 3.608 in 2012). Importantly, however, whilst the decrease for the first question (from 2.82 to 2.58) approached, but did not reach, statistical significance (t (241) = 1.748, p = .082), the increase for the third question (from 3.51 to 3.83) is statistically significant, t (239) = -2.263, p = .025. Our respondents thus indicated not only that, for researchers, the definitional issues around terrorism in general remain as important as five years ago and are no closer to being resolved, but also that a specific definition of cyberterrorism is *more necessary* now than it was then.

In their entries in the free text box, respondents to the 2017 survey offered reasons for the importance of definitional clarity. In respect of researchers, the principal reason was analytic clarity. As one respondent stated, without a clearly articulated definition of terrorism, research into the topic descends into a "largely amorphous mass of competing assumptions based on a shifting base" (R7041). In respect of policymakers, the principal reason concerned delimiting the scope of terrorism-related powers. Here, definitional clarity is seen to guide policymakers' decision-making, including decisions about where to direct funding, and guards against the creation and misapplication of overly broad state powers, including the power to prosecute. Some respondents also pointed out that definitional clarity is valuable in facilitating exchanges between the research and policymaker communities.

At the same time, it should be noted that a significant number of respondents expressed skepticism about efforts to define terrorism and/or cyberterrorism. First, some queried the value of the term cyberterrorism itself. One respondent described it as "anachronistic" (R7036), whilst another regarded it as unnecessary: "A proper, strategic definition of terrorism would cover cyberterrorism. The vehicle of delivery is irrelevant to the definition" (R7015). Another suggested that a clear definition of cyberterrorism would involve some sacrifice of flexibility, in that it would restrict the ability of the term to encompass "possible epiphanies of cyberterrorism", i.e., previously unforeseen types of incident (R7062). Second, some opined that the (mis)use of the terms terrorism and cyberterrorism is a greater problem than the construction of a satisfactory definition. For example, one respondent suggested that definitional clarity is unattainable because policymakers wish to retain maximum "rhetorical ambiguity" (R7098), whist another stated that policymakers and researchers alike “continue to subvert the already established scientifically valid definition” for political motives (R7095). And, third, there were some respondents that doubted whether there is any value in seeking to construct unambiguous definitions in the first place, stating, for example, that “Language is too fluid to nail down” (R7080).

Questions four and five sought respondents’ views on the defining features of cyberterrorism. Question four asked respondents to select, from a list of ten items, those characteristics that they considered to be important elements of cyberterrorism. The results are shown in Figure 1.

Figure 1: which of the following are important elements of cyberterrorism?



(The response rates for this question were 99% in 2017 and 97% in 2012)

Two key points emerge from Figure 1. First, for a majority of respondents there are three important distinguishing features of cyberterrorism: a political or ideological motive; digital means or target; and, fear as an outcome. These same three features were identified by a majority of respondents in 2012. It is worth noting that, whereas in 2012 87% of respondents opined that a political or ideological motive is an important element of cyberterrorism, in 2017 this figure increased to 100%, representing a significant increase, $\chi^2(1) = 14.985$, $p < .001$. The second key point, however, is that, notwithstanding this consensus regarding the importance of a political/ideological motive, there remains substantial disagreement around other possible distinguishing features. Not only is opinion split as to whether an act must result in physical harm to people or property in order to qualify as an instance of cyberterrorism, there are also a number of other possible distinguishing features (such as targeting civilians, perpetrated by non-state actors, and conducted by a group or organization) that were considered important by a sizeable minority of respondents.

Question five offered respondents the opportunity to identify (in a free text box) any important elements of cyberterrorism they felt were missing from the list provided in question four. A total of 48 respondents took up this opportunity (response rate: 39%), with four items being identified by at least three respondents. These were: targets critical infrastructure (eight respondents); state sponsored, supported or perpetrated (eight respondents); intention to coerce or compel a target audience (four respondents); and, other targets, e.g., government, military, economic and financial targets (three respondents). This is very similar to the 2012 results, in which four items were also identified by three or more respondents in response to this question, including the first three items above. The difference between the two years was that the fourth most common response in 2017 (other targets) was not amongst the answers offered five years earlier, whereas the fourth most common response in 2012 (demonstration of perpetrator skill/capability) was not offered in 2017.

The divergent understandings of cyberterrorism evidenced in the previous two paragraphs – at least at the penumbra of the term, if not its core – are also illustrated by the responses to question six. The equivalent question in the 2012 survey set out eight different combinations of digital or physical preparation, means and target and asked respondents whether each combination did constitute cyberterrorism, could potentially constitute cyberterrorism, or did not constitute cyberterrorism. Given the reservations expressed by some respondents five years ago,[38] we reformulated this question for the 2017 survey. Question six accordingly set out six hypothetical scenarios and asked respondents whether or not each scenario constituted cyberterrorism (with the additional option to select "Don't know"). The results are shown in Table 2.

Table 2: In which of the following scenarios do the actions of a terrorist group constitute cyberterrorism?

	Constitutes cyberterrorism	Does not constitute cyberterrorism	Don't know
1. A terrorist group interferes with an air traffic control system, causing two passenger aircraft to collide in mid-air	81.5%	6.5%	12.1%
2. Tensions between two communities boil over, resulting in violent rioting. Several people are killed. A terrorist group seeks to further inflame the situation. Posing as members of one of the communities, they post gruesome images and videos on social media and issue threats against members of the other community.	29.8%	61.3%	8.9%
3. A terrorist group remotely accesses the processing control systems of a cereal manufacturer and changes the level of iron supplement. As a result, large numbers of children fall ill, and some die.	81.3%	9.8%	8.9%
4. A terrorist group hacks into the computer system of the nation's stock exchange, sending the national economy into chaos and causing significant economic damage.	76.6%	10.5%	12.9%
5. A terrorist group plants a bomb in the computer control room of the nation's stock exchange. Although no-one is killed, the computers are destroyed, sending the national economy into chaos and causing significant economic damage.	29.0%	63.7%	7.3%
6. A terrorist group plans to hijack a plane and crash it into a busy urban area. They buy their flight tickets online.	6.5%	90.3%	3.2%

(The response rate for this question was 100%, with the exception of the third scenario where it was 99.2%)

As Table 2 shows, for some of the scenarios there was a high degree of consensus amongst our respondents, if not unanimous agreement. 90.3% agreed that scenario six did not constitute cyberterrorism (suggesting that, in contrast to more expansive conceptions, most researchers do not consider acts of digital preparation to be sufficient for an attack to qualify as cyberterrorism[39]). In contrast, 81.5% and 81.3% believed that scenarios one and three respectively did constitute cyberterrorism. These respondents emphasized that in both scenarios the perpetrators had caused serious physical harm via digital means. Yet there were dissenting voices. For scenario one, 12.1% of respondents said that they did not know whether the scenario constituted cyberterrorism or not. The most common reasons for this response were: first, that the wording of the question did not specify the nature of the interference with the air traffic control system (as one respondent remarked, "What does interfere mean? Mess with software or blows it up with a bomb?" (R7102)); and, second, that it would depend on the intention and motive of the perpetrators. A further 6.5% of respondents stated that the scenario did not constitute cyberterrorism. The most common reason was that the attack targeted human life – not a digital system or critical infrastructure – and so should be regarded as terrorism, not cyberterrorism. Turning to scenario three, the most common reasons offered by the 8.9% of respondents unsure whether this scenario constituted cyberterrorism were: first, that it would depend on whether the terrorist group publicly communicated what they had done; and, second, that it would depend on the perpetrators' intention and motive. The 9.8% of respondents that felt that this scenario did not constitute cyberterrorism also emphasized uncertainty over the perpetrators' motive. Some also suggested that the scenario would be better understood as an instance of (industrial) sabotage or cybercrime.

An even more confused picture emerges when looking at the other three scenarios. In response to scenario five, 63.7% opined that it did not constitute cyberterrorism, whereas

29.0% felt that it did. The latter highlighted that the attack had a digital target (the computer network of a nation's stock exchange) (e.g., "Attacking cyber, even with kinetic means, can be cyberterrorism" (R7084)), whereas the former emphasized that a physical, not digital, means of attack was employed (a bomb) (e.g., "Explosives are not cyber means. It would be a terrorist action but not a cyberterrorist one" (R7006)). Opinion was similarly split in response to scenario two. 29.8% opined that this scenario constituted cyberterrorism, emphasizing that digital means (social media) had been used to instigate violence and instill fear. In contrast, 61.3% stated that the scenario did not constitute cyberterrorism. A number of these respondents pointed out that, whilst the terrorist group had used social media, their actions fell short of a (cyber)terrorist attack. Such actions instead – in the view of these respondents – constituted an "information campaign" (R7017), "propaganda" (R7034), "advertising" (R7010) or "incitement" (7025).

Lastly, in response to scenario four, 76.6% of respondents stated that it did constitute cyberterrorism, whereas 10.5% said that it did not. The latter emphasized that, whilst the perpetrators had hacked into the nation's stock exchange and caused significant economic damage, their actions did not result in physical harm to people or property. Similarly, several of the 12.9% of respondents that said that they did not know whether the scenario amounted to cyberterrorism or not also pointed to the consequences of the perpetrators' actions, stating that they would need more information about the "chaos" caused to the national economy to be able to classify the incident. In contrast, a number of the respondents that believed that the scenario did constitute cyberterrorism highlighted the economic harm caused by the perpetrators. This is noteworthy, given that – as we saw above in response to question four – 50% of respondents identified violence against people or property as an important element of cyberterrorism. A considerable proportion of respondents were thus willing to classify this scenario as cyberterrorism notwithstanding their contradictory response to the earlier question.

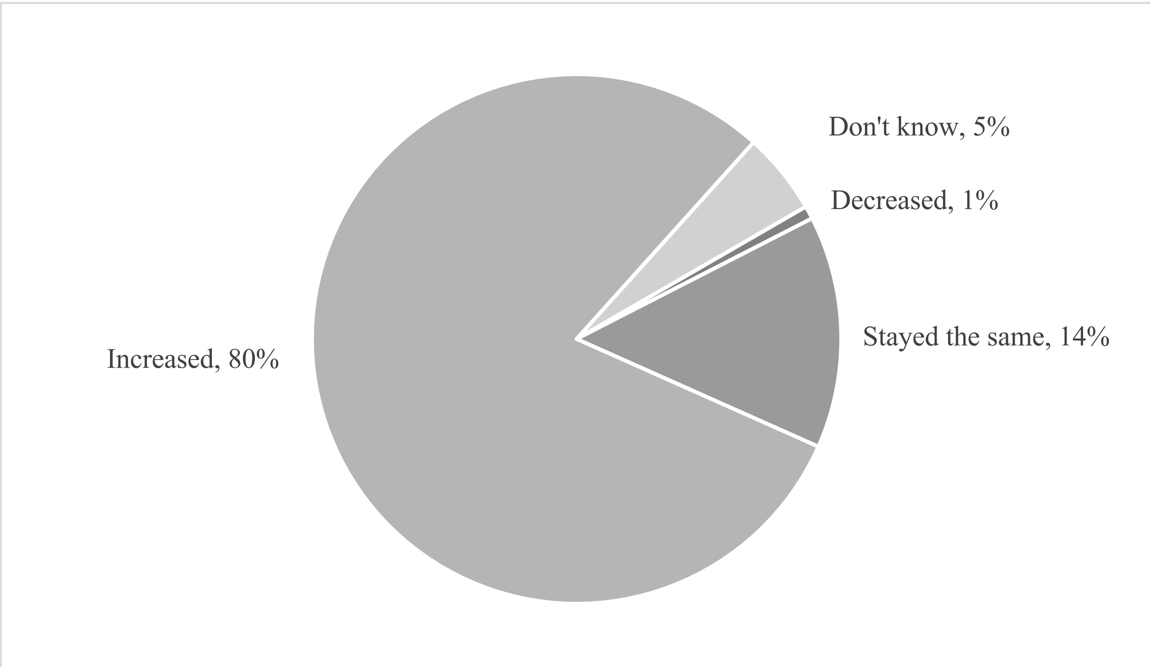
Taken together, the responses to these definitional questions highlight that despite continuing disagreement around its utility there appears to be increasing academic convergence on some of the term's core characteristics. Thus, if debate continues around the importance, for instance, of digital harm or civilian targets, for our respondents at least there is significant and growing agreement on definitional issues relating to motivation and wider societal consequences. This consensus might be indicative of this discussion's maturity; a sense that the key definitional issues and fault lines have now been mapped out. Indeed, it might also be as close as we can come to resolving this definitional question, for – as Alex Schmid argues of the term 'terrorism' more widely: "a full consensus will never be reached. Yet what we can hope for is that a majority of academic analysts can agree on the core elements. There will always be borderline cases where honest people can disagree."[40]

This convergence around cyberterrorism's core features poses important implications for academic discussion. In the first instance, it potentially diminishes the significance of the longstanding debate between 'narrow' and 'broad' understandings of this term.[41] Such positions – read through the lens of our survey, at least – concern the concept's reach, rather than its essence, with a minimal, core understanding of cyberterrorism potentially compatible with each of these. Focusing on this common core understanding may also bear fruit for another – relational – question of definition that runs through this debate, which is: how is cyberterrorism similar to, and/or different from, other phenomena (such as other forms of violence or other online behaviors). Although our survey only allows limited comparison with other cyberthreats, if cyberterrorism's core can be identified with sufficient specificity – as, potentially, indicated by the above – it might, for instance, be possible to differentiate cyberterrorism from other, ostensibly similar, phenomena. If moving toward resolution of these questions through identification of core characteristics is likely to involve a level of abstraction or simplicity some will find unsatisfactory, it does signal (some) hope for a usable, or 'good enough', definition of this term,[42] with all of the benefits for academic debate, policymaking and political critique this may bring.[43] Such a resolution might also, indeed, have implications for our understanding of second order questions around cyberterrorism's threat, and – indeed – appropriate responses to this threat. Yet, as indicated now below, this is less straightforward than one might expect.

Assessing the cyberterrorism threat

Questions seven to thirteen of our survey focused on threat assessment. Question twelve asked respondents whether, in their opinion, the threat level presented by cyberterrorism had changed in the past five years. Respondents were able to select from one of four options: decreased; stayed the same; increased; or, don't know. The results are shown in Figure 2.

Figure 2: In your opinion, has the cyberterrorism threat level changed in the last five years?

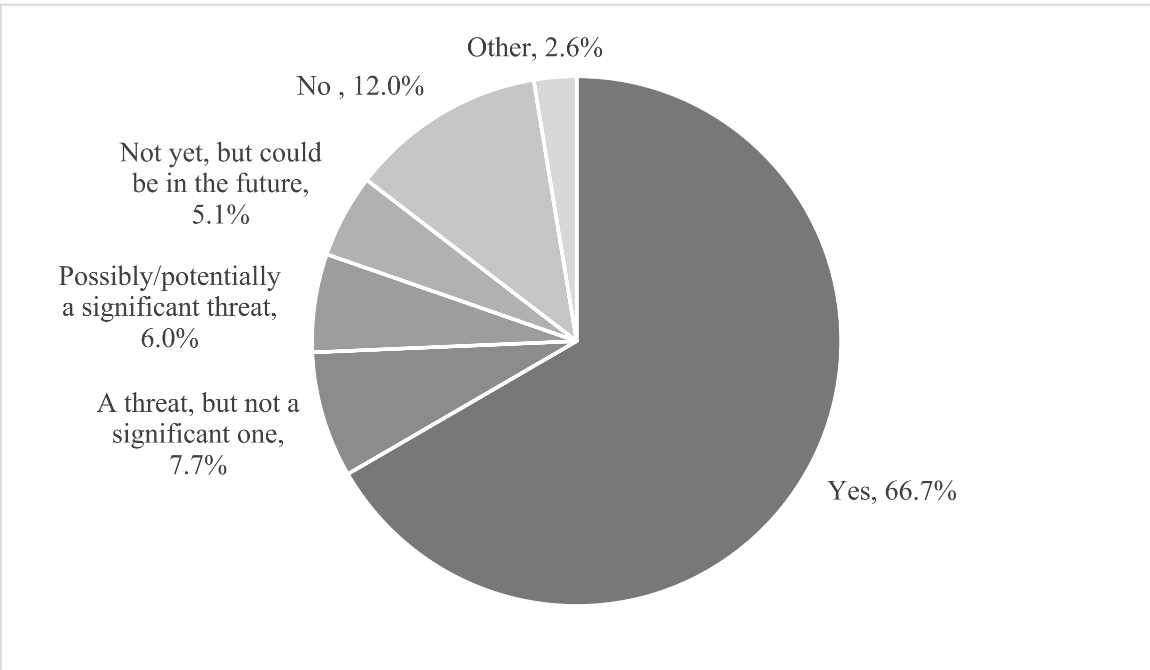


(The response rate for this question was 96.8%)

As Figure 2 shows, a large majority (80.0%) believed that the cyberterrorism threat level had increased in the five-year period from 2012 to 2017. Just one of the 120 respondents that answered this question thought the threat level had decreased (0.8%); all other respondents selected either stayed the same (14.2%) or don't know (5.0%).

The general view that the threat posed by cyberterrorism had increased during this period was also evident in responses to question seven. This question required respondents to assess the seriousness of the threat, by asking: in your view, does cyberterrorism constitute a significant threat? Respondents entered their answers in a free text box. After reviewing the responses, a total of six coding categories were created: yes; a threat, but not a significant one; possibly/potentially a significant threat; not yet, but could be in the future; no; and, other. The frequency of these is shown in Figure 3.

Figure 3: In your view, does cyberterrorism constitute a significant threat?



(The response rate for this question was 94.4%)

In the 2012 survey, 57.2% of respondents answered yes in response to this question, whilst 20.0% answered no. As Figure 3 shows, in 2017 the proportion of respondents that answered yes increased to 66.7% and the proportion of respondents that answered no decreased to 12.0%. Although both of these were sizeable changes, neither the increase in affirmative responses ($\chi^2(1) = 1.399$, $p = .237$) nor the decrease in negative ones ($\chi^2(1) = 2.173$, $p = .140$) reached statistical significance.[44] A number of those respondents who answered yes pointed to a growing dependence on cyber (including the Internet of Things) and/or vulnerabilities in existing systems. For example, one commented: “The combination of increased risk as more elements of our society become cyber-related and the lack of security as shown by recent successful malware attacks indicate that this is a significant risk” (R7064). In contrast, those who answered no tended to focus instead on whether terrorist groups have the capacity needed to commit a cyberterrorist attack. For example, one stated “Not for the moment considering the capacities of most terrorist groups” (R7049), whilst another remarked that “So far, at least, terrorists lack the capability to carry out what I would consider to be true cyberterrorism” (R7052).

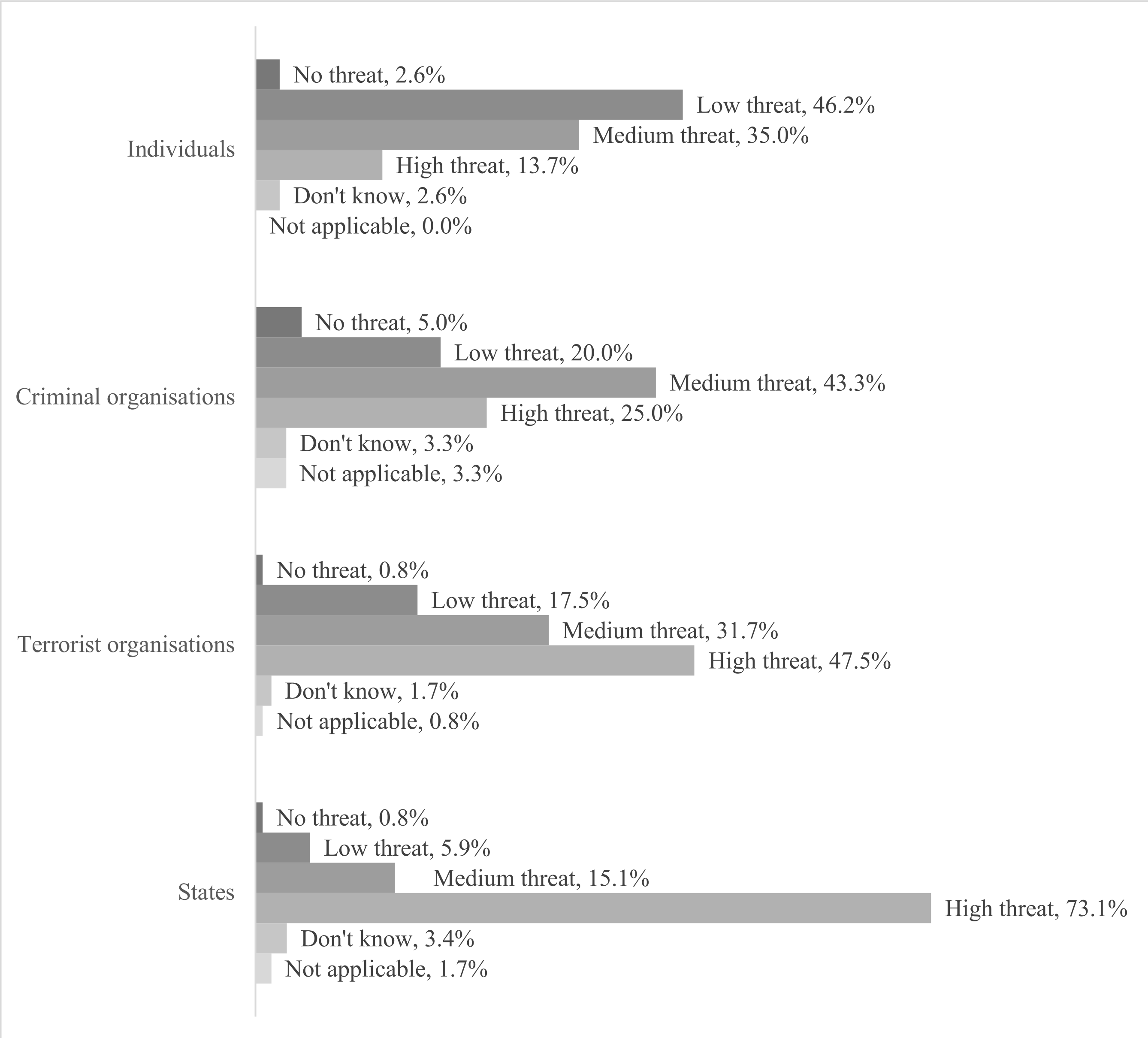
In the 2012 survey, three further coding categories were created besides yes and no: possibly/potentially (11.8% of respondents); unsure (5.5%); and, other (5.5%). To reflect respondents’ answers to the 2017 survey as closely as possible, it was necessary to refine this list.[45] A total of 5.1% of respondents opined that cyberterrorism is not yet a significant threat but could be in the future. One, for example, said “Not at the moment. It probably will in the future, but we are not there yet” (R7050). A further 6.0% stated that cyberterrorism is possibly, or potentially, a significant threat. In contrast to the not yet responses, the possibly/potentially responses suggested that the threat of cyberterrorism is a present one, albeit one that has not yet materialized. As one respondent stated, “A significant potential threat. It has not really been operationalized by groups and individuals yet” (R7058).

Meanwhile, some respondents (7.7%) considered cyberterrorism to be a threat, but not a significant one. Some of these respondents explained their answer by comparing the threat of cyberterrorism to other cyber threats (such as "cyber-enhanced interstate conflict or cybersabotage" (R7011)) or other forms of terrorism that they regarded as posing a graver threat (e.g., "Cyberterrorism constitutes a threat, but not a significant one. Probability of other attack forms (mass shootings, IEDs, suicide attacks) is more likely" (R7064)). Others offered an alternative, lesser description than significant (e.g., "Between medium to high, but not significant at this juncture" (R7020); "I'd say it constitutes a slight threat – or some description in between slight and significant. It's a low to moderate problem" (R7034)).

Question eight built on the previous question by asking: If so, against whom or what is the threat focused? Again, a free text box was provided for respondents. The response rate was 74.2%. There was a total of four different threat referents identified by ten or more respondents: governments/states (28 respondents); critical infrastructures/computer networks (26 respondents); civilians/individuals (26 respondents); and, organizations/private sector/economy/corporations (19 respondents). This is very similar to the responses received in the 2012 survey, in which governments/states (23 respondents), followed by critical infrastructures/computer networks (19 respondents) and then civilians/individuals and organizations/private sector/corporations/economy (10 respondents each) were the most commonly cited referents or targets.

Questions nine, ten and eleven were new questions not included in the 2012 survey. Each sought to probe a different aspect of respondents' perception of the cyberterrorist threat: actors; origins; and, vulnerabilities. Question nine asked respondents to specify the threat level (none, low, medium, or high) posed by four different types of actor: individuals; criminal organizations; terrorist organizations; and, states. Respondents were also given the opportunity to specify any other actors not represented in the question. The results are shown in Figure 4.

Figure 4: What, in your opinion, is the cyberterrorism threat level posed by each of the following actors?



As Figure 4 shows, respondents not only implicitly recognized that states may engage in cyberterrorism – something explicitly addressed in the 2012 survey[46] – they also felt that states posed the greatest threat. 73.1% of respondents opined that states present a high threat, with a further 15.1% stating medium threat and only 5.9% answering low threat. In the view of our respondents, then, states pose a significantly greater threat than terrorist organizations; less than half (47.5%) of respondents believed that terrorist organizations pose a high threat of cyberterrorism. The lowest threat levels were associated with criminal organizations (where the most common response was medium threat (43.3%)) and individuals (most common response: low threat (46.2%)). In terms of other actors, the most common responses were "groups" or "networks" of individuals (five respondents) and hacktivists (four respondents). Five respondents also declined to name specific actors, commenting on the difficulty or futility of attempting to do so given the nature of cyberterrorism.

Questions ten and eleven asked respondents from where in the world cyberterrorism is most likely to emerge, and where in the world is most vulnerable to cyberterrorism. For both questions a free text box was provided. Responses were categorized into five groups, which are shown in Table 3.

Table 3: Anticipated origins of and vulnerabilities to cyberterrorist attacks

	From where in the world is cyberterrorism most likely to emerge?	Number of respondents	Where in the world is most vulnerable to cyberterrorism?	Number of respondents
Specific locations	Russia	31 (25.0%)	United States	20 (16.1%)
	China	16 (12.9%)	China	3 (2.4%)
	North Korea	8 (6.5%)	Russia	3 (2.4%)
	United States	6 (4.8%)	Canada	2 (1.6%)
	Israel	3 (2.4%)	Japan	2 (1.6%)
			United Kingdom	2 (1.6%)
Broad geographic locations/regions	Anywhere/everywhere	27 (21.8%)	The West/Western countries	11 (8.9%)
	Middle East	13 (10.5%)	Anywhere/everywhere	10 (8.1%)
	Asia	4 (3.2%)	Europe/the EU	9 (7.3%)
	Soviet Union or Eastern Europe	4 (3.2%)	Western Europe	5 (4.0%)
	The West	4 (3.2%)	North America	3 (2.4%)
	An Arab location	2 (1.6%)		

State-related descriptors	States (no further qualification)	7 (5.7%)	References to states indicating a positive development status	4 (3.2%)
	Non-state	2 (1.6%)	References to states indicating a negative development status	3 (2.4%)
	Rogue states	2 (1.6%)		
	State-supported	2 (1.6%)		
Party or identity-based classifications	Terrorist(s)	5 (4.0%)		
	ISIS	3 (2.4%)		
	Islam/Islamic	3 (2.4%)		
	Al-Qaeda	2 (1.6%)		
	Intelligence agencies	2 (1.6%)		
Non-geographic or participant-specific classifications	Developed places	3 (2.4%)	Developed places	11 (8.9%)
	Developing places	3 (2.4%)	Dependent places	8 (6.5%)
	Places facing conflict	2 (1.6%)	Reliant on networks	6 (4.8%)
			Connected places	5 (4.0%)
			Developing places	5 (4.0%)
			References cyber	4 (3.2%)
			Includes society/societies	4 (3.2%)
			References technology	4 (3.2%)
			Includes advanced	3 (2.4%)
			References economy	3 (2.4%)
			References networks	3 (2.4%)
			Democracies	2 (1.6%)
			The Third World	2 (1.6%)

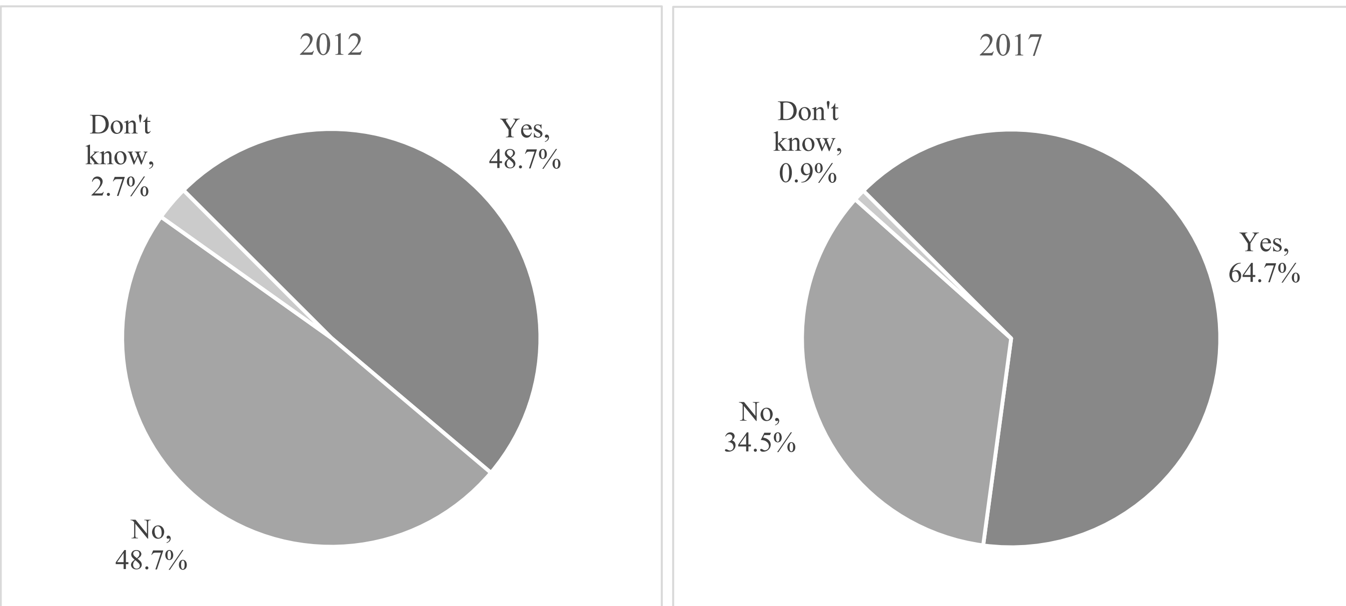
(The response rates for these questions were 83.0% and 79.8% respectively. Only those responses that were mentioned by two or more respondents are displayed).

In terms of from cyberterrorism's likely geographical origins, a significant proportion of respondents answered anywhere or everywhere (21.8%). Of those that offered specific countries or regions, the most common answers were Russia (25.0%), China (12.9%), the Middle East (10.5%) and North Korea (6.5%). In keeping with the responses to question nine, a number of respondents also offered a state-related descriptor. As well as simply the word 'states', with no further qualification, these descriptors included: rogue states (two respondents); state-supported (two respondents); state-related (one respondent); and, states with terrorism (one respondent).

In terms of vulnerability to cyberterrorism, although a number of respondents (8.1%) again stated anywhere and everywhere, others focused on levels of national development. These generally emphasized either a state's developed (8.9%) or positive development status (3.2%) or its dependence on digital systems (e.g., dependent places (6.5%), reliant on networks (4.8%), connected places (4.0%)), but there were also a small number of responses that emphasized a state's developing (4.0%) or negative development status (2.4%). Of those that offered specific countries or regions, the most common answers were the United States (16.1%), the West (8.9%), Europe/the EU (7.3%) and Western Europe (4.0%).

Question thirteen (which also appeared in the 2012 survey), finally, asked respondents whether, in light of their previous answers, they considered a cyberterrorist attack has ever taken place. Respondents were able to select either yes, no or don't know, with a free text box for elaboration. Figure 5 compares the responses from the two years.

Figure 5: With reference to your previous responses, do you consider that a cyberterrorist attack has ever taken place?



(The response rates were 96% and 93.6% in 2012 and 2017 respectively)

Whilst opinion had been equally split in 2012, in 2017 a majority (64.7%) considered that a cyberterrorist attack has taken place, which was significantly higher, $\chi^2(1) = 5.324$, $p = .021$. In their explanations, respondents identified a total of 26 different incidents that they regarded as instances of cyberterrorism. Seven of these incidents were mentioned by two or more respondents.[47] They were: Stuxnet (eight respondents); attacks on Ukraine (five respondents); WannaCry ransomware (five respondents); attacks on Estonia (four respondents); interference in the 2016 U.S. Presidential election (three respondents); Petya ransomware (two respondents); and, attack on TV5Monde (two respondents). It should be pointed out, however, that in the eyes of some of our respondents it is contestable whether these incidents do in fact constitute examples of cyberterrorism. Indeed, some respondents expressly mentioned several of these incidents to explain why there has *not* yet been a true instance of cyberterrorism. For example, one remarked “I don’t think any of the cases that we know of, e.g., Estonia, Stuxnet, ransomware, identity theft, and the 2016 US election are examples of cyberterrorism” (R7001). In the opinion of these respondents, examples like those listed above lack at least one important feature of cyberterrorism. Six respondents observed that cyberattacks to date have been committed by perpetrators lacking the intention to create terror and/or a political motive; five respondents stated that cyberattacks to date have not resulted in violence against people or property; four commented that cyberattacks to date have not been severe enough to qualify as cyberterrorism; and, three said that cyberattacks to date have not been perpetrated by non-state actors.

Just as the above discussion of definitional matters indicated some measure of convergence around cyberterrorism’s core characteristics, here we find (even greater) convergence on this question of threat amongst the global research community.

Cyberterrorism – as seen above – is now widely seen as a significant threat to various referents. And, indeed, very widely seen as a threat that has increased in the five years since our original survey. Notwithstanding important instances of dissent and disagreement noted above, when the responses to our questions are combined, we encounter a dominant construction of cyberterrorism's most threatening incarnation as: (i) a state-led activity, (ii) potentially emanating from anywhere, but (iii) with especial risk posed by Russia, China, North Korea and the Middle East, and (iv) with the greatest vulnerability being found in developed states heavily reliant on digital systems, (v) in particular the United States, Europe or the West more broadly.

This increasing researcher concern with the threat posed by cyberterrorism is noteworthy, in part, because it does not – as indicated above – appear to stem from empirical developments in the years between our two surveys. Many of the most widely cited examples of cyberterrorism from our 2017 survey pre-dated our initial, 2012, research (Stuxnet, and the cyber-attacks in Estonia and Ukraine). Indeed, occurrences that had taken place in the intervening period received only twelve mentions in total in the 2017 survey. It might, perhaps, be the case that those earlier events either continue to resonate as very contemporary (perhaps because of continuing media and academic attention) and are therefore still taken as indicative of current or future threats. Alternatively, it might be the case that more recent, if lower profile, events have served to augment more generalized perceptions of threat, even if earlier, more noteworthy, events such as Stuxnet are the ones which come to mind when examples are sought from researchers. Alternatively still, and perhaps counter-intuitively, it might even be the case that the very *absence* of obvious cyberterrorist attacks in the years surrounding our surveys is interpreted as evidence of a growing threat. To borrow Joseba Zulaika's argument of terrorism more broadly, concern with cyberterrorism might represent an instance in which "the most ominous sign is the absence of a sign, which only confirms that this has to be simply the lull before the storm. It can only be the silence of the enemy while plotting the unknown sudden attack."[48]

Two additional explanations for a growing concern with the threat posed by cyberterrorism relate to epistemological rather than empirical developments in the years between our surveys. It might be the case that some of the more prominent examples - or the significance thereof for inferences around the future of cyberterrorism (such as, perhaps the Stuxnet attack, or the attacks in Estonia) – were less familiar to respondents of our earlier survey than those who completed its 2017 incarnation. Alternatively, it might be the case that the meaning and significance of those earlier events is now being reconsidered in light of new academic understandings or norms. The re-interpretation of past events is, of course, commonplace, witnessed in recent debates around the parameters of sexual harassment in light of the #metoo movement, and – indeed – periodic public discussions about the need for contemporary apologies for historical wrongs such as colonialism or slavery. It might, therefore, be the case that events not previously entering cyberterrorism's discursive orbit are now treated as such due to transformations in understandings of this threat, with implications for assessments of the present/future threat that it poses. Although our survey findings cannot confirm or repudiate such explanations, there is a tension here with the definitional questions discussed in the preceding section which appeared to point to a convergence around cyberterrorism's core characteristics, rather than new or unusual ways of reworking our understanding of this term to facilitate its stretching.

A third form of explanation – not incompatible with some of the above – is that a growing researcher concern around cyberterrorism represents a response neither to empirical or epistemological developments, but rather to a growing securitization of this threat in the intervening period. A range of studies have explored the processes to which cyberterrorism and related threats have been securitized – by which we mean depicted or constructed as exceptional threats to security – in media discourse, political language, popular culture and beyond.[49] As Myriam Dunn Cavelty puts it, in an exploration of US cybersecurity discourse:

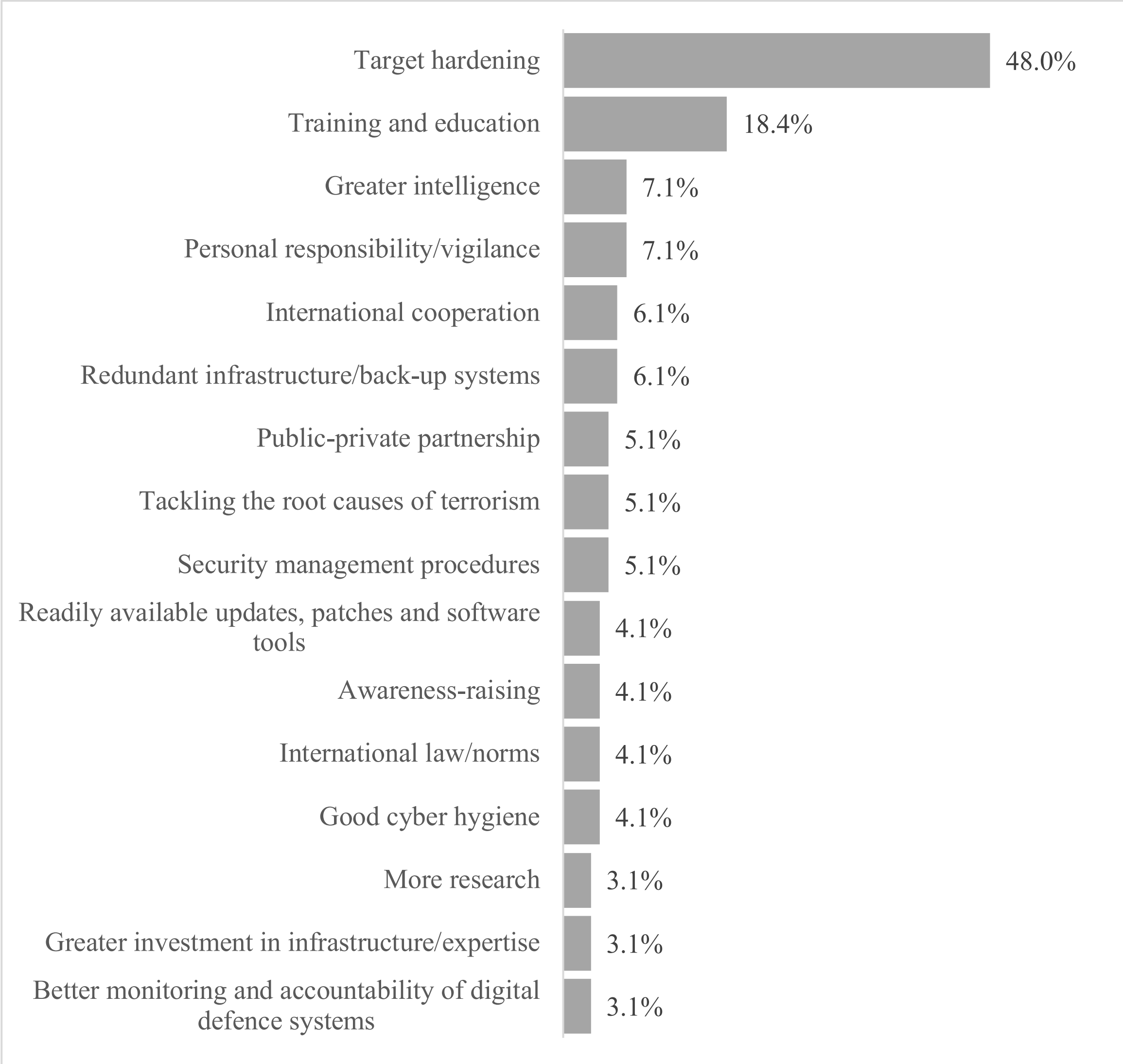
> The cyber-terror frame as a sub-theme of the general cyber-threats frame combines two of the great fears of the late 20th century: The fear of random and violent victimization and the distrust or outright fear of computer technology, which both feed on the fear of the unknown (Pollitt, 1997). Terrorism is feared, and is meant to be feared, because it is perceived as being random, incomprehensible, and uncontrollable. Technology, including information technology, is feared because it is seen as complex, abstract, and arcane in its impact on individuals.[50]

This widespread securitization of cyberterrorism – and other cyber threats – is not limited to the time period of our surveys but there might again be a temporal lag at work here. Such an explanation also, of course, displaces rather than resolves the underpinning explanatory question (why is cyberterrorism being constructed as such a significant threat anywhere?). Yet, if this securitization is part of the explanation for growing researcher concern, then we might also expect to see recommendations on how best to respond to this threat situated within a similarly securitized logic of exceptionalism, rather than more moderate, banal practices of normal politics and routine security. The following section turns precisely to this question.

Responding to the cyberterrorism threat

The final three questions of our survey focused on issues of response. Question fourteen asked respondents: in your view, what are the most effective countermeasures against cyberterrorism? Answers were entered into a free text box. Figure 6 shows the sixteen countermeasures that were mentioned by at least three respondents.

Figure 6: In your view, what are the most effective countermeasures against cyberterrorism?



(The response rate for this question was 79.0%).

The same question appeared in the 2012 survey. As in 2012, by far the most common response was target-hardening (37.6% in 2012; 48.0% in 2017). Five more of the countermeasures shown in Figure 6 also appeared in the top twelve responses received in 2012: greater intelligence; international cooperation; public-private partnership;[51] tackling the root causes of terrorism;[52] and, more research. However, there were also some notable differences between the two sets of responses. First, the respondents to the 2017 survey produced a much longer list of countermeasures. In the 2012 survey there were 93 respondents who answered this question and a total of twelve countermeasures that were mentioned by two or more respondents. In contrast, in the 2017 survey there were 98 respondents who answered this question and a total of twenty-four countermeasures that were mentioned by two or more respondents.[53] Arguably, this more extensive list of countermeasures reflects the attention that the topic received during the five years between the surveys. Second, when examining the countermeasures that were identified in 2017 but not five years earlier, certain themes emerge. One of these is the importance of the human factor. In addition to the second most common response – training and education (18.4%) – respondents also mentioned personal responsibility/vigilance (7.1%), awareness-raising (4.1%) and good cyber hygiene (4.1%). Another theme was the importance of regulation, with respondents mentioning security management procedures (5.1%), international law/norms (4.1%) and better monitoring and accountability of digital defense systems (3.1%). These themes supplement those of resilience/prevention, intelligence, cooperation and collaboration and addressing the root causes of terrorism that were evident in both 2012 and 2017.

Question fifteen asked respondents to identify the most pressing issues in the realm of cyberterrorism for policymakers, whilst question sixteen asked them to identify the major limitations, gaps, or weaknesses within academic research into cyberterrorism. For each question, a free text box was provided for answers. Table 4 shows the most common responses.

Table 4: Most pressing issues facing policymakers and researchers

What are the most pressing issues in the realm of cyberterrorism for policymakers?		What are the major limitations, gaps, or weaknesses within academic research into cyberterrorism?	
Resilience/protection of critical infrastructure and the Internet of Things	19.4%	Access to data	30.9%
New national and international	14.0%	Lack of definitional consensus	14.4%

laws, norms and regulations			
Not exaggerating or distorting the threat	9.7%	Fragmented/siloed research community	9.3%
Educating the public and policymakers	8.6%	Lack of financial support/resources	9.3%
Defining cyberterrorism	7.5%	Need a better understanding of whether terrorist groups plan to commit cyberterrorist attacks (and what might cause them to do so)	7.2%
Coordination and collaboration across different jurisdictions and stakeholders	7.5%	Some researchers exaggerate the threat/the issue does not exist	7.2%
Conducting threat assessments	6.5%	Lack of cyber knowledge	6.2%
State activities in cyberspace	4.3%	Lack of government and industry collaboration with academia	5.2%
Anonymity and attribution	4.3%	Weak theoretical/conceptual analysis/research tends to be too descriptive	4.1%
The human factor/individuals' poor security practices online	3.2%	Existing research is insufficiently practical	2.1%
Provision of training	3.2%	Lack of a focus on vulnerabilities	2.1%
Responding to the threat whilst ensuring respect for human rights	3.2%		
Investment	2.2%		
Keeping pace with technology	2.2%		
Developing effective protocols	2.2%		
Reorganising governmental structures and defence systems	2.2%		

(The response rates for these questions were 75.0% and 78.2% respectively. Only those responses that were mentioned by two or more respondents are displayed)

As Table 4 shows, the most common response to question fifteen was resilience/protection of critical infrastructure and the Internet of Things (19.4%). This was also the most common response to this question in 2012. In fact, six of the seven most common responses in 2017 also featured amongst the seven most common responses in 2012.[54] Beyond these, and in keeping with the answers to question 14, respondents in 2017 also emphasized the importance of educating the public and policymakers (8.6%), as well as of training (3.2%) and the human factor (3.2%). State activities in cyberspace was also identified as a pressing issue for policymakers; this reflects the responses to the threat assessment questions discussed above.

As argued above, findings from our survey indicate that the research community has, first, increasingly converged on a core understanding of cyberterrorism, and, second, become increasingly concerned with the threat that cyberterrorism poses. If this does indicate a growing securitization of this phenomenon, it is interesting that the findings discussed in this section demonstrate two features one might not expect. First, is considerable diversity in the range of responses identified by respondents, albeit with a far stronger concentration on one measure – target-hardening – than in previous years. This diversity might indicate increasing researcher literacy around cybersecurity challenges and the range of potential responses that may be employed against this threat. Alternatively, it might be connected to the problem's complexity – and the need for a range of technical, legal, and political mechanisms for its address.

It is also interesting – in light of increasing researcher concern with cyberterrorism's threat – that so many suggested responses lack the exceptionality we would typically expect when an issue has become successfully securitized. Indeed, there is considerable overlap between our survey findings and the recent academic literature discussed at this article's outset in which human responsiveness and cyber hygiene feature prominently. Beyond this emphasis on the everyday or banal work of citizens, there is also a considerable emphasis on the sorts of 'normal' legislative and governmental activity that would accompany resolution of any political problem. Thus, if cyberterrorism has become increasingly perceived as a threat, it is not – our findings indicate – one that is widely seen to test the limits of ordinary political life.

Conclusion

The findings in Table 4 above indicate the extent of the challenges still faced by researchers working on issues around cyberterrorism. When we asked our respondents about these challenges specifically in 2012, by far the most common response we encountered was the need for greater definitional or conceptual clarity. In 2017, this was again highlighted by a significant proportion of respondents (14.4%), albeit considerably less than five years earlier (33.7%). The most common response in 2017 was instead access to data (30.9%). This was one of a number of obstacles to research that respondents identified, with others including disciplinary boundaries (9.3%), lack of funding and resources (9.3%) and lack of collaboration with non-academic stakeholders (5.2%). Other common responses seemed to hint at the different disciplinary approaches that respondents felt hinder interdisciplinary efforts. These included: lack of cyber knowledge (6.2%), weak theoretical or conceptual analysis (4.1%), research being insufficiently practical (2.1%) and a lack of a focus on vulnerabilities (2.1%).

This article represents an attempt to document and to begin to address some of these challenges. In so doing, we have sought to show what appear to be significant developments within this research community, notably: (i) growing convergence on cyberterrorism's core characteristics; (ii) growing researcher concern with the threat posed by cyberterrorism (albeit in the absence of specific instances); and, (iii) support for a wide portfolio of counter-measures, accompanied by increasing faith in the importance of target-hardening mechanisms. We have also sought, simply, to document other findings from aspects of the survey that relate, more specifically to questions of definition, threat and response. Although our methodology means this article can only offer a comparison of these two surveys, our hope is that the findings have value as the first and only effort to capture the development of expert opinion on this topic amongst the global research community.

Acknowledgements

We would like to thank all of the respondents for taking the time to complete the survey. Thanks also to Kimberly Corderoy and Conor Burns for excellent research assistance, and the anonymous reviewer for valuable feedback.

---

[1] BBC News Online, "Christchurch shootings: How the attacks unfolded", 18 March 2019, online via https://www.bbc.co.uk/news/world-asia-47582183 (last accessed 26 April 2019).

[2] David Mair. "#Westgate: a case study: how al-Shabaab used Twitter during an ongoing attack", *Studies in Conflict and Terrorism* 40(1) (2017), pp.24-43.

[3] Jason Burke, "Technology is terrorism's most effective ally. It delivers a global audience", *The Guardian*, 17 March 2019, online via https://www.theguardian.com/commentisfree/2019/mar/17/technology-is-terrorisms-most-effective-ally-it-delivers-a-global-audience (last accessed 26 April 2019).

[4] BBC News Online, 'UK cyber-security efforts criticised by audit office', 15 March 2019, online via https://www.bbc.co.uk/news/technology-47574943 (last accessed 26 April 2019).

[5] Lee Jarvis and Stuart Macdonald, "What is Cyberterrorism? Findings from a Survey of Researchers", *Terrorism and Political Violence* 37(1), pp.68-90.

[6] Lee Jarvis and Stuart Macdonald, "Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon", *Perspectives on Terrorism* 8(2) (2014), pp.52-65.

[7] Lee Jarvis, Stuart Macdonald and Lella Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers", *Studies in Conflict & Terrorism* 37(1) (2015), pp.68-90.

[8] Lee Jarvis, Stuart Macdonald and Lella Nouri "State Cyberterrorism? A Contradiction in Terms?", *Journal of Terrorism Research* 6(3) (2015), pp.62-75.

[9] Matthew Field – Telegraph – 'Wannacry cyber attack cost the NHS £92m as 19,000 appointments cancelled'

[10] For an overview of this research paradigm, see Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds.) *Cyberterrorism: Understanding, Assessment and Response* (2014), London: Springer.

[11] James D. Boys, "The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)", Intelligence and National Security, 33(5) (2018), pp.755-770; Marco Marsili, "The War on Cyberterrorism", *Democracy and Security* (2018), DOI: 10.1080/17419166.2018.1496826.

[12] Fidele Vlavo, “Framing digital activism: The spectre of cyberterrorism”, *First Monday* 20(10) (2015), n.p.

[13] Michael L. Gross, Daphna Canetti and Dana R. Vashdi, “Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes”, *Journal of Cybersecurity*, 3(1) (2017), pp.49–58, p.50.

[14] Jian Hua, Yan Chen, and Xin Robert Luo, “Are we ready for cyberterrorist attacks? Examining the role of individual resilience”, *Information & Management* 55(7) (2018), pp.928-938, p.928.

[15] David Bieda and Leila Halawi. "Cyberspace: A venue for terrorism." *Issues in Information Systems* 16(3) (2015), pp.33-42, p.34.

[16] E.g. Namosha Vererasamy and Marthie M. Grobler, “Logic Tester for the Classification of Cyberterrorism Attacks”, *International Journal of Cyber Warfare and Terrorism*, 5(1) (2015), pp.30-46.

[17] Gary C. Kessler, “Lone-Operator Cyberterrorism”, *Journal of Information Warfare* 15(1) (2016), pp.15-28.

[18] Thomas J. Holt, Mattisen Stonhouse, Joshua Freilich & Steven M. Chermak, “Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups”, *Terrorism and Political Violence*, (2019) DOI: 10.1080/09546553.2018.1551213.

[19] E.g. Fidele Vlavo, “Framing digital activism: The spectre of cyberterrorism”, *First Monday* 20(10) (2015), n.p.

[20] Gareth Mott, “Terror from behind the keyboard: conceptualising faceless detractors and guarantors of security in cyberspace”, *Critical Studies on Terrorism* 9(1) (2016), pp.33-53; James D. Boys, “The Clinton administration’s development and implementation of cybersecurity strategy (1993–2001)”, Intelligence and National Security, 33(5) (2018), pp.755-770.

[21] See, amongst others: Conway, Maura. “Reality bytes: Cyberterrorism and terrorist 'use' of the Internet”, *First Monday*, 7(11) (2002), n.p.; Stohl, Michael. “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) (2006): 223-238; Cavelty, Myriam Dunn. “Cyber-terror – looming threat or phantom menace? The framing of the US cyber-threat debate”, *Journal of Information Technology & Politics* 4(1) (2008), pp.19-36.

[22] Andrew Futter, “‘Cyber’ semantics: why we should retire the latest buzzword in security studies”, *Journal of Cyber Policy* 3(2) (2018), pp.201-216.

[23] E.g. Barney Warf & Emily Fekete, “Relational geographies of cyberterrorism and cyberwar”, *Space and Polity*, 20(2) (2016), pp.143-157.

[24] John J. Klein, "Deterring and Dissuading Cyberterrorism." Journal of Strategic Security 8(4) (2015):, pp.23-38, p.25.

[25] Michael L. Gross, Daphna Canetti and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes", *Journal of Cybersecurity*, 3(1) (2017), pp.49–58.

[26] Eitan Azani & Nadine Liv, "A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks", *Studies in Conflict & Terrorism* (2018), DOI: 10.1080/1057610X.2018.1494874, p3.

[27] Jian Hua, Yan Chen, and Xin Robert Luo, "Are we ready for cyberterrorist attacks? Examining the role of individual resilience", *Information & Management* 55(7) (2018), pp.928-938, p.928.

[28] James D. Boys, "The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)", Intelligence and National Security, 33(5) (2018), pp.755-770.

[29] Miguel Alberto Gomez and Eula Bianca Villar, "Fear, uncertainty, and dread: Cognitive heuristics and cyber threats", *Politics and Governance* 6(2) (2018), pp.61-72.

[30] David Bieda and Leila Halawi. "Cyberspace: A venue for terrorism." Issues in Information Systems 16(3) (2015), pp.33-42, p.37; Bernd W. Wirtz & Jan C. Weyerer, "Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats", *International Journal of Public Administration*, 40:13 (2017), pp.1085-1100; Jian Hua, Yan Chen, and Xin Robert Luo, "Are we ready for cyberterrorist attacks? Examining the role of individual resilience", Information & Management 55(7) (2018), pp.928-938; Stefano Armenia & Georgios Tsaples, "Individual Behavior as a Defense in the "War on Cyberterror": A System Dynamics Approach", *Studies in Conflict & Terrorism*, 41(2) (2018), pp.109-132.

[31] Miron Lakomy, "Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace", *Perspectives on Terrorism* 11(3) (2017), pp.40-53; Kyung-shick Choi, Claire Seungeun Lee and Robert Cadigan, "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS", *International Journal of Cybersecurity Intelligence & Cybercrime* 1(1) (2018), pp.21-49.

[32] Eitan Azani & Nadine Liv, "A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks", Studies in Conflict & Terrorism (2018), DOI: 10.1080/1057610X.2018.1494874; Marco Marsili, "The War on Cyberterrorism", *Democracy and Security* (2018), DOI: 10.1080/17419166.2018.1496826.

[33] Tim Stevens, "Cyberweapons: power and the governance of the invisible", *International Politics*, 55(3-4), (2018), pp.482-502.

[34] Jian Hua, Yan Chen, and Xin Robert Luo, "Are we ready for cyberterrorist attacks? Examining the role of individual resilience", Information & Management 55(7) (2018), pp.928-938; Stefano Armenia & Georgios Tsaples, "Individual Behavior as a Defense in the "War on Cyberterror": A System Dynamics Approach", *Studies in Conflict & Terrorism*, 41(2) (2018), pp.109-132.

[35] Andrew Futter, "'Cyber' semantics: why we should retire the latest buzzword in security studies", *Journal of Cyber Policy* 3(2) (2018), pp.201-216.

[36] John J. Klein, "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security* 8(4) (2015):, pp.23-38; also Andrew Futter, "'Cyber' semantics: why we should retire the latest buzzword in security studies", *Journal of Cyber Policy* 3(2) (2018), pp.201-216.

[37] The complete list of 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.

[38] Nine respondents stated that they felt the question was unclear or lacked sufficient explanation.

[39] Sarah Gordon and Richard Ford, "Cyberterrorism?," *Computers & Security* 21(7) (2002), pp.636–647.

[40] Alex P. Schmid, "The Definition of Terrorism", in Alex P. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. Abingdon: Routledge (2011), pp. 39-98, p.85.

[41] Lee Jarvis and Stuart Macdonald, "What is Cyberterrorism? Findings from a Survey of Researchers", *Terrorism and Political Violence* 37(1) (2015), pp.68-90, p.658-661.

[42] Alex P. Schmid, "The Definition of Terrorism", in Alex P. Schmid (ed.) *The Routledge Handbook of Terrorism Research*. Abingdon: Routledge, (2011) pp. 39-98, p.42.

[43] Lee Jarvis "The Spaces and Faces of Critical Terrorism Studies", *Security Dialogue* 40(1) (2009), pp.5-27.

[44] The failure to reach statistical significance here may reflect, in part, a growing tendency among participants to give somewhat ambiguous responses to this difficult question. This is partly owing to the fact that we employed an open-ended question which the authors subsequently coded and categorized. In 2012, responses were categorized as follows: yes; no; possibly/potentially; unsure; and other. In 2017, respondents' thinking could not be so neatly

categorized. For instance, whilst 78 respondents were categorized as "yes", a further 9 responses (7.7%) were coded as "a threat, but not a significant one". Similarly, whilst 14 respondents (12.0%) and 7 (6.0) were interpreted as a straightforward "no" or "possibly" respectively, another new category emerged: "not yet, but could in the future" (6 respondents, 5.1%). Because the categories which merged in the 2012 and 2017 data are not identical, a direct comparison of variance could not be empirically performed. When analyzing variance using the Chi-Square test of independence it was therefore necessary to either compare all positive responses with others (including no responses) and all negative against other responses (including yeses), which masks the above observations in the "other" category. We found similar results when conducting a 2x3 test (year of survey; yes, no, all other responses). Thus, we conclude that whilst our statistical test does not meet the threshold of significance, the increases in affirmative responses, the reduction in negative responses, and the observed emergence of caveat responses are nonetheless meaningful.

[45] The other category was retained. The three responses that fell within this category were each equivocal, in different respects. One said that it would depend on what "threat" means (R7003); one said that it would depend on what "significant" means (R7078); and, the other simply said "Depends" (R7101).

[46] Lee Jarvis, Stuart Macdonald and Lella Nouri, "State Cyberterrorism: A Contradiction in Terms?", *Journal of Terrorism Research* 6, no. 3 (2015), pp.62-75.

[47] The other nineteen incidents, each mentioned by a single respondent, were: attack on Israeli power systems; attack on UK Parliament's email system; interference in Brexit referendum; attack on Georgia; oil pipeline explosion in Turkey; CENTCOM; 2017 attack on U.S. power plants; during 1999 Bosnia conflict; 1996 attack on an Internet Service Provider in Massachusetts by white supremacist; 2006 cyberattack on US Naval War College, Newport, Rhode Island; 2007 cyberattack on the Pentagon; Daesh tweeting that a bomb exploded in the White House, sending the Dow Jones spiralling; 2013 Syrian Electronic Army takeover of New York Times; Ardit Ferizi (hacker who sent personal information of U.S. service members to Daesh); SWIFT banking hack; attack on Saudi Aramco; U.S. Office of Personnel Management data breach; Sony attack; and, online threats that caused a village in Kashmir to be evacuated.

[48] Joseba Zulaika, "The terror/counterterror edge: when non-terror becomes a terrorism problem and real terror cannot be detected by counterterrorism", *Critical Studies on Terrorism* 3(2) (2010), pp.247-260, p.248.

[49] See, for instance, Myriam Dunn Cavelty, "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics* 4(1) (2008), pp.19-36; Lene Hansen and Helen Nissenbaum. "Digital disaster, cyber security,

and the Copenhagen School." *International Studies Quarterly* 53(4) (2009), pp.1155-1175; Lee Jarvis, Stuart Macdonald and Andrew Whiting, "Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage", *Global Society* 30(4) (2016), pp. 605-623.

[50] Myriam Dunn Cavelty, "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics* 4(1) (2008), pp.19-36.

[51] In 2012 this was worded as greater private sector involvement.

[52] In 2012 this was worded as preventing radicalisation.

[53] Countermeasures that were mentioned by two respondents were: offensive cyber capabilities for deterrence; risk management; imposition of penalties; collaborating with hackers; reducing our dependence on cyber; counter-narratives; better information-sharing; and, air-walling.

[54] New national and international laws, norms and regulations (11% in 2012; 14.0% in 2017); not exaggerating or distorting the threat (13% in 2012; 9.7% in 2017); defining cyberterrorism (12% in 2012; 7.5% in 2017); coordination and collaboration across different jurisdictions and stakeholders (13% in 2012; 7.5% in 2017); conducting threat assessments (16% in 2012; 6.5% in 2017).