The Centre for the Study of Terrorism and Political Violence
Journal of Terrorism Research

State Cyberterrorism: A Contradiction in Terms?

by Lee Jarvis, Stuart Macdonald and Lella Nouri

This article explores findings from a global survey of the terrorism research community to explore whether states may be deemed capable of conducting cyberterrorism. The article begins with a brief review of recent literature on state terrorism, identifying empirical and analytical justifications for greater engagement with this concept. Following a discussion of our research methodology we then make two arguments. First, that there exists considerable 'expert' support for the validity of the proposition that states can indeed engage in cyberterrorism. Second, that whether states are deemed capable of cyberterrorism has implications for subsidiary debates, including around the threat that cyberterrorism poses.

Keywords: State terrorism, Cyberterrorism; Terrorism; Internet; Threat; Security; Survey

Introduction

Violence conducted in cyberspace presents important challenges for academic disciplines such as International Relations and Law which traditionally work with a state-centric ontology. Two of the most obvious of these challenges are the reduced significance of national boundaries within cyberspace – which encourages a rethinking of the importance of territorial entities – and the anonymity this offers would-be belligerents, which requires new forms of knowledge about security threats. This article contributes to contemporary debate on a particular category of violence in cyberspace – 'cyberterrorism' – asking about the significance of actor and non-actor based definitions of this phenomenon. In so doing, it aims to connect these debates to the recent upsurge of interest in the concept of 'state terrorism' in order to ask whether or not states may be deemed capable of committing cyberterrorism, and what might be gained (and indeed lost) in such judgements.

In order to do this, the article introduces original empirical data drawn from a survey of the global research community on cyberterrorism. The survey was designed to chart areas of disagreement, consensus and ambiguity in relation to this term, and received responses from 118 researchers working across 24 different countries. In this article we report on findings relating specifically to the question of whether or not states can engage in cyberterrorism. These are then connected to researcher views on the threat posed by cyberterrorism, and accounts of whether or not cyberterrorism has ever taken place that were given within the same survey.

Our engagement with this research question is driven by two dynamics. The first is the continuing contestability of the term 'cyberterrorism' within academic, legal and other debate (Jarvis and Macdonald 2014). Establishing – or enquiring into – *who* can commit cyberterrorism here offers potential for taking stock of the state of current opinion on an important generative characteristic of this term. The second driver is the rise of recent scholarly research on the nature of 'state terrorism' more broadly. Exploring whether researchers believe states can commit *cyber*terrorism might, we suggest, tell us something important about the distinctiveness of this phenomenon.

The article begins with a review of relevant academic literature on state terrorism. Here, we identify two arguments for taking the notion of state terrorism more seriously than is sometimes the case. First, is a relatively straightforward empirical argument which justifies increased attention to state terrorism due to the higher human costs that result from state based violences. Second, is an analytical argument which insists that greater attention should be paid to state violence in order to achieve greater consistency in the application of existing definitions of terrorism. These arguments, this article suggests constitute a powerful attempt to broaden the agenda of terrorism studies. The article's second section then details our research methodology, reflecting on the sampling strategy, distribution of respondents and formulation of our questions. A third section introduces qualitative and quantitative data from answers to the three questions on which we here focus. The article concludes by pointing to the importance of these findings for the state terrorism debate, and more specifically for a (re)thinking of the rationale behind the state/non-state actor divide in terrorism studies.

State Terrorism: Issues and Debates

Recent years have witnessed a fairly dramatic growth of interest in the concept of state terrorism. This has been driven, in part, by a series of explicit and powerful critiques of the historical disengagement with the state within terrorism studies; a field of research which, for many, has too long prioritised the violences of non-state actors (see, for example, Blakeley 2007; Jackson et al 2010). These arguments have drawn stimulation from two contemporary developments in particular. The first is the recent 'critical turn' in terrorism studies (see, for example, Gunning 2007; Jackson 2007; Egerton 2009; Jackson et al 2009; Jackson et al 2011) and its attempt to deconstruct this field's established theoretical and methodological assumptions. The second is a concerted hostility toward contemporary counter-terrorism practices associated with the post-9/11 'war on terrorism' and its violent excesses. Although this momentum within state terrorism research is, therefore, comparatively recent, such work builds on a small number of important earlier attempts to re-centre the study of terrorism around the violences of states (see, for example, George 1991; Claridge 1996; Chomsky 2001; Chomsky 2002). For new and old alike there are at least two powerful reasons for so doing.

The first, and perhaps most common, justification is a simple empirical calculation of the human costs of state and non-state violence. State or 'wholesale' terrorism, in this line of argument, has brought far greater harm to humanity than have the activities of non-state groups; a trend widely acknowledged, if not necessarily prioritised, within scholarship on terrorism (for comparison, see Blakeley 2008; Horgan and Boyle 2008). As Michael Stohl notes, "the number of victims produced by state terror is on a scale exponentially larger than that of insurgent terrorists" (Stohl 2008: 6). Goodin, similarly, in a discussion of 'revolutionary terrorism', argues that, "…state terrorism is an enormously important subject; it is incontestable, for example that state terrorism has claimed many more victims than has terrorism as I define it here" (Goodin 2006: 2027). What is important to note, however, is that – for these authors – the liberal democracies of the 'global North' have been as culpable as the totalitarian regimes of the twentieth-century to which we might instinctively turn upon hearing the phrase 'state terrorism' (see, for example, Blakeley 2007; Blakeley 2009; Primoratz 2004; Gareau 2004). In short, there is, for some, a tremendous disconnect between research priorities and empirical realities within scholarship on terrorism.

A second set of arguments for taking state terrorism more seriously are more strictly analytical. In the first instance, there are arguments for greater consistency in the *application* of existing definitions of terrorism

(see, for example, Chomsky 1991; Jaggar 2005; Blakeley 2007). Such definitions, approached from this perspective, are, in essence, adequate for the capture of a multitude of violences. It is their usage in practice – by policymakers and 'terrorologists' alike – that limits discussion of state violences within the language of terrorism. Here there is much to be gained – in analytical as well as political terms – for refusing the temptation toward definitional flexibility (for contrasting perspectives see Richardson 2006; Crenshaw and Robinson 2010). In Chomsky's description of what he terms the 'literal' approach to the study of terrorism, for example, "…we begin by determining what constitutes terrorism. We then seek instances of the phenomenon – concentrating on the major examples, if we are serious – and try to determine causes and remedies" (Chomsky 1991: 12; see also Chomsky 2001).This argument for greater consistency is pertinent to many, perhaps most, understandings of terrorist violence. A strategy favoured by many working in this area, indeed, is to juxtapose official US definitions of the term with its historical engagements in Nicaragua, Chile, Cuba and beyond. The argument's value is more limited, however, where actor-specific clauses are built into particular definitions of terrorism such as that employed by the US State Department in which terrorism is approached as, "…premeditated, politically motivated violence perpetuated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience" (cited in Whittaker 2003: 3; see also Stohl 2006). In response to actor-specific understandings of terrorism such as these, an alternative argument is often made on behaviouralist grounds: one that suggests that terrorism is a form of violence which is separable from its practitioner. Hence, for Jackson et al, for example:

> *To suggest when state agents engage in the very same strategies as non-state terrorists, such as when they blow up civilian airliners (the Lockerbie bombing) or a protest ship (the Rainbow Warrior bombing) or plant a series of bombs in public places (the Lavon affair), it ceases to be terrorism is effectively the abandonment of scholarly research principles* (Jackson et al 2010: 3).

For Teichman, similarly:

> *….we have to acknowledge that governments often do things, both to their own people, and against enemies in peace and war, which share the features of the worst types of revolutionary terrorism. State terrorism is characterized by such actions as the kidnapping and assassination of political opponents of the government by the police or the secret service or the army; imprisonment without trial; torture; massacres of racial or religious minorities or of certain social classes; incarceration of citizens in concentration camps; and generally speaking government by fear* (Teichman 1989: 509).

If we take them together, these arguments constitute a powerful (if still nascent) attempt to broaden the agenda of terrorism studies (Jarvis 2009). Minimally, the aim is to extend the study of terrorism beyond its traditional, narrow, parameters in order to facilitate the analysis of certain state violences under this rubric (for example Gunning 2007). Maximally, where articulated most ambitiously, the ultimate aim is the advancement of emancipatory political projects predicated on a refusal to remain silent in the face of any (terrorist) violences, whoever their authors (see Blakeley 2008; McDonald 2009; Toros and Gunning 2009). Thus, for Jackson *et al,* for example:

> *…there are important ethical-normative reasons for retaining the term 'state terrorism'. For example, due to the powerful connotations of the 'terrorism' label, its retention as a descriptor of certain forms of state violence could be an important means of advancing a progressive political project aimed at protecting marginalized and vulnerable populations from indiscriminate and oppressive forms of state violence, whether they occur under the rubric of war or counter-terrorism* (Jackson et al 2010: 5).

With the ground thus prepared for greater engagement with state terrorism, the research agenda of this literature to date has focused on attempting to define and typologise this form of violence (Jarvis and Lister 2014). Engagements with definitional issues often lead to reflection on the core characteristics of state terrorism, with the following themes particularly dominant therein: the involvement of state representatives in the commission or practice of violence; instrumental or purposive behaviour where acts of violence and their victims function as means to future ends; an identifiably communicative or symbolic function; and, the experience of terror in a broader population (compare Blakeley 2010 and Raphael 2010). Such reflection leads some to define state terrorism as a distinctive form of violence, for example:

> *…the intentional use or threat of violence by state agents or their proxies against individuals or groups who are victimised for the purpose of intimidating or frightening a broader audience* (Jackson et al 2010: 3).

Or:

> *Terrorism by states is characterized by official support for policies of violence, repression, and intimidation. This violence and coercion is directed against perceived enemies that the state has determined threaten its interests or security. Although the perpetrators of state terrorist campaigns are frequently government personnel, and directives do originate from government officials, those who carry out the violence are also quite often unofficial agents of the government* (Martin, cited in Jackson et al 2011: 178).

Others prefer instead to define 'terrorism' more inclusively before applying this understanding to the actions of states as appropriate. The following, for instance, is the definition employed in Gareau's account of US involvement in state terrorism:

> *Terrorism consists of deliberate acts of a physical and/or psychological nature perpetrated on select groups of victims. Its intent is to mould the thinking and behaviour not only of those targeted groups, but more importantly, of larger sections of society that identify or share the views and aspirations of the targeted groups or who might easily be led to do so. The intent is to intimidate or coerce both groups by causing them intense fear, anxiety, apprehension, panic, dread, and/or horror* (Gareau 2004: 14).

Typologies of state terrorism seek to differentiate the various forms that this phenomenon can take. Michael Stohl, for example, distinguishes between overt engagements in coercive diplomacy; covert participation in assassinations, coups, and the like; and, surrogate activities, whereby assistance is offered to a secondary state or insurgent organisation engaging in terrorist violence (Stohl 1984). Blakeley, more recently, separates state perpetration and state sponsorship of terrorism (Blakeley 2009). She also, moreover, distinguishes "limited state terrorism" which is targeted at a specific, narrow audience, from "generalised" state terrorism, which works to target entire populations (Blakeley 2009: 44). Although (as we might expect) no single, universally accepted typology of state terrorism exists (Primoratz 2002), these discussions do remind us that the terrorism of states can take myriad forms, and use myriad techniques and technologies. With this in mind, we proceed now to our discussion of whether states can commit cyberterrorism and what responses to this may mean for the literature discussed in this section. First, however this article outlines the methodology used to collect the empirical data on 'expert' opinion on cyberterrorism.

Methodology

Our attempt to contribute to these ongoing discussions around the phenomenon of state terrorism draws from a recent empirical research project on cyberterrorism. This research made use of an 'expert survey', which was distributed to over six hundred members of the global research community between June and November 2012. Respondents to the survey were identified using a purposive – hence non-probabilistic – sampling strategy with four primary strands. The first of these was a targeted literature review search to identify researchers who have published on cyberterrorism within peer-reviewed journals, monographs, edited books, or other literature. This was completed using the main catalogue of the British Library, as well as 47 other online databases[1]. Our search was limited to outputs that had been published on or after 1 January 2004.

The second strand was to target active researchers within the terrorism research community more widely. Whilst these individuals may not have published on cyberterrorism specifically, their knowledge of the major debates around terrorism meant they would be well-positioned to contribute to this research. Thus, individuals that had published in any of the following four journals since January 1st 2009 were added to the sample: *Studies in Conflict and Terrorism*, *Terrorism and Political Violence, Critical Studies on Terrorism*, and, *Perspectives on Terrorism*. Members of the editorial boards of these journals (as of August 1st 2012) were also added, given their similarly prominent standing within terrorism research.

The third strategy was a 'snowball method' in which we contacted potential respondents who were explicitly identified to us by individuals who had already completed the survey. The fourth was via two mailing lists maintained by British academic associations: the Terrorism and Political Violence Association[2], and the British International Studies Association Critical Terrorism Studies Working Group[3]. Although there was, of course, overlap in the individuals identified in our four strategies, these latter two methods engendered far fewer responses than did our initial literature review searches.

The use of a purposive, non-probabilistic, sampling strategy was, we argue, appropriate to the survey's ambitions. Whilst it involves sacrificing any strict claim to statistical representativeness, this may be defended given the nature of the population in whom we were interested: the terrorism research community. Where the boundaries of this community lie, and who may be considered a legitimate member of it, are, of course, entirely contestable. Moreover, as with any epistemic community – indeed, perhaps more than many – the field of terrorism research is, by its nature, fluid and porous. Individuals enter and leave according to their evolving research interests, and any effort to capture opinion therein can offer only a brief and temporary snapshot of a dynamic enterprise. In this sense, the sacrifice of strict representativeness in our study of researchers is justified given that no discernible, definitive, population could reasonably be said objectively to exist.

A total of 118 responses from researchers working in 24 countries across six continents were generated by our survey. Of the 117 responses that provided geographical information to us, our sample had a majority of respondents working in the United States of America and the United Kingdom: 41 (35% of the total) and 32 (27%) respectively. The next largest sites were Australia (7 respondents, 6%) and Canada (4 respondents, 3%). This weighting toward anglophonic countries is unfortunate, but unsurprising, given the traditional anglocentricism of terrorism research (Stump and Dixit 2013). In terms of professional status, the distribution of our respondents was skewed toward permanent and temporary academic staff as follows: Academic Staff (Permanent): 75 (64%); Academic Staff (Temporary): 16 (14%); Research Student: 9 (8%); Independent Researcher: 11 (9%); Retired: 2 (2%); and, None of the Above: 5(4%). In terms of disciplinary

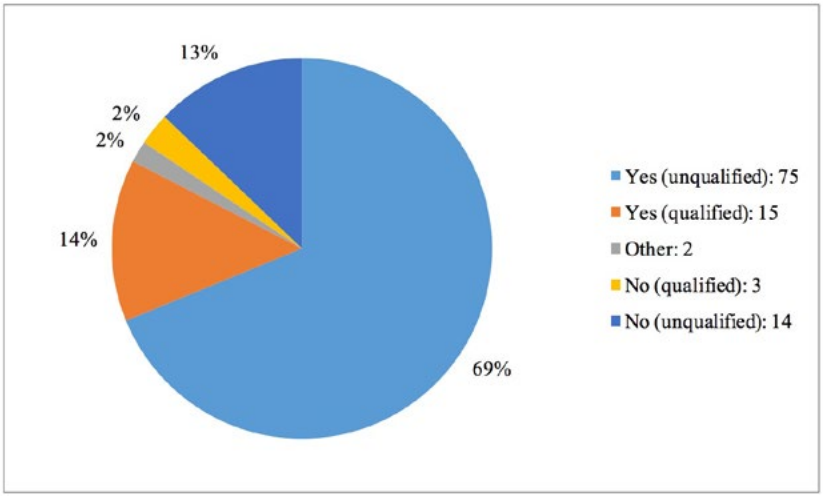
background, finally, our sample described themselves in the following way, with several researchers self-identifying with more than one academic discipline: Political Science/International Relations: 69 (50%); Psychology/Anthropology: 20 (15%); Engineering/Computer Science/Cyber 17(12%); Law/Criminology: 15 (11%); Literature/Arts/History: 9 (7%); Independent Researchers/Analysts: 5 (4%); and, Economics/Business: 2 (1%).

Our survey employed a combination of open-ended and closed questions designed to generate quantitative and qualitative data. Twenty questions were included in total. These focused on the following: demographic information; definitional issues around terrorism and cyberterrorism; the cyberterrorism threat; countering cyberterrorism; and, views of current research on this phenomenon, including the major challenges facing contemporary scholars. To encourage as high a completion rate as possible, the questionnaire was made available in two formats: an online survey and a word processing document. In the following section, this article turns to the findings of the survey in relation to the concept of state cyberterrorism and the impact this has on responses to questions on the significance and existence of the cyberterrorism threat.

Findings and Analysis

The first question of relevance from our survey – numbered Question 13 – asked respondents, 'In your view, can states engage in cyberterrorism?' A free text box was provided for responses, in order to allow respondents to develop and explain their answers. In total, the question was answered by 109 respondents (response rate: 92%). Answers were subsequently analysed and coded using the following five categories: yes (unqualified); yes (qualified); other; no (qualified); and, no (unqualified). As chart 1 demonstrates, a total of 83% of respondents agreed that states can potentially engage in cyberterrorism. Moreover, the vast majority of these respondents offered unqualified agreement.

Chart 1: Can states engage in cyberterrorism?



When explaining their view that states can engage in cyberterrorism, several respondents explicitly rejected any attempt to distinguish between state and non-state actors. One respondent, for example, argued that: 'Any social actor with sufficient knowledge, means and intent can utilise any particular tactic, be it cyberterrorism or anything else, be they states or any other social entity'[4]. Another, drawing on similarly behaviouralist reasoning, stated: 'By definition all forms of terrorism are a tactic open to all and therefore no individual or entity is exempt from the option of using this tactic'[5]. Others still drew analogy with alternative forms

of terrorism, arguing that since states can engage in offline terrorism there is no reason why states cannot also engage in cyberterrorism[6]. In fact, one respondent went so far as to suggest that, without state involvement, the technological complexities render cyberterrorism impossible[7]. By contrast, there were other respondents who – whilst agreeing that states can engage in cyberterrorism – described states' potential involvement in more limited terms. In their opinion, a cyber-attack would only constitute cyberterrorism if state actors played no more than a supporting or facilitative role. For example, one respondent answered: 'Only as state sponsors of terrorist groups'[8], whilst others referred to the role of the state as a place to 'harbour'[9] or 'support'[10] non-state actors who launch cyberterrorist attacks.

There were other respondents who answered affirmatively to this survey question, yet qualified their answer by querying whether cyberterrorism is the most appropriate label for cyber-attacks perpetrated by state actors. Like some of the respondents mentioned in the previous paragraph, some of these individuals drew an analogy with traditional forms of terrorism. But unlike those mentioned above, these respondents asserted that offline terrorists are conventionally regarded as non-state actors. Hence one respondent answered: 'Yes [states can engage in cyberterrorism], although the standard definition of terrorism rules out state action (so Hiroshima isn't formally an act of terrorism)'[11]. Similarly, another answered: 'Yes, just like states can engage in terrorism, however the standard definition of terrorism does focus on non-state armed groups only, leaving terrorist behaviour of states out of the equation'[12]. This respondent went on to suggest that state cyberterrorism should instead be labelled as a crime against humanity. Others also suggested alternative labels. One commented: 'In effect [states can engage in cyberterrorism], even if it should be more carefully labelled as espionage/sabotage'[13], whilst another observed that: 'States can engage in the act of terrorism, including cyberterrorism (though we still call them states, not terrorists)'[14].

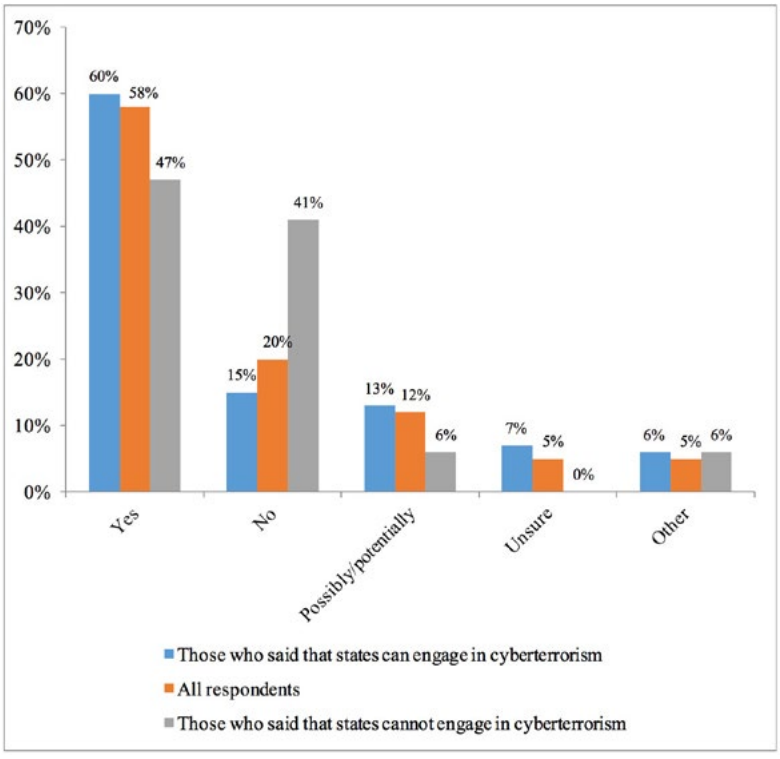
A further significant finding from our survey is that a number of respondents drew on empirical reasoning similar to that discussed in the above literature review to argue that there exists a greater threat of state cyberterrorism than non-state cyberterrorism. One went so far as to suggest that: '[state cyberterrorists] are the greatest threat, and make non-government sources of this threat nearly inconsequential in comparison'[15]. The most common reason respondents offered for this view was that states have access to far greater resources and capabilities than non-state actors[16]. Others pointed out that cyberterrorism is likely to prove attractive to states because of the difficulties of attribution and concomitant potential for anonymity. As one respondent remarked, states engage in cyberterrorism 'because of the ease with which a state operator can mask itself online'[17]. In fact, several respondents claimed that states already engage in cyberterrorism[18], with a number of examples being offered in support of this assertion. The most commonly cited of these was Stuxnet[19] with other suggested examples including the cyber-attacks on Estonia[20] and Georgia,[21] attempted attacks on the US by China and North Korea[22] and 'acts perpetrated by Russia and China'[23].

As chart 1 showed, there were a total of 17 respondents (15%) who said that states cannot engage in cyberterrorism. In the opinion of a number of these respondents, the concept of state cyberterrorism is simply a misnomer. Different reasons were offered in support of this view. The most common reason was that terrorism is, by its very nature, a non-state activity[24]. If the perpetrator is a state actor, then the conduct is cyberwarfare[25] or cyber espionage[26], not cyberterrorism. Second, one respondent suggested that cyber-attacks orchestrated by state actors may not be terroristic in nature. Using Stuxnet as an example, this respondent argued that it 'was not used in a way that appears intended to create terror. These acts are probably best thought of as politically or strategically motivated sabotage'[27]. Lastly, one respondent argued that it is mistaken to talk of state cyberterrorism because cyberterrorism itself is a misnomer, despite the

fact that, 'Cyberattacks and espionage which originate from states certainly do exist'[28]. Meanwhile, there were other respondents that were willing to accept the concept of state cyberterrorism in principle, but who nonetheless answered no to the survey question on the basis that it is preferable to use a different label[29]. As one explained, 'actions by states are best viewed in terms of warfare/coercive foreign policy. Reserving the term [cyberterrorism] for non-state actors (even if sponsored by states) affords a certain degree of analytical clarity'[30].

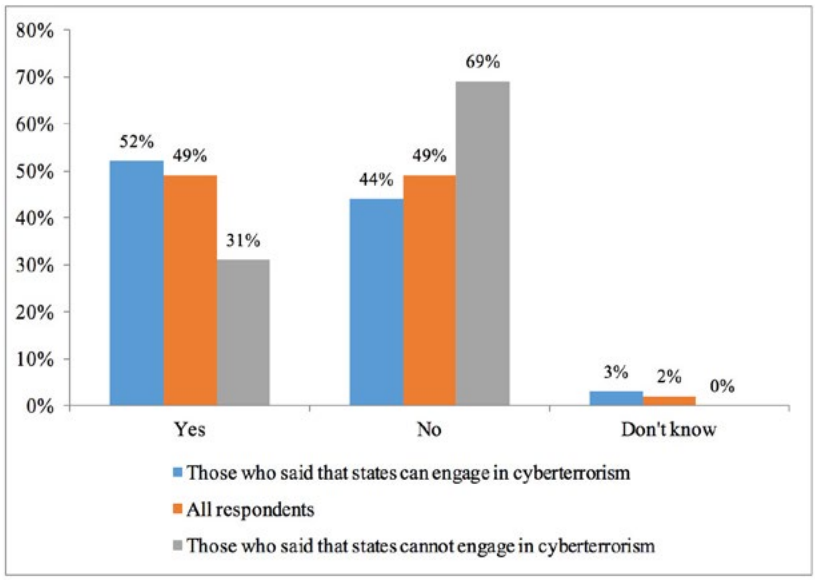
Finally, it is important to note that respondents' views on the state cyberterrorism question had a discernible impact on their answers to other important questions, particularly surrounding the significance of the cyberterrorist threat. Chart 2 shows the answers to question 10 of our survey – 'In your view, does cyberterrorism constitute a significant threat?' – for three groups: all respondents; those respondents for whom states can engage in cyberterrorism; and, those respondents who argued that states cannot engage in cyberterrorism. 60% of researchers who said that states can engage in cyberterrorism also believed that cyberterrorism poses a significant threat. This figure was considerably lower for those who said that states cannot engage in cyberterrorism, at 47%. Similarly, only 15% of those who said that states can engage in cyberterrorism opined that cyberterrorism is not a significant threat, compared to 41% of those who said that states cannot engage in cyberterrorism.

Chart 2: Does cyberterrorism pose a significant threat?



A similar pattern is evident in chart 3, which shows the answers of the same three groups of respondents to question 11 of our survey: 'do you consider that a cyberterrorism attack has ever taken place?'. 69% of those who said that states cannot engage in cyberterrorism believed that no cyberterrorist attack has ever occurred – compared to 44% of those who said that states can engage in cyberterrorism.

Chart 3: Do you consider that a cyberterrorist attack has ever taken place?



So, just as an individual's view on whether cyberterrorism should be conceived in narrow terms (as a terrorist attack which has computers as its means and/or target) or broad terms (as any form of online terrorist activity) affects that individual's assessment of the cyberterrorism threat (Jarvis et al 2014), so too does an individual's view of whether states can engage in cyberterrorism.

Concluding Remarks

Our survey revealed general agreement that states have perpetrated cyberattacks, with respondents offering a number of examples including Stuxnet and the attacks on Estonia and Georgia. This article has raised the question of how we should conceive of these attacks. Should they be understood as instances of cyberterrorism perpetrated by state actors? Or should we employ a different label, and reserve the term cyberterrorism for non-state actors? Answering these questions requires consideration of two issues. First, is it possible to speak of state cyberterrorism, or is the term oxymoronic? And, second, if it is possible to speak of state cyberterrorism, should we do so?

As explained previously, perhaps the most common justification for employing the term state terrorism in discussions of offline violences is the empirical claim that historically states have inflicted more harm than non-state actors. The same appears to hold true in the cyber realm, in that a number of our respondents pointed out that most or all of the large-scale cyberattacks to date have been perpetrated by state actors. In fact, it has been argued that from a cost-benefit perspective it is unlikely that non-state terrorists will attempt to launch Stuxnet-like cyberattacks at any point in the foreseeable future (Conway 2014; Al-Garni and Chen 2015). But whilst the majority of our respondents suggested that states can commit acts of cyberterrorism, there were also dissenting voices. In fact, even some of those that said that states can commit acts of cyberterrorism qualified their answers by suggesting that another label might be more apt.

The second set of arguments that we outlined previously for engaging with the concept of state terrorism were analytical in nature. Our findings suggest that, as noted above, the argument that existing definitions of terrorism should be applied with greater consistency is of limited utility. The argument presupposes that definitions of terrorism are not actor-specific. But whilst a number of our respondents explicitly rejected any attempt to distinguish between state and non-state actors, there were others who insisted on the importance of this distinction, claiming that terrorism is by definition a non-state activity. For the same reason, the alternative argument – that terrorism is a form of violence which has nothing to do with its practitioner – is, for these respondents at least, equally problematic.

In summary, the diversity of opinions offered by our respondents demonstrates that there is nothing inherent in the concept of terrorism that requires a particular answer to the question of whether states can commit terrorist acts. The choice of definition, and of typology, is a political one. Our findings do suggest, however, that the dominant view within the research community at present is that states can commit acts of cyberterrorism. The cyber realm thus presents a challenge to the traditional view that emphasises the distinction between state and non-state actors and lends weight to the growing interest in the concept of state terrorism.

About the authors

Lee Jarvis *is a Reader in International Security and a member of the Critical Global Politics research group at the University of East Anglia. His work has been published in journals including Millennium: Journal of International Studies, Security Dialogue and Political Studies, and recent books include Security: A Critical Introduction (with Jack Holland, Palgrave: 2015) and Anti-Terrorism, Citizenship and Security (with Michael Lister, Manchester University Press, 2015).*

Stuart Macdonald *is Associate Professor in Law and Deputy Director of the Centre for Criminal Justice and Criminology at Swansea University. He is co-editor of Cyberterrorism: Understanding, Assessment and Response (New York: Springer, 2014) (with Lee Jarvis and Thomas Chen) and Terrorism Online: Politics, Law and Technology (Abingdon: Routledge, 2015) (with Lee Jarvis and Thomas Chen). His research has been published in journals including Cornell Journal of Law and Public Policy, Studies in Conflict and Terrorism, Terrorism and Political Violence, Criminal Law and Philosophy and Sydney Law Review. He has held visiting scholarships at Columbia University Law School, New York, the Institute of Criminology at the University of Sydney and the Faculté de Droit at the Université de Grenoble.*

Lella Nouri *lectures in the Department of Criminology at Swansea University. She is currently completing her PhD which investigates the construction of cyberterrorism as an issue of national security within US political discourse. Since undertaking her doctorate she has had work published on a range of topics that reflect her research interests including: terrorism, cyberterrorism and online radicalisation.*

Notes

[1] The complete list is as follows: ACM Digital Library; Anthropoligical Index Online; Applied Social Sciences Index and Abstracts; Bibliography of British & Irish History; BioMed Central Journals; British Humanities Index (CSA); British Periodicals (XML); Business Source Complete (EBSCO); CINAHL Plus (EBSCO); Cochrane Database of Systematic Reviews (Wiley); Education Resources Information Centre; Emerald; HeinOnline; HMIC (Ovid); IEEE Xplore; INSPEC (Ovid); International Bibliography of the

Social Sciences; IOP Journals Z39; JISC Journals Archives; JSTOR; Kluwer Law Journals; Lecture Notes in Computer Science (Springer Link); Lexis Library; MathSciNet (AMS); Medline (EBSCO); MLA International Bibliography; Oxford Journals; Periodicals Archive online; Philosopher's Index (Ovid); Project Muse; Proquest Business Collection; PsycARTICLES (Ovid); PsycINFO (Ovid); PubMed; Royal Society Journals; SAGE Journals Online; Scopus (Elsevier); Social Care Online (SCIE); Springer Link (Metapress); Taylor & Francis Online; Web of Knowledge (Cross Search); Web of Knowledge (ISI); Web of Science (Cross Search); Web of Science (ISI); Westlaw; Wiley Interscience; and, Zetoc.

[2] For further information on the association, please see: http://tapva.com/.

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

[4] R65.

[5] R8.

[6] R6, R62.

[7] R31.

[8] R49. Similarly, R90 stated: 'If states sponsor non-state groups to do cyberattacks, then that could easily be described as states (indirectly) engaging in cyberterrorism'.

[9] R59.

[10] R33.

[11] R75.

[12] R106.

[13] R99.

[14] R78.

[15] R15.

[16] R30, R45.

[17] R20. R10 also commented, 'Of course [states can engage in cyberterrorism], but they are likely to have their participation hidden'.

[8] In response to the survey question, R111 wrote 'Most terrorism, including cyberterrorism, is conducted by states', whilst R102 simply wrote 'They already do'.

[9] R16, R27, R45, R80.

[20] R51, R69.

[21] R69.

[22] R85.

[23] R37.

[24] R3, R9, R52, R55, R71, R83, R87, R108.

[25] R3, R9, R52, R71, R83.

[26] R26, R83, R87.

[27] R87.

[28] R26.

[29] R1, R63, R64, R73.

[30] R1.

References

Al-Garni, T. and Chen, T. (2015). An Updated Cost-Benefit View of Cyber Terrorism. In: Jarvis, L., Macdonald, S. & Chen, T. eds., *Terrorism Online: Politics, Law and Technology*. Abingdon: Routledge, pp.72-85.

Blakeley, R. (2007).Bringing the State Back Into Terrorism Studies. *European Political Science*. **6**(3), pp.228-235.

Blakeley, R. (2008). The Elephant in the Room: a Response to John Horgan and Michael J. Boyle. *Critical Studies on Terrorism*. **1**(2), pp.151-165.

Blakeley, R. (2009). *State Terrorism and Neoliberalism: The North in the South*. Abingdon: Routledge.

Blakeley, R. (2010). State Terrorism in the Social Sciences: Theories, Methods and Concepts. In: Jackson, R., Murphy, E. and Poynting, S. eds., *Contemporary State Terrorism: Theory and Practice*. Abingdon: Routledge, pp.12-27

Burnett, J. and Whyte, D. (2005). Embedded Expertise and the New Terrorism. *Journal for Crime, Conflict and the Media*. **1**(4), pp.1-18.

Chomsky, N. (1991). International Terrorism: Image and Reality. In: George, A. ed., *Western State Terrorism*. Cambridge: Polity Press, pp12-38.

Chomsky, N. (2001). *9-11*. New York, NY: Seven Stories Press.

Chomsky, N. (2002). *Pirates and Emperors, Old and New: International Terrorism in the Real World*. London: Pluto Press.

Claridge, D. (1996). State Terrorism? Applying a Definitional Model. *Terrorism & Political Violence*. **8**(3), pp.47-63.

Conway, M. (2014). Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In: Chen, T., Jarvis, L. and Macdonald, S. eds., *Cyberterrorism: Understanding, Assessment, and Response*. New York, NY: Springer, pp.103-121.

Crenshaw, E. and Robinson, K. (2010). Political Violence as an Object of Study: The Need for Taxonomic Clarity. In: Leicht, K. T. and Jenkins, J.C. eds., *Handbook of Politics: State and Society in Contemporary Perspective*. New York, NY: Springer, pp.235-246.

Egerton, F. (2009). A Case for a Critical Approach to Terrorism. *European Political Science*. **8**(1), pp.57-67.

Gareau, F. H. (2004). *State Terrorism and the United States: From Counterinsurgency to the War on Terrorism*. London: Zed Books.

George, A. ed. (1991). *Western State Terrorism*. Cambridge: Polity Press.

Goodin, J. (2006). A Theory of Categorical Terrorism. *Social Forces*. **84**(4), pp.2027-2046.

Gunning, J. (2007). A Case for Critical Terrorism Studies. *Government and Opposition*. **42**(3), pp.363-393.

Halkides, M. (1995). How Not to Study Terrorism. *Peace Review*. **7**(3-4), pp.253-260.

Halperin, S. and Heath, O. (2012). *Political Research: Methods and Practical Skills.* Oxford: Oxford University Press.

Herman, E. S. (2002). Wholesale Terrorism Escalates: The Threat of Genocide. *Arab Studies Quarterly.* **24**(2-3), pp.119-128.

Herman, E. and O'Sullivan, G. (1989). The 'Terrorism' Industry: The Experts and Institutions That Shape Our View of Terrorism. New York, NY: Pantheon Books.

Horgan, J. and Boyle. M. J. (2008). A Case against Critical Terrorism Studies. *Critical Studies on Terrorism*. **1**(1), pp.51-64.

Jackson, R. (2007). The Core Commitments of Critical Terrorism Studies. *European Political Science*. **6**(3), pp.244-251.

Jackson, R., Breen Smyth, M. and Gunning, J. eds. (2009). *Critical Terrorism Studies: A New Research Agenda*. Abingdon: Routledge.

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

Jackson, R., Murphy, E. & Poynting, S. (2010). Introduction: Terrorism, the State and the Study of Political Terror. In: Jackson, R., Murphy, E. and Poynting, S. eds., *Contemporary State Terrorism: Theory and Practice*. Abingdon: Routledge, pp.1-11.

Jaggar, A. M. (2005). What Is Terrorism, Why Is It Wrong, and Could It Ever Be Morally Permissible? *Journal of Social Philosophy*. **36**(2), pp.202-217.

Jarvis, L. (2009). The Spaces and Faces of Critical Terrorism Studies. *Security Dialogue*. **40**(1), pp.5-27.

Jarvis, L. and Lister, M. (2014). State Terrorism Research and Critical Terrorism Studies: an Assessment. *Critical Studies on Terrorism*. **7**(1), pp.43-61.

Jarvis, L., and Macdonald, S. (2014). What is Cyberterrorism? Findings from a Survey of Researchers. *Terrorism and Political Violence*. Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2013.847827 (last accessed 2 June 2015).

Jarvis, L., Macdonald, S. and Nouri, L. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism*. **37**(1), pp.68-90.

McDonald, M. (2009). Emancipation and Critical Terrorism Studies. In: Jackson, R., Breen Smyth, M. and Gunning, J. eds. *Critical Terrorism Studies: A New Research Agenda*. Abingdon: Routledge, pp.109-124.

Mueller, J. (2008). The Terrorism Industry: The Profits of Doom. In: Kassimeris, G. ed., *Playing Politics with Terrorism: A User's Guide*. New York, NY: Columbia University Press, pp.301-320.

Primoratz, I. (2004). What is Terrorism? In: Primoratz, I. ed. *Terrorism: The Philosophical Issues*. Basingstoke: Palgrave, pp.15-30.

Primoratz, I. (2002). State Terrorism. In: Coady, T. and O'Keefe, M.eds., *Terrorism and Justice: Moral Argument in a Threatened World*. Carlton, Victoria: Melbourne University Press, pp.31-42.

Raphael, S. (2010). Paramilitarism and State Terror in Colombia. In: Jackson, R., Murphy, E. and Poynting, S. eds., *Contemporary State Terrorism: Theory and Practice*. Abingdon: Routledge, pp.163-180.

Richardson, L. (2006). *What Terrorists Want: Understanding the Terrorist Threat*. London: John Murray.

Stohl, M. (1984). International Dimensions of State Terrorism. In: Stohl, M. and Lopez, G., A. eds., *The State as Terrorist: The Dynamics of Governmental Violence and Repression*. Westport, CT: Greenwood Press, pp.43-58.

Stohl, M. (2006). The State as Terrorist: Insights and Implications. *Democracy and Security*. **2**(1), pp.1-25.

Stohl, M. (2008). Old Myths, New Fantasies, and the Enduring Realities of Terrorism. *Critical Studies on Terrorism*. **1**(1), pp.5-16.

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

Teichman, J. (1989). How to Define Terrorism. *Philosophy*. **64**(250), pp.505-517.

Toros, H. and Gunning, J. (2009). Exploring a Critical Theory Approach to Terrorism Studies. In: Jackson, R., Breen Smyth, M. and Gunning, J. eds., *Critical Terrorism Studies: A New Research Agenda* Abingdon: Routledge, pp.87-108.

Whittaker, D. (2003). *The Terrorism Reader*. 2nd ed. Abingdon: Routledge.

Wilkinson, P. (2001). *Terrorism Versus Democracy: The Liberal State Response* . London: Frank Cass.