# What is Cyberterrorism? Concepts and Contests From the World of Research

https://www.e-ir.info/2013/03/13/what-is-cyberterrorism-concepts-and-contests-from-the-world-of-research/

LEE JARVIS STUART MACDONALD AND TOM CHEN, MAR 13 2013

The threat of cyberterrorism is referred to with ever-increasing frequency in contemporary political discourse, popular culture, academic debate and beyond. However, as with its parent concept 'terrorism', this frequency of usage is not matched by anything resembling consistency of definition. For instance, where some authors reserve the term for attacks targeted against cyber infrastructure, others are willing to invoke it in any coalescence of digital technologies and irregular conflict, including the preparation or planning of non-cyber attacks.

As an attempt to contribute to understanding of this phenomenon, Swansea University's Cyberterrorism Project has recently undertaken a 'state of the discipline' survey of the global research community.[1] The survey was completed by 118 individuals working in 24 countries across six continents, the findings of which have now been published in a research report.[2] The survey asked researchers for their view on a range of questions relating to the concept, threat, and appropriate responses to cyberterrorism. And, as suggested below, it threw up a number of our findings that might seem counter-intuitive to students and researchers familiar with academic debates on terrorist violences more widely.

A first finding of interest – and one that relates specifically to questions of definition – was that only 77% of our respondents believed 'digital means or target' to be an important element of cyberterrorism. This figure was considerably fewer than the 87% of respondents who highlighted the significance of some form of 'political or ideological motive'. This discrepancy seems to highlight the continuing importance of some criterion of intentionality within many researchers' understandings of terrorism.

If we turn, next, to the type of actor capable of committing cyberterrorism, 69% of our respondents indicated to us that states could perpetrate acts of cyberterrorism, with a further 14% offering a qualified yes to this question. However valid this view, it is some distance from the dominant academic approach to (or focus upon) terrorism as a form of non-state violence.[3] Although some of our respondents did argue that cyber-attacks originating from states should be discussed as forms of warfare or foreign policy, this perspective's relative minority implies that the cyber-prefix might be doing something important to the concept of terrorism that extends beyond simply adding another case to this category.[4] In other words, adding cyber- to terrorism may have implications for our understanding of what terrorism is, as well as for the parameters of related debates on its causes, significance, perpetrators, and so forth.

A third finding worth noting – and one that further evidences this concept's current contestability – concerned responses to a question on whether or not a cyberterrorist attack had ever taken place. In answering this, 49% of our respondents answered in the negative, and 49% in the affirmative. Those that did cite examples to evidence its past occurrence pointed, most frequently, to attacks on Estonia, Georgia and Iran. While other potential security challenges might have their causes or their status *as* security issues debated (for instance, global climate change), and others might have their *future* probability questioned (for instance, great power conflict), it is difficult to think of another security issue whose *past* occurrence is so contested by the research community.

That the existence, as well as the meaning, significance, protagonists and responses to cyberterrorism can be so contested only adds, we suggest, to the compelling nature of this security issue (if that's what cyberterrorism even is). In this sense, our aim in conducting this research was only to provide a snapshot of current academic perspectives on this phenomenon, rather than to work toward, much less provide, any definitive resolution to these questions. Attempting to do the latter by aggregating our findings would have been complicated by at least two factors. The first is that respondents to our survey demonstrated entirely incompatible meta-theoretical assumptions and perspectives in the responses they provided. Thus, where some researchers viewed cyberterrorism unequivocally as a security threat, others approached it instead as a discursive or performative production. In the second instance, resolving these conceptual and normative issues cannot be a purely quantitative task, approachable by the totting up of majority opinion: expert or otherwise. Our hope, however, is that this research can inform and stimulate further work on what will surely become an increasingly significant presence within security discourse and practice throughout forthcoming years. An increasingly significant presence, indeed, whatever one's meta-theoretical, political or normative stance.

—

**Lee Jarvis** *is a Senior Lecturer in the Department of Political and Cultural Studies at Swansea University, UK. He is author of Times of Terror: Discourse, Temporality and the War on Terror (Palgrave, 2009) and co-author (with Richard Jackson, Jeroen Gunning and Marie Breen Smyth) of Terrorism: A Critical Introduction (Palgrave, 2011). He has articles on terrorism and counter-terrorism in print or forthcoming in journals including Security Dialogue, Political Studies, International Relations, and Critical Studies on Terrorism.*

**Stuart Macdonald** *is a Senior Lecturer at Swansea University who researches criminal law and criminal justice. He has written a number of articles examining frameworks for analysing and evaluating anti-terrorism policies and legislation. These have been published in leading international journals, including the Sydney Law Review and the Cornell Journal of Law and Public Policy.*

**Thomas Chen** *is a Professor in Swansea University's College of Engineering, and an expert in computer and network security. His previous research projects have explored Internet security, intrusion detection, attack modelling, malicious software and cybercrime, with support from various US agencies and companies. He is co-editor of Broadband Mobile Multimedia: Techniques and Applications (2008) and Mathematical Foundations for Signal Processing, Communications, and Networking (2011), co-author of ATM Switching Systems (1995), and has published papers in a number of IEEE journals including IEEE Computer, IEEE Security and Privacy, IEEE Internet Computing, and IEEE Transactions on Smart Grid.*

[1] For more information on the project and its activities, please see: http://www.cyberterrorism-project.org/

[2] The report is available via free of charge, via: http://www.cyberterrorism-project.org/cyberterrorism-report/

[3] Jackson, R. *et al* (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, p.175.

[4] See Weinberg, L. *et al* (2012) 'The challenges of conceptualizing terrorism', in J. Horgan & K. Braddock (eds.) *Terrorism Studies: A Reader*. Abingdon: Routledge, p.77.