Analogy and authority in cyberterrorism discourse:

An analysis of global news media coverage

LEE JARVIS, STUART MACDONALD and ANDREW WHITING

This article explores constructions of cyberterrorism within the global news media between 2008 and 2013. It begins by arguing that the preoccupation with questions of definition, threat and response in academic literature on cyberterrorism is problematic, for two reasons. First, because it neglects the constitutivity of representations of cyberterrorism in the news media and beyond; and, second, because it prioritises policy-relevant research. To address this, the article provides a discursive analysis drawing on original empirical research into 31 news media outlets across the world. Although there is genuine heterogeneity in representations of cyberterrorism therein, we argue that constructions of this threat rely heavily on two strategies. First, appeals to authoritative or expert 'witnesses' and their institutional or epistemic credibility. And, second, generic or historical analogies, which help shape understanding of the likelihood and consequences of cyberterrorist attack. These strategies have particularly discursive importance, we argue, given the lack of readily available empirical examples of the 'reality' of cyberterrorism.

Key words: cyberterrorism; discourse; news; media; terrorism.

Introduction

The potential ramifications of a serious cyberterrorist attack enjoy periodic emergence within the global news media. A 2013 article in *The Washington Post*, for example, asked 'Is the

U.S. Prepared for Cyberterrorism?';[1] returning to themes raised by *Fox News* two years prior: '10 Years After 9/11, Are America's Cyberdefenses Weaker?'[2] The UK's *Daily Mail* reported related concerns because of an over-dependence on cyber-technology within the British national security architecture: 'Cyber terrorists could inflict 'fatal' attack on Britain because Armed Forces rely so heavily on computers, MPs warn'.[3] Meanwhile, also in 2010, *The Australian* similarly cautioned: 'Cyber terrorism threat 'not taken seriously enough''.[4]

Headlines such as these indicate a widespread concern with the threat posed by cyberterrorism to various referents. Indeed, as several authors have argued, the news media has been one of the most prominent sites in which this threat has been securitized. Gabriel Weimann, for instance, suggests that, 'much of the discussion of cyberterrorism has been conducted in the popular media, where journalists typically strive for drama and sensation

[1] Carter Eskew, "Is the U.S. prepared for cyberterrorism?," *The Washington Post*, March 29 2013, accessed December 15 2014, http://www.washingtonpost.com/blogs/post-partisan/wp/2013/03/29/is-the-u-s-prepared-for-cyberterrorism/.

[2] John R. Quain, "10 Years After 9/11, Are America's Cyberdefenses Weaker?," *Fox News*, September 10 2011, accessed December 15 2014, http://www.foxnews.com/tech/2011/09/10/10-years-after-11-are-americas-cyberdefenses-weaker/.

[3] Ian Drury, "Cyber terrorists could inflict 'fatal' attack on Britain because Armed Forces rely so heavily on computers, MPs warn," *Mail Online*, January 9 2013, accessed December 15 2014, http://www.dailymail.co.uk/news/article-2259374/Military-cyber-attack-threat-Armed-Forces-rely-heavily-computers-MPs-warn.html.

[4] Fran Foo, "Cyber terrorism threat 'not taken seriously enough'," *The Australian*, September 14 2010, accessed December 15 2014, http://www.theaustralian.com.au/technology/cyber-terrorism-threat-not-taken-seriously-enough/story-e6frgakx-1225921434904?nk=8348714490b52fe465d858bc0dc812e2.

rather than for good operational definitions of new terms'.[5] Maura Conway, more recently, notes that with 'the aid of the mass media, cyberterrorism came to be viewed as the "new" security threat *par excellence'*.[6] In some ways, there is little unusual here. Print, broadcast and other forms of journalism are frequently accused of exaggerating risks. What makes efforts at securitizing cyberterrorism particularly interesting, however, is that they operate in the absence of two conditions that might increase their plausibility. First, some measure of intellectual consensus that cyberterrorism does indeed pose a significant security threat. And, second, some form of substantiating empirical evidence. In other words, if media discourse does indeed demonstrate a widespread concern with this threat, that concern must be articulated and repeated without the use of possible (and especially dramatic) examples of this phenomenon, on the one hand. And, on the other hand, without invocation of a broader 'common sense' amongst relevant academic 'experts'. This may help explain why, as Michael Stohl notes: 'the media, when they report the possibilities raised by various governmental officials, bureaucrats as well as elected officials, don't necessarily discriminate between those threats which are possible and/or probable and those which are not'.[7]

This article contributes to these explorations by offering the first systematic study of media representations of cyberterrorism of its size. Specifically, it reports on original research into competing constructions of cyberterrorism published by 31 different news

[5] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?", *United States Institute of Peace Special Report* Vol. 119 (2004), n.p.; See also, Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict and Terrorism*, Vol. 28, No. 2 (2005), pp. 129–149.

[6] Maura Conway, "The Media and Cyberterrorism: A Study in the Construction of 'Reality'", (2008). Available: http://doras.dcu.ie/2142/1/2008–5.pdf (accessed 16 May 2013), pp. 43–44.

[7] Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?", *Crime, law and social change*, Vol. 46, No. 4-5 (2006), pp. 223-238, 228.

media outlets across the world between 1 January 2008 and 8 June 2013. The article's first contribution is therefore, simply, to add empirical depth to the conceptual accounts considered above. This is important because, as demonstrated below, there exists some heterogeneity within media constructions of the figure of the 'cyberterrorist' and the threat that s/he poses. At the same time, we are also able to demonstrate that a dominant focus on (i) the activities of offline terrorist groups within media discourse, as well as (ii) a privileging of apprehensive threat assessments around cyberterrorism adds credibility to the above fears around hyperbole and exaggeration. The article's second – analytical – contribution is to highlight the importance of two features which are integral to this discourse yet relatively under-explored. These are, first, the importance of analogy and other forms of comparison with offline or historical events in the construction of threat scenarios. And, second, the role of specific authoritative voices – frequently from the cybersecurity industry – within media coverage, which are widely employed to make sense of the likely consequences of a cyberterrorist attack. These features, we argue, together compensate for the lack of substantiating empirical evidence within news media discourse on cyberterrorism noted above.

The article begins with a brief review of the relevant academic literature on cyberterrorism. Here, we argue that, with few exceptions, this literature is overwhelmingly oriented toward three research questions: (i) what is cyberterrorism?, (ii) what threat does cyberterrorism pose, and to whom?, and (iii) how should this threat be countered? This orientation is problematic, we suggest, for two reasons. First, because it neglects the constitutivity of linguistic and other representations of cyberterrorism. And, second, because it prioritises problem-solving, policy-relevant research over critical enquiry. A second section situates this article within constructivist approaches to security discourse, upon which we

introduce our research methodology and analysis. The article concludes by reflecting on the significance of our findings, before pointing to scope for future research.

Defining, assessing and countering cyberterrorism

Although cyberterrorism presents a comparatively recent addition to our security imaginaries,[8] a burgeoning academic literature has now begun to emerge around this phenomenon. To date, three sets of questions have dominated this work. These concern: (i) the meaning of this term; (ii) the significance of the threat posed by cyberterrorism; and, (iii) appropriate forms of response to this threat.

To begin with definitional issues, four features of the term cyberterrorism generate particular disagreement. The first is the type of conduct required for an act to be considered thus.[9] Broad conceptions encompass the full range of terrorists' online activities, from radicalisation, communication and attack planning through to fundraising, training and propaganda. For some, such an understanding has value for unpacking the plurality of ways in which the Internet has penetrated all aspects of 'the terrorism matrix'.[10] The contrasting – and dominant – view, however, is that the term should not incorporate preparatory and support activities for offline attacks, and that more is to be gained by restricting its use to actual attacks or threats thereof via digital technologies.[11] This leads to a second contested

[8] The origins of the term cyberterrorism are typically located in the mid-1980s, see for example: Barry Collin, "The future of cyberterrorism", *Criminal Justice International*, Vol. 13, No. 2 (1997), pp. 15–18.

[9] Lee Jarvis and Stuart Macdonald, "What is Cyberterrorism? Findings from a Survey of Researchers", *Terrorism and Political Violence*, Vol. 37, No. 1 (2014), pp. 68-90.

[10] Sarah Gordon and Richard Ford, "Cyberterrorism?", *Computers & Security*, Vol. 21, No. 7 (2002), pp. 636-647, 638.

[11] For example, see: Weimann, "Cyberterrorism: The Sum of all Fears?", *op. cit*., pp. 129-149.

feature: the harm requirement. Whilst some definitions – such as Collin's depiction of cyberterrorism as 'hacking with a body count'[12] – insist that a cyberterrorist attack must engender physical violence against people, alternative approaches accept the possibility of other types of target and damage, such as significant economic[13] or environmental damage[14] or even online effects alone.[15] A third contestation concerns intentionality. A common feature of many existing definitions of cyberterrorism is a political or ideological motive and the creation of fear.[16] Others, however, such as Holt argue that relaxing any 'generation of fear' requirement is beneficial for defining cyberterrorism since it recognizes the fact that, 'extremist groups utilize the Internet in ways that more closely resemble the characteristics of

---

[12] Quoted in James D. Ballard, Joseph G. Hornik and Douglas McKenzie, "Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues", *American Behavioral Scientist*, Vol. 45, No. 6 (2002), pp. 989-1016, 992.

[13] Jian Hua and Sanjay Bapna, "How Can We Deter Cyber Terrorism?", *Information Security* Journal, Vol. 21, No. 2 (2012), pp. 102-114.

[14] Keiran Hardy and George Williams, 'What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism' in in T. Chen, L. Jarvis and S. Macdonald (eds.), *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer, 2014), pp. 1-24.

[15] Cronin, A. K. "Behind the curve: Globalisation and international terrorism", *International Security*, Vol. 27, No. 3 (2002-2003), pp. 46-47.

[16] See: Dorothy Denning. "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives", (May 2000), available: <http://www.stealthiss.com/documents/pdf/CYBERTERRORISM.pdf> (accessed 28 June 2015); Jerrold M. Post, Keven G. Ruby and Eric D. Shaw, "From car bombs to logic bombs: The growing threat from information terrorism", *Terrorism and Political Violence*, Vol. 12 No. 2 (2000), p. 101; Ronald Heickerö, "Cyberterrorism: Electronic Jihad", *Strategic Analysis*, Vol. 38, No. 4, (2014), p. 556.

cybercrimes including the dissemination of information to incite violence and harm'.[17] The final contested definitional issue concerns agency. Some stipulate that only non-state actors can perpetrate such acts.[18] On this view, attacks by states are better captured via an alternative label, such as cyberwarfare or cyberespionage. However, the predominant view amongst researchers is that states are also capable of engaging in cyberterrorism, with some authors arguing that they already do so.[19]

A second prominent debate concerns the magnitude of the cyberterrorism threat. Prominent within the 'concerned' literature here are hypothetical examples of the damage cyberterrorists could inflict. In an influential piece published in 1997, for instance, Collin offers several such scenarios including the disruption of air traffic control systems to cause a collision between two large civilian aircraft.[20] Warnings of particular vulnerabilities within cyberspace are prominent too, with many arguing these will increase as further aspects of life migrate online.[21] Wilson, for example, expresses particular concern about zero-day exploits – codes which take advantage of previously unknown vulnerabilities in computer systems –

[17] Thomas J. Holt, "Exploring the Intersections of Technology, Crime, and Terror", *Terrorism & Political Violence*, Vol. 24, No. 2 (2012), pp. 337-354, 341.

[18] Mark M. Pollitt, "Cyberterrorism: Fact or Fancy", *Computer Fraud & Security*, Vol. 2 (1998), pp. 8-10.

[19] Heickerö, *op. cit.*, p. 556; Lee Jarvis, Stuart Macdonald and Lella Nouri, "State Cyberterrorism: A Contradiction in Terms?", *Journal of Terrorism Research*, Vol. 6, No. 3 (2015), pp. 62-75.

[20] Collin, *op. cit*., pp. 15–18.

[21] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community", *Senate Select Committee on Intelligence* (January 2014), available: <http://online.wsj.com/public/resources/documents/DNIthreats2014.pdf> (accessed 28 June 2015).

since no technical defence exists until after their discovery.[22] Weimann, moreover, suggests that cyberattacks may prove attractive to terrorist groups given the wider selection of available targets, the ability to conduct attacks remotely, and the Internet's potential for anonymity.[23] More sceptical views argue cyberterrorism remains unlikely because of a range of factors including: the higher cost of cyberattacks, relative to conventional physical attacks; the complexity of such attacks, and the risks involved in outsourcing to professionals to mitigate this; the proven destructive potential of traditional methods; and, the limited media impact of cyberattacks.[24] More formal cost-benefit analyses similarly conclude that the cost of perpetrating cyberattacks relative to physical attacks such as 9/11 suggests the former are likely to remain an unattractive option for terrorist groups.[25]

The final debate focuses on responses to cyberterrorism. Target-hardening, including the enhanced use of firewalls to act as a form of 'perimeter defence'[26] is one frequently discussed aspect of this debate. Devising appropriate legislation to combat cyberterrorism is

---

[22] Clay Wilson, "Cyber Threats to Critical Information Infrastructure" in T. Chen, L. Jarvis and S. Macdonald (eds.), *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer, 2014), pp. 123-136.

[23] Weimann, "Cyberterrorism: How Real is the Threat?", *op. cit.*

[24] Maura Conway, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism" in T. Chen, L. Jarvis and S. Macdonald (eds.), *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer, 2014), pp. 103-121.

[25] Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", *Studies in Conflict and Terrorism*, Vol. 27, No. 5 (2004), pp. 387-408; Tom Chen and Turki Al-Garni, "A Cost-Damage View of Cyberterrorism" in T. Chen, L. Jarvis and S. Macdonald (eds.), *Terrorism Online: Politics, Law and Technology* (Abingdon: Routledge, 2015), pp. 72-85.

[26] William A. Wulf. and Anita K. Jones, "Reflections on cybersecurity", *Science*, Vol. 326, No. 5955 (2009), p. 943.

another prominent topic of discussion;[27] however the effectiveness of enacting such laws at the domestic level has been questioned.[28] This is, in part, because of the significant problems of attribution in the cyber realm, and the scope for a knowledgeable attacker to avoid detection.[29] Difficulties of attribution also pose challenges for states wishing to respond to cyberattacks under international law given the ability of malicious actors to commit acts without being 'entirely within the territory of a single sovereign'[30] by routing attacks through intermediate systems prior to hitting their target [31] The need for international and public/private coordination therefore attracts much attention in these literatures, [32] although cooperation at each level remains beset by considerable problems.

---

[27] Neal K. Katyal, "Criminal law in cyberspace", *University of Pennsylvania Law Review*, Vol. 149, No. 4 (2001), pp. 1003-1114; Richard W. Downing, "Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime", *Columbia Journal of Transnational Law*, Vol. 43, No. 3 (2005), pp. 705-762.

[28] Patrick Bishop, "Cyberterrorism, Criminal Law and Punishment-based Deterrence" in T. Chen, L. Jarvis and S. Macdonald (eds.), *Terrorism Online: Politics, Law and Technology* (Abingdon: Routledge, 2015), pp. 107-124.

[29] Hua and Bapna, *op. cit.*, pp. 102-114.

[30] Susan W. Brenner, "Cybercrime jurisdiction", *Crime, Law and Social Change*, Vol. 46, No. 4-5 (2006), p. 190.

[31] Susan W. Brenner, ""At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law & Criminology*, Vol. 97, No. 2 (2007), pp. 379-475.

[32] See, for example: Johannes M. Bauer and Michel J. G. van Eethen "Cybersecurity: Stakeholder incentives, externalisites and policy options", *Telecommunications Policy*, Vol. 33, No. 10-11 (2009), pp. 706-719; Steve Purser, "The European cooperative approach to securing critical information infrastructure", *Journal of Business Continuity & Emergency Planning*, Vol. 5, No. 3 (2011), p. 237; Stepanie T. Solansky. and Tammy E. Beck, "Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism

Cyberterrorism discourse

Despite the diversity of perspectives within the above debates, existing literature is overwhelmingly oriented toward a conception of cyberterrorism as an extra-discursive phenomenon. Whether cyberterrorism is approached narrowly or broadly, whether it is perceived as a significant or exaggerated threat, whether or not it is even deemed to have occurred, the actual or potential existence of something that may appropriately be described as 'cyberterrorism' is (at least) implicit in much of this work. Indeed, this general ontological consensus is precisely why the above questions are so intensely debated. Criticisms of overly expansive uses of the term are only possible because they are grounded in alternative (narrower) understandings. Sceptical retorts to hyperbolic threat scenarios, similarly, argue for a reinterpretation of risk by reworking assessments of vulnerability and the likely cost-benefit calculations would-be cyberterrorists might make.[33] A correspondential approach to cyberterrorism knowledge, then, underpins these discussions in which claims are assessed or critiqued for the accuracy with which they represent reality.

This approach to cyberterrorism as something capable of capture in our labels and risk assessments is problematic, we argue, because it neglects the constitutivity of competing

---

exercises", *Administration & Society*, Vol. 40, No. 8 (2009), pp. 852-872; Pardis M. Tehrani and Nazura A. Manap and Hossein Taji, "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime", *Computer Law & Security Review*, Vol. 29, No. 3 (2013), pp. 207-215.

[33] Although this is overwhelmingly the case in the literature on the cyberterrorism threat, alternative - constructivist and deconstructivist - approaches toward desecuritization are, of course also feasible. On this, see: Paul Roe, "Securitization and Minority Rights: Conditions of Desecuritization", *Security Dialogue*, Vol. 35, No. 3 (2004), pp. 279-294.

knowledge claims thereof.[34] Definitions and understandings of cyberterrorism - in law, scholarship, media discourse and elsewhere - create that which they only purport to describe. Cyberterrorism is produced as an identity - as well as a threat - through these very attempts to establish its meaning and significance. Such attempts, moreover, are themselves embedded in etymological and other genealogies, saturated with intertextual relations, reliant upon the positing of sameness and difference between cyberterrorism and other phenomena, and located in (open, yet contested) contexts of cultures, norms, institutions and power relations. Security issues, such as cyberterrorism, are 'made' through social and discursive practice, not 'given'.[35] As such, efforts to define and model it serve to reify cyberterrorism by overlooking the contingent and constructed character of this 'threat'.[36] And, this is the case of numerically-inclined as well as linguistic contributions to this literature, for, 'even when data speak, the language with which they do so is only ever ours, including the categories and algorithms that do the mining and thus constitute the data in the first place'.[37]

---

[34] See: Charlotte Epstein, "Constructivism or the eternal return of universals in International Relations. Why returning to language is vital to prolonging the owl's flight", *European Journal of International Relations*, Vol. 19, No. 3 (2013), pp. 399-519.

[35] For a recent overview on debates over how this process takes place within securitization theory, see Mark B. Salter and Can E. Mutlu, "Securitisation and Diego Garcia", *Review of International Studies*, Vol. 39, No. 4 (2013), pp. 815-834.

[36] Eva Herschinger, "A Battlefield of Meanings: The Struggle for Identity in the UN Debates on a Definition of International Terrorism", *Terrorism and Political Violence*, Vol. 25, No. 2 (2013), pp. 183-201, 184.

[37] Epstein, *op. cit.*, p. 500.

A related, but potentially separable limitation of much existing literature is its problem-solving emphasis.[38] The importance of the question of response considered above, and its connection to ostensibly preliminary work of definition and threat assessment, indicates the value attached to policy relevance within this research. The risk here, of course, is that this reproduces an unnecessarily circumscribed conception of what scholarship should look like that has been widely critiqued within the broader fields of terrorism research and International Relations; a conception that prioritises knowledge's instrumental rather than critical value.[39] Although Cox[40] - and others[41] - attribute merit to problem-solving research in certain contexts, two limitations might be identified. The first is that it risks overlooking the partiality - incompleteness and situatedness - of any knowledge of (here) cyberterrorism. As Breen-Smyth suggests, paraphrasing Cox, 'research, like theory, is from somewhere and for someone…and therefore…claims to objectivity and value-freedom are highly problematic'.[42]

---

[38] Robert W. Cox, "Social Forces, States and World Orders: Beyond International Relations Theory", *Millennium: Journal of International Studies*, Vol. 10, No. 2 (1981), pp. 126-155.

[39] See, amongst others, Jeroen Gunning, "A Case for Critical Terrorism Studies?", *Government and Opposition*, Vol. 42, No. 3 (2007), pp. 363-393; Richard Jackson *et al*, *Terrorism: A Critical Introduction* (Basingtoke: Palgrave, 2011); Lee Jarvis, "The spaces and Faces of Critical Terrorism Studies", *Security Dialogue*, Vol. 40, No. 1 (2009), pp. 5-27.

[40] Cox, *op. cit.*

[41] For example, Harmonie Toros, "'We Don't Negotiate with Terrorists!' Legitimacy and Complexity in Terrorist Conflicts", *Security Dialogue*, Vol. 39, No. 4 (2008), pp. 407-426.

[42] Marie Breen Smyth, "Subjectivities, 'suspect communities', governments, and the ethics of research on 'terrorism'", in R. Jackson, M. B. Smyth and J. Gunning (eds.), *Critical Terrorism Studies: A New Research Agenda* (Abingdon: Routledge, 2009), pp. 194-215.

The second is that paradigmatic norms such as these too readily facilitate the dismissal of non policy-relevant work via charges including pedantry, obscuritanism and irrelevance.[43]

These problems of reification and research orientation have been addressed in relation to terrorism more generally via the emergence of a growing body of 'critical' work sketching the production of terrorism in discourse, practice and technologies.[44] Whilst some of this self-designates as 'critical terrorism studies';[45] much speaks to related audiences within International Relations.[46] On cyberterrorism specifically, a small number of studies now also exist in which a similar meta-theoretical scepticism might be identified. Dunn Cavelty,[47] for instance, employs framing theory to explore the securitization of cyberterrorism within US political discourse. Her 'mini-case study',[48] focused on 'official policy papers, hearings, and

[43] See, for example, David Martin Jones and M.L.R. Smith, "We're all Terrorists Now: Critical - or Hypocritical - Studies "on" Terrorism", *Studies in Conflict & Terrorism*, Vol. 32, No. 4 (2009), pp. 292-302.

[44] See, amongst many others, Louise Amoore and Marieke de Goede, eds., *Risk and the War on Terror* (Abingdon: Routledge, 2008); Ty Solomon, "Social Logics and Normalisation in the War on Terror", *Millennium: Journal of International Studies*, Vol. 38, No. 2 (2009), pp. 269-294; Charlotte Heath-Kelly, "Counter-Terrorism and the Counter-Factual: Producing the 'Radicalisation' Discourse and the UK Prevent Strategy", *British Journal of Politics and International Relations*, Vol. 15, No. 3 (2013), pp. 394-415.

[45] For example, Richard Jackson, *Writing the War on Terrorism: Language, Politics and Counterterrorism* (Manchester: Manchester University Press, 2005); Lee Jarvis, *Times of Terror: Discourse, Temporality and the War on Terror* (Basingstoke: Palgrave, 2011).

[46] Stuart Croft, *Culture, Crisis and America's War on Terror* (Cambridge: Cambridge University Press, 2006); Jack Holland, *Selling the War on Terror: Foreign Policy Discourses after 9/11* (Abingdon: Routledge, 2012).

[47] Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, Vol. 4, No. 1 (2008), pp. 19-36.

[48] Ibid., p. 23.

other statements of key actors';[49] a decision justified for her because, 'Top-level documents reflect actual presidential intentions, as opposed to public statements of purpose, which frequently leave out sensitive details and, on occasion, directly conflict with the stated goals of the administration'.[50] Maura Conway,[51] similarly, sets out to 'excavate'[52] the development of 'cyberterrorism' through an exploration of popular, media and scholarly engagements therewith, while Bowman-Grieve engages with social psychology literature to read news media representations of 'cyberterrorism' through the category of 'moral panics'.[53] Her analysis highlights the importance of different authoritative voices within this process, to which we turn in our discussion below, and draws on a selection of 100 Anglo-American media sources published between 1996 and 2013. It is also possible, finally, to identify constructivist explorations of cyber-security discourse more broadly, wherein cyberterrorism is treated as one of several (discursively) connected threats. Barnand-Wills and Ashenden, for instance, draw on Foucauldian governmentality, 'to identify a relatively consistent discourse of cyber security that involves trends of uncertainty, risk perception, securitization, and potential militarization'[54] within 'current cyber security policy developments in both the

---

[49] Ibid., p. 23.

[50] Ibid., p. 23.

[51] Maura Conway, "Cyberterrorism: Media Myth or Clear and Present Danger?", in J. Irwin (ed.) *War and Virtual War: The Challenges to Communities* (Amsterdam: Editions Rodopi B.V., 2004), pp. 79-98.

[52] Ibid., p. 81.

[53] Lorraine Bowman-Grieve, "Cyber-terrorism and Moral Panics: A reflection on the discourse of cyberterrorism", in T. Chen, L. Jarvis and S. Macdonald (eds.), *Terrorism Online: Politics, Law and Technology* (Abingdon: Routledge, 2015), pp. 86-106.

[54] David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2 (2012), pp. 110-123, 110.

United Kingdom and United States'. [55] Hansen and Nissenbaum, similarly, apply securitization theory to the 2007 cyber war against Estonia to identify, 'three ''security grammars'' distinct to the cyber security sector: hypersecuritizations, everyday security practices, and technifications'.[56]

This article seeks to advance this nascent body of research via a discourse analysis of media representations of cyberterrorism.[57] In contrast to the literature discussed in the above section, it focuses not on what cyberterrorism is, nor on how 'we' should confront this threat. Rather, it asks how cyberterrorism is produced as an identity and a threat within the mainstream news media. This approach is applied to findings from a research project into news items published within thirty-one different international media outlets between 1 January 2008 and 8 June 2013.[58] The project's corpus was generated using a key word search for the terms <cyber terrorism>, <cyberterrorism> and <cyber terror> on the internal search

[55] Ibid., p. 111.

[56] Lene Hansen and Helen Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School", *International Studies Quarterly*, Vol. 53, No. 4 (2009), pp. 1155-1175, 1171.

[57] For more expansive overviews of the commitments of discourse theory than possible here, see Jacob Torfing, *New Theories of Discourse: Laclau, Mouffe and Žižek* (Oxford: Blackwell, 1999); David Howarth, *Discourse* (Buckingham: Open University Press, 2000); David Howarth and Jacob Torfing, eds., *Discourse Theory in European Politics: Identity, Policy and Governance* (Basingstoke: Palgrave, 2005).

[58] To facilitate comparative analysis of the importance of media type, our research included broadsheet newspapers, tabloid newspapers and the websites of media production companies. The thirty-one sources selected were: ABC News, al Aljazeera, The Australian, Australian Financial Review, The Australian Telegraph, BBC, Boston Globe, Channel 4 News, China Daily, CNN, Daily Mail, Financial Times, Fox News, The Guardian, The Herald Sun, The Independent, LA Times, The New York Times, Reuters, Russia Today, Sky News, South China Morning Post, The Straits Times, The Sun, The Sydney Morning Herald, The Telegraph, The Times of India, USA Today, The Wall Street Journal, The Washington Post, The West Australian.

engines of our identified publications. This generated a total of 535 relevant items, including news stories on current affairs, technology stories, opinion pieces, editorial reflections, cultural analysis - including reviews of fictional representations of cyberterrorism[59] - and special reports.

2008 and 2013 were set as the project's parameters for two reasons. First, because this provided sufficient data through which to explore developments in reportage on cyberterrorism: 1986 days of media content in total. And, second, because this period incorporated relevant events which had attracted considerable media coverage, including cyber-attacks on Georgia (2008), revelations of the Stuxnet attack (2010), publication of the UK's *National Security Strategy* (2010), and release of the UK's *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (2011). The thirty-one news outlets were chosen for: reasons of accessibility, which included the availability of a searchable online archive and English medium content;[60] diversity of political perspective, given the prominence of concerns around privacy and liberty within cyberterrorism discourse; to incorporate a range of corporation types; size of readership, where possible favouring publications with the highest circulation figures; and, diversity of geographical origin, seeking to complement the study's primary focus on news outlets in the UK, US and

[59] For instance, cyberterrorism featured prominently in discussion and reviews on the twenty-third film in the James Bond franchise, *Skyfall*, which was released at the end of 2012.

[60] Where possible this research used internal search engines in order to better understand the original presentation of news items around cyberterrorism (including the positioning of photographs, use of sub-headings, and so forth). Where this was not possible – for reasons including institutional subscription and temporal limits on results from internal search engines – we employed LexisNexis.

Australia with others from China, India, Singapore and beyond in order to facilitate international comparison.[61]

Following collection of our data, each news item was subject to a discourse analysis involving two stages. The first stage identified a range of relevant descriptive information under the following headings: Publication title; Online only publication?; Date of publication; URL; Country of publication; Article headline; Article length; and, Is there accompanying imagery, if so of what? The second stage involved an immersive reading of each article 'through' the following themes: What type of piece is the news item (for example is it a current affairs discussion or a technology blog)?; What is the geographical focus of the item?; What, if any, background knowledge is assumed?; Is a specific cyber event mentioned, and if so what?; Is a specific non-cyber event mentioned, and if so what?; Is cyberterrorism the primary or secondary focus, or only mentioned in passing?; How is cyberterrorism depicted (for example, is a narrow or broad understanding evident)?; To what is cyberterrorism compared or contrasted?; Are sources cited, and if so whom or what?; What referent objects are posited? How concerned is the item about the cyberterrorism threat?; How are cyberterrorists represented? What subject position is the reader invited to inhabit?; Any other information of interest or relevance? These categories were generated from our research questions as well as iteratively via analysis of the relevant academic literature and preliminary reading of our data.

Although this article deals with research material generated across the above 'themes' its primary focus is upon questions relating to: representations of cyberterrorism; comparisons between cyberterrorism and other threats; and, citation or invocation of

[61] As one anonymous reviewer identified, there is considerable scope for subsequent research in this area with greater focus on news media sources located within the global South. Better understanding of representations of cyberterrorism within African news sources, in particular, would add to the findings presented in this article.

sources.[62] Moreover, although many of our sources also maintain social media accounts,[63] these accounts tend to focus on directing potential readers to news items. Our commitment to an immersive discourse analysis of news media coverage meant that we therefore focused our research on the news items themselves, rather than any social media output of these organisations.

Cyberterrorism and the news media

It is important to begin our analysis by noting that there is no uniform, uncontested discourse on cyberterrorism within the international news media. Distinct and frequently contrary voices may be identified therein, and uses of the term 'cyberterrorism' are far from consistent.[64] Thus, although cyberterrorism is overwhelmingly presented as a serious, destructive and imminent threat,[65] assessments of the risk this threat poses vary considerably.[66]

A particularly prominent use of the term cyberterrorism in media discourse is with reference to the manipulation of digital technologies by those associated with offline terrorist

---

[62] For findings related to other themes from this research - specifically the volume and tone of media coverage - see Jarvis, L., Macdonald, S. and Whiting, A. "Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage", *Perspectives on Terrorism,* Vol. 9, No. 1 (2015), pp. 60-75.

[63] We are grateful to one of the anonymous reviewers for this point.

[64] See Mark Trevelyan, "Security experts split on "cyberterrorism" threat," *Reuters*, April 17 2008, accessed December 15 2014, http://uk.reuters.com/article/2008/04/17/us-security-cyberspace-idUKL1692021220080417.

[65] See N.A, "Terrorism and cyber-attacks UK's biggest threats," *Channel 4 News*, October 18 2010, accessed December 15 2014, http://www.channel4.com/news/terrorism-and-cyber-attacks-uks-biggest-threats.

[66] See Martin Robinson, "Cyber terror threat to UK is on an 'industrial scale'", *Mail Online*, June 26 2012, accessed 15 December 2014, http://www.dailymail.co.uk/news/article-2164780/Cyber-terror-threat-UK-industrial-scale--says-MI5-chief-reveals-company-lost-800-MILLION-result-state-sponsored-espionage.html.

groups such as al-Qaeda and the Tariq bin Ziyad Brigades. Occasionally such accounts hone in on newsworthy individuals such as Younis Tsouli. Tsouli – a UK resident, and active member on jihadi forums who also committed acts of cyber-crime to fund affiliated causes between 2003 and 2005 – was depicted as one of al-Qaeda's 'most influential cyber-terrorists'.[67] Other stories adopt a more generalized position, for example warning of how Al-Qaida is plotting "cyber jihad" against Britain and the West, making use of 'crack units to target key computer systems'.[68] While these understandings distinguish 'cyberterrorism' from the activities of states, other accounts collapse any such distinction.[69] Mikhel Tammet, Chair of Estonia's Cyber-defence Co-ordination Committee, for example, argues in a piece published by Reuters that there is nothing oxymoronic in likening Russia's alleged 2007 attack on Estonia to 'a kind of terrorism':

---

[67] John Steele, "IT 'anorak' who spread al-Qa'eda hate," *The Telegraph*, January 17 2008, accessed December 15 2014, http://www.telegraph.co.uk/news/uknews/1575842/IT-anorak-who-spread-al-Qaeda-hate.html.

[68] Newscore, "Al-Qaida lotting 'cyber jihad", 14 July 2011, accessed 28 June 2015, http://www.dailytelegraph.com.au/al-qaida-plotting-cyber-jihad/story-fn6e1m7z-1226094225380.

[69] Iran, China and North Korea are frequently associated with cyberterrorism in media coverage. See, respectively: Associated Press, "Iran's foreign ministry says country ready for flexibility at nuclear talks," *Fox News*, October 13 2012, accessed December 15 2014, http://www.foxnews.com/world/2012/10/13/iran-supreme-leader-vows-to-defeat-sanctions-military-threats-and-oft-wars/; Dylan Welch, "Cyber soldiers," *The Sydney Morning* Herald, October 9 2010, accessed December 15 2014, http://www.smh.com.au/technology/technology-news/cyber-soldiers-20101009-16c7e.html; Associated Press and Daily Mail Reporter, "North Korea 'preparing to test another nuclear missile' amid feats of a cyber attack on the U.S.," *Mail Online*, April 8 2013, accessed December 15 2014, http://www.dailymail.co.uk/news/article-2305617/North-Korea-preparing-nuclear-missile-test-amid-fears-cyber-attack-U-S.html.

> The act of terrorism is not to steal from a state, or even to conquer it. It is, as the word suggests, to sow terror itself. If a highly IT country cannot carry out its everyday activities, like banking, it sows terror among the people.[70]

North Korea's alleged 2011 hack of a South Korean bank was portrayed in similar terms. Two stories in our sample implied this constituted cyber-terrorism; three others made an explicit connection, with two of these quoting South Korean prosecutor Kim Young-dae's description of the hack as an 'unprecedented act of cyber terror'.[71]

Activist groups operating online – more widely referred to as 'hacktivists' – also, at times, attract this soubriquet. CNN reported that the most familiar of these groups, Anonymous, found themselves 'dubbed cyberterrorists'.[72] Another collective AntiSec's hacking of more than 70 U.S. law enforcement institutions saw this organisation similarly described as a 'cyberterrorist collaboration'.[73] Coverage of the 2012 hack of Israeli credit card details attributed to Saudi hacker OxOmar also made frequent use of the words of Israeli Deputy Foreign Minister Danny Ayalo,[74] who argued that this constituted, 'a breach of

---

[70] Tammet Mikhel quoted in Adrian Blomfield, "Russia accused over Estonia 'cyber-terrorism'," *The Telegraph*, May 17 2007, accessed December 15 2014, http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html.

[71] Kim Young-dae quoted in Jeremy Laurence and Jonathan Thatcher, "North Korea behind cyber attack on S.Korea bank-prosecutors," *Reuters*, May 3 2011, accessed December 15 2014, http://www.reuters.com/article/2011/05/03/korea-north-cyber-idUSL3E7G31BT20110503.

[72] Ben Brumfield, "Hackers attack Australian spy agency website," *CNN*, August 10 2012, accessed December 15 2014, http://edition.cnn.com/2012/08/10/world/asia/australia-hacking/.

[73] John D. Sutter and Phil Gast, "Group says it hacked 70 U.S. law enforcement sites," *CNN*, August 7 2011, accessed December 15 2014, http://edition.cnn.com/2011/CRIME/08/06/hacking.websites/.

[74] In 8 of the 13 articles that mentioned this event the Minister was quoted comparing the hack to terrorism.

sovereignty comparable to a terrorist operation'.[75] Meanwhile, attacks on businesses are also frequently framed as evidence of the risk of cyberterrorism[76] with the widespread reporting of the following remarks by Sony's former CEO, Sir Howard Stringer indicative here:

> I think you see that cyber terrorism is now a global force, affecting many more companies than just Sony…If hackers can hack Citibank, the FBI and the CIA, and yesterday the video game company Electronics Arts, then it's a negative situation that governments may have to resolve.[77]

Other media reports, finally, 'stretch' this concept still further, with disparate activities including IRA propaganda videos[78], the use of Twitter[79] and hoax terrorist e-mails designated 'cyberterrorist'.[80]

---

[75] Danny Ayalon quoted in N.A., "Israel says credit card hack is 'terrorism'," *Aljazeera*, January 6 2012, accessed December 15 2014, http://www.aljazeera.com/news/middleeast/2012/01/20121845638240672.html.

[76] Donna Fuscaldo, "Protecting small businesses from Cyber Terrorism," *Fox Business*, October 8 2010, accessed December 15 2014, http://smallbusiness.foxbusiness.com/sbc/2010/10/08/protecting-small-businesses-cyber-terrorism/.

[77] Howard Stringer quoted in Reuters, "Sony says Protecting content made it hackers' target," *Fox Business*, June 28 2011, accessed December 15 2014, http://www.foxbusiness.com/technology/2011/06/28/sony-says-protecting-content-made-it-hackers-target/.

[78] Henry McDonald, "MP calls on YouTube to remove Real IRA propaganda videos," *The Guardian*, August 2 200, accessed December 15 2014, http://www.theguardian.com/technology/2009/aug/02/youtube-ira-facebook-cyber-terrorism.

[79] Julian Miglierini, "Mexico 'Twitter terrorism' charges causes uproar," *BBC News*, September 6 2011, accessed December 15 2014, http://www.bbc.co.uk/news/world-latin-america-14800200.

[80] Mateen Hafeez, "Boredom, revenge drive terror hoax calls," *The Times of India*, October 12 2011, accessed December 15 2014, http://timesofindia.indiatimes.com/city/mumbai/Boredom-revenge-drive-terror-hoax-callers/articleshow/10322361.cms.

Analogy, authority and threat construction

Despite this flexibility in the use of the cyberterrorism lexicon, news media coverage is overwhelmingly concerned with the seriousness of this (ambiguous) threat.[81] According to an article in The West Australian, for instance, 'Islamists want to take the world back to the primitive social relations and religious ethos of the 7th century, [and] they are utilising the most advanced digital technology of the modern era in their cause'.[82] The Washington Post, likewise, cites the Assistant Attorney General for National Security John Carlin to inform readers that we are 'very vulnerable'[83] to a terrorist attack on critical infrastructure. Indeed, this is a vulnerability that for, ex-executive assistant director of the FBI Shawn Henry is second only to a 'weapon of mass destruction going off in one of our major cities'.[84]

Dissenting voices do, of course, emerge. Stephen Cummings, former director of the UK Government's Centre for the Protection of National Infrastructure, for example, is cited in a 2008 Reuters story to suggest that cyberterrorism 'distracts our attention

---

[81] See: Jarvis, L., Macdonald, S. and Whiting, A. "Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage", *Perspectives on Terrorism*, Vol. 9, No. 1 (2015), pp. 60-75

[82] N.A., "Jihad waged on digital battlefield," *The West Australian*, November 15 2010, accessed December 15 2014, https://au.news.yahoo.com/thewest/news/a/10806192/jihad-waged-on-digital-battlefield/.

[83] John Carlin quoted in Sam Horwitz, "Justice Department trains prosecutor to combat cyber-espionage," *The Washington Post*, July 25 2012, accessed December 15 2014, http://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html.

[84] Shawn Henry quoted in Sari Horwitz, "Justice Department trains prosecutor to combat cyber-espionage."

from the more pressing terrorist threats, which are still physical'.[85] Cummings concludes, 'Cyberterrorism is a myth'.[86] Other critics offer civil liberty concerns about the uses to which this (fabricated) threat is put. Head of the Australian Council of Civil Liberties Terry O'Gorman, for example, argues to ABC News that attempts to tighten national laws on the grounds of cyberterrorism risk, 'losing the balance between giving the intelligence services sufficient powers to fight terrorism while at the same time keeping longstanding and cherished civil liberties'.[87] These voices of caution are, however, comparatively rare[88] and frequently drowned out by reports of risk and vulnerability. US Senator Dianne Feinstein's discussion of terrorists opening the floodgates of a dam, disrupting air traffic control, or shutting down the New York Stock Exchange is given coverage in a CNN piece titled 'There's nothing virtual about cyber attack'.[89] A 2010 article written by the Daily Mail's Science Editor, Michael Hanlon, outlines a detailed yet entirely fictional example of cyberterrorism from the year 2017 that has catastrophic financial, energy, communication and social consequences far beyond its projected death toll

---

[85] Stephen Cummings quoted in Mark Trevelyan, "Security experts split on "cyberterrorism" threat."

[86] Stephen Cummings quoted in Mark Trevelyan, "Security experts split on "cyberterrorism" threat."

[87] Terry O'Gorman quoted in N.A, "Civil liberties expert slams email spying plans," *ABC News,* April 14 2008, accessed December 15 2014, http://www.abc.net.au/news/2008-04-14/civil-liberties-expert-slams-email-spying-plans/2403100.

[88] Of the news items studied which had cyberterrorism as their primary or secondary focus (n=400), just 12 (3%) were categorised as either sceptical or sceptical with elements of concern, whilst 301 (75%) were classed as concerned or concerned with elements of scepticism. The remainder were classified as either balanced or neither. See: Jarvis, L., Macdonald, S. and Whiting, A, *op. cit.* pp. 60-75.

[89] Dianne Feinstein quoted in Bob Greene, "There's nothing virtual about cyber attack," CNN, October 7 2012, accessed June 28 2015, http://edition.cnn.com/2012/10/07/opinion/greene-cyber-real/.

of 2900. Hanlon dubs this 'Britain's Pearl Harbor': an event that 'brought one of the world's most advanced nations almost to its knees'.[90]

The above examples demonstrate the importance of two features of news media cyberterrorism discourse noted in this article's introduction. The first of these is widespread citation of, or reference to, named figures such as intelligence professionals, political elites and industry representatives with some claim to authority in the area of cyber-security. A Washington Post article of 2010, for example, cites former FBI Director, Robert S. Mueller III, in a discussion of the 'clear interest' terrorists have shown in pursuing 'hacking skills', for inflicting further damage upon 'our economy and our psyche'.[91] In the UK, former Minister for Security and Counter-terrorism Lord West of Spithead,[92] and ex-MI5 Chief Jonathan Evans[93] are similarly cited to reference the ability of terrorist groups

---

[90] Michael Hanlon, "Why Britain is desperately vulnerable to cyber terror," *Mail Online*, October 19 2010, accessed December 15 2014, http://www.dailymail.co.uk/debate/article-1321729/Why-Britain-vulnerable-cyber-terror-attacks.html.

[91] Robert S. Mueller III quoted in Ellen Nakashima, "FBI director warns of 'rapidly expanding' cyberterrorism threat," The Washington Post, 4 March 2010, accessed June 28 2015, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

[92] Lord West of Spithead quoted in Nigel Morris and Jerome Taylor, "Hackers recruited to help fight against cybercrime," *The Independent*, 26 June 2009, accessed June 28 2015, http://www.independent.co.uk/news/uk/crime/hackers-recruited-to-help-fight-against-cybercrime-1719995.html.

[93] Jonathan Evans quoted in Wesley Johnson, "MI5 warning over terror-trained Britons', The Independent, 26 June 2012, accessed 28 June 2015, http://www.independent.co.uk/news/uk/crime/mi5-warning-over-terrortrained-britons-7887775.html; Jonathan Evans quoted in Martin Robinson, "Cyber terror threat to UK is on an 'industrial scale', says MI5 chief as he reveals one company lost £800 MILLION as a result of state-sponsored espionage," Mail Online, 26 June 2012, accessed 28 June 2015,

to cause cyber-disruption. Former Home Secretary, David Blunkett, informs the BBC that 'jihadists', 'could be planning to attack national infrastructure - power grids, telecommunications and the like - via the internet, in order to hit a big and symbolic target: the 2012 London Olympics'.[94] Finally, there are industry experts such as Eugene Kaspersky who asserts that there is a real imminent danger from cyberterrorism: 'I don't want to speak about it' Kaspersky argues, before suggesting: '…we are close, very close, to cyber terrorism. Perhaps already the criminals have sold their skills to the terrorists – and then ... oh, God'.[95]

Invocations of professionals such as the above within this coverage make use of two potentially separable claims to authority. The first, and most obvious, is via reference to the professional standing of the cited individual. So, the Washington Post, for instance, invokes '*Defense Secretary* Leon E. Panetta [who] said that digital attacks "could be as destructive as the terrorist attack on 9/11" and virtually paralyze the country'.[96] A CNN study of the credibility of cyberterrorism-related scenarios within the James Bond film, Skyfall, similarly involved conversation with: 'Morgan Wright, a *decorated former law enforcement officer*

---

http://www.dailymail.co.uk/news/article-2164780/Cyber-terror-threat-UK-industrial-scale--says-MI5-chief-reveals-company-lost-800-MILLION-result-state-sponsored-espionage.html.

[94] David Blunkett quoted in BBC, "Is the UK safe from cyber attack?," BBC News, 30 April 2009, accessed 28 June 2015, http://news.bbc.co.uk/1/hi/technology/8025148.stm.

[95] Eugene Kaspersky quoted in Newscore, "Security expert warns of cyber world war," Fox News, 1 November 2011, accessed 28 June, 2015, http://www.foxnews.com/tech/2011/11/01/expert-at-london-internet-security-conference-warns-cyber-war/.

[96] Robert O'Harrow Jr., "CyberCity allows government hackers to train for attacks," *The Washington* Post, November 26 2012, accessed June 28 2015, http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html (our emphasis).

who has done work relating to cyberterrorism for the United States Department of Justice, the Department of Homeland Security, and the Department of Defense'.[97] And, perhaps most strikingly, a short article written by Jim Dexter at CNN in 2010 sought to establish the "facts" on the cyber threat by gravitating towards a number of experts including the ex-National Intelligence Director Dennis Blair, ex-Senate Intelligence Chairman Dianne Feinstein, the Center for Strategic and International Studies, Robert Knake of the Council on Foreign Relations and Professor Irving Lachow and Courtney Richardson of The National Defense University.[98] Citations such as these make use of what Finlayson and Atkins, following Aristotle, term 'witnesses', understood as: 'anyone (or anything) we bring into our speech to support our claims; anyone whose thoughts might bring insight and whom we think our audience will take seriously'.[99] The persuasiveness of this use of quotation works by an *ad hominem* logic, in which the credentials of the 'witness' are appropriated in order to add credibility due to 'the stature with which the source quoted is held (and thus on collective assumptions about what counts as a valid knowledge claim, and who can make one)'.[100] Thus, in the above examples, it is the implied venerability of political executives or law enforcement officers which encourages audiences to take their arguments seriously – and the lack of such credentials which diminishes the force of dissenting voices.

---

[97] Scott Pierce, "How real is 'Skyfall's' portrayal of cyberterrorism?," CNN, November 14 2012, accessed June 28 2015, http://edition.cnn.com/2012/11/14/showbiz/movies/skyfall-cyberterrorism-pierce/ (our emphasis).

[98] Jim Dexter, "Fact check: Cyberattack threat," CNN, February 16 2010, accessed June 28 2015, http://edition.cnn.com/2010/TECH/02/16/fact.check.cyber.threat/.

[99] Judi Atkins and Alan Finlayson, "... A 40-Year-Old Black Man Made the Point to Me': Everyday Knowledge and the Performance of Leadership in Contemporary British Politics," *Political Studies*, Vol. 61, No. 1 (2013), p. 163.

[100] Ibid.

The second invocation of authority within this coverage is via processes of predication through which particular properties are attributed to quoted individuals that go beyond their institutional affiliations.[101] 'Expertise' is a particularly common attribute here, as with the BBC story on a hacking of the IMF which spoke to, 'Tom Kellerman, a *security expert* who has worked for the IMF',[102] or a story from the same source which ran the following caption beneath a photograph of an individual wearing the now infamous Guy Fawkes mask: 'Anonymous may opt for amusing disguises, but they are a real danger, *according to experts'*.[103]

Track records of previous accurate predictions are also cited. A Telegraph article, for instance, discusses a new book by former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism Richard Clarke which 'paints a doomsday scenario' in which terrorists annex 'the American computer system', noting that, 'Mr Clarke *has been right before*. As anti-terrorism tsar under Mr Clinton and then Mr Bush, he issued dire warnings of the need for better defences against al-Qaeda'.[104] These invocations of

---

[101] See Roxanne Lynn Doty, "Foreign policy as social construction: A post-positivist analysis of US counterinsurgency policy in the Philippines", *International Studies Quarterly* Vol. 37, No. 3, (1993): 297-320; also Linda Ahall and Stefan Borg, "Predication, Presupposition and Subject-Positioning", in Laura J. Shepherd (ed.) *Critical Approaches to Security*. (Abingdon, Routledge: 2013), pp.196-207.

[102] BBC, "Government 'may have hacked IMF'," *BBC News*, June 13 201, accessed June 26 2015, http://www.bbc.co.uk/news/technology-13748488.

[103] Maggie Shiels, "Wikileaks has made leaking secrets 'sexy' say experts," *BBC News*, February 17 2011, accessed June 26 2015, http://www.bbc.co.uk/news/technology-12492933 (our emphasis).

[104] Alex Spillius, "Cyber attack 'could fell US within 15 minutes," *The Telegraph*, May 7 2010, accessed June 28 2015, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7691500/Cyber-attack-could-fell-US-within-15-minutes.html.

expertise provide an important supplement to the above references to institutional authority because of their role in affirming a 'quality, attribute, or property of a person or thing'.[105] Predicates, as Doty points out, construct identities for particular subjects,[106] in this case increasing the reliability of the quoted individuals. As argued in the article's introduction, this is particularly significant given the lack of academic agreement around the meaning or threat of cyberterrorism.

A second prominent feature of this discourse which may also be identified in a number of the examples above is the use of analogy to concretise the potential consequences of a 'cyberterrorist' attack.[107] At times, this involves generic comparison with physical weapons of war. ABC News, for instance, cites the British government's warning that 'a cyberattack on the nation's vital computer networks could be *as disastrous as a bombing*'[108]. The Australian, similarly, reports that 'a nation can be as easily crippled by the loss of its critical infrastructure *as it can by any number of well-placed missiles'*.[109] Alongside such generic analogous reasoning, we also witness comparisons to specific historical events such

---

[105] Doty *op cit*, p.306.

[106] *Ibid*.

[107] This feature has been discussed within the academic literature also, see: Stohl, *op. cit*., 223-238; Conway, 'The Media and Cyberterrorism', *op. cit*., 1-53.

[108] Timothy McDonald, "Governments on alert for cyber terror threat," *ABC News*, October 19 2010, accessed December 15 2014, http://www.abc.net.au/news/2010-10-19/governments-on-alert-for-cyber-terror-threat/2303774. (our emphasis)

[109] Anthony Wong, "Attacking a growing cyber terrorism threat," *The Australian*, March 22 2011, accessed December 15 2014, http://www.theaustralian.com.au/technology/attacking-a-growing-cyber-terrorism-threat/story-e6frgakx-1226025058588?nk=fba151128507993e5a570a5ffa584bf6 (our emphasis).

as the Mumbai attacks of 2008,[110] or – more frequently – to 9/11, Pearl Harbor, the July 7th 2005 London bombings, and even Hurricane Katrina.[111]

Fears around an electronic- or cyber- Pearl Harbor go back to the early 1990s, although these have gained traction in recent years. Remarks by Leon Panetta on this possibility were widely reported in 2012,[112] although comments by former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, Richard Clarke, also generated coverage, as in a Daily Telegraph article titled: 'Cyber attack "could fell US within 15 minutes"'.[113] Panetta has also been widely cited in media use of the 9/11 analogy, such as the Washington Post article warning that a digital attack 'could be *as destructive as the terrorist attack on 9/11*', virtually paralysing the country.[114] As former NSA director Mike McConnell similarly argued – reported in 2012 – American unpreparedness is such that Internet-savvy terrorists could pull off an attack '*in the manner of the raids of September*

---

[110] Matthew Harwood, "America's cybersecurity threat," *The Guardian*, June 7 2009, accessed December 15 2014, http://www.theguardian.com/commentisfree/cifamerica/2009/jun/01/obama-us-cybersecurity-tsar.

[111] Similarities between a potential cyber-attack and the 9/11 events provided the most frequent of these comparisons, occurring in seven separate articles.

[112] Adam Samson, "Another week, another threat against U.S. banks," *Fox Business*, October 16 2012, accessed December 15 2014, http://www.foxbusiness.com/industries/2012/10/16/another-week-another-threat-against-us-banks/.

[113] Alex Spillius, "Cyber attack 'could fell US within 15 minutes," *The Telegraph*, May 7 2010, accessed December 15 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7691500/Cyber-attack-could-fell-US-within-15-minutes.html.

[114] Leon Panetta quoted in Robert O'Harrow Jr., "CyberCity allows government hackers to train for attacks," *The Washington Post*, November 26 2012, accessed July 23 2014, http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html. Our emphasis

11'.[115] In a Guardian report of 2009, it was 9/11's unpredictability rather than destructiveness which was put to analogous effect: 'just *as the 9/11 attacks were an unprecedented attack* with unconventional weapons, so too could a major cyber attack'.[116] The same newspaper also later reported on US efforts to bolster resilience to cyberterrorism through legislation '*aimed at avoiding a cyber "Hurricane Katrina" situation* in which a disaster is aggravated by a bungled government response'.[117] Sami Saydjari – CEO of online security company Cyber Defence Agency – took this analogy further in an open letter to George W. Bush discussed in the BBC and the Guardian to suggest that the: 'potential costs of a multi-critical infrastructure attack on the banking system, the power grid and so on in a sequence designed to do maximum damage approaches the trillions, and *the damage would look like a thousand hurricane Katrinas'*.[118]

The use of analogy in media coverage of cyberterrorism is vital in the construction of this security threat. Images of the destructive potential inherent to generically-framed

---

[115] Mike McConnell quoted in Sari Horwitz, "Justice Department trains prosecutors to combat cyber-espionage," *The Washington Post*, 25 July 2012, accessed 28 June 2015, http://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html.

[116] Bobbie Johnson, "Terrorists could use internet to launch nuclear attack: report," *The Guardian*, July 24 2009, accessed December 15 2014, http://www.theguardian.com/technology/2009/jul/24/internet-cyber-attack-terrorists. (our emphasis)

[117] Daniel Nasaw, "US takes steps to create infrastructure against cyber attack," *The Guardian*, April 7 2009, accessed December 15 2014, http://www.theguardian.com/technology/2009/apr/07/cyber-security-legislation-usa (our emphasis).

[118] Sami Saydari quoted in Ben Hammersley, "Is the UK safe from cyber attack?"; Sami Saydjari quoted in Ravi Somaiya, "Defenders of cyberspace," *The Guardian*, October 2 2008, accessed December 15 2014, http://www.theguardian.com/technology/2008/oct/02/4.

'missiles' and 'bombs' underscore the seriousness of ill-understood technologies and actors for readers. References to specific historical events such as Pearl Harbor, 9/11 and Hurricane Katrina do likewise, while simultaneously reminding audiences that unexpected events do occur. These analogies highlight, modulate and even camouflage aspects of the 'threats' being discussed, not least because events such as 9/11 have been so heavily (re)mediated that their meaning appears, almost, taken-for-granted.[119] As David Mutimer argues in his discussion of proliferation metaphors[120]:

> we must recognize that the metaphors with which a security problem is understood will shape the nature of the problem and its solutions, focusing on the aspects that are highlighted and marginalizing, or ignoring those that are downplayed or hidden in the metaphor's entailments.

Without diminishing the power of these rhetorical figures in shaping understanding of security threats, it is important to note that analogies such as those discussed above do not go uncontested within media discourse. A piece in the Straits Times, for instance, cites Dr Irving Lachow, Senior Associate at the Centre for Strategic & International Studies, who claims that cyberterrorists '*do not have the technical skills* that are up to the mark when it comes to *executing a digital attack with an impact equivalent to 9/11'*. As Lachow, therefore, concludes, cyberterrorism is 'not a likely scenario'.[121] In an article for Aljazeera, similarly,

---

[119] Jacques Derrida, "Autoimmunity: Real and Symbolic Suicides", in G. Borradori (ed.) *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida*, (London, University of Chicago Press: 2003), pp. 85-136.

[120] See also: Myriam Dunn-Cavelty, "From cyber-bombs to political fallout: Threat representation with an impact in the cyber-security discourse", *International Studies Review*, Vol. 15, No. 1 (2013), pp. 105-122.

[121] Irving Lachow quoted in Grace Chng, "Cyber war: One strike, and you're out", *Straits Times*, July 18 2010.

Karen Greenberg discusses the '*old alarm bell* "cyber Pearl Harbor"' in critiquing the 'chilling image' raised by Panetta that 'a cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11'.[122] Greenberg argues that such 'early warnings of dire consequences' sound '*tediously familiar'*, pointing out that in:

> the wake of the actual 9/11 attacks, governmental overreach became commonplace, based on fear-filled scenarios of future doom' that should make us equally suspicious of 'doomsday predictions and distrustful of claims that extraordinary measures are necessary to protect "national security".[123]

Conclusion

Discourses – on security threats and anything else – are productive rather than representational: they create identities and threats while seeming only to refer to them.[124] In this article, we have argued that existing academic literature on cyberterrorism has tended to neglect this insight, due to its organisation around three quite specific questions: definition, threat and response. These questions, we argued, contributed to a widespread (though not uncontested) meta-theoretical frame of reference and sense of scholarly purpose in which cyberterrorism is approached as a real-world problem to be solved. As an attempt to contribute to discursively-oriented explorations of the constitution of 'cyberterrorism' as cyberterrorism, we then introduced findings from our own research into the international news media. Our analysis, we argued, offered two contributions to scholarship. First, it

---

[122] Karen Greenberg, "Will the apocalypse arrive online?," *Aljazeera*, October 28 2012, accessed December 15 2014, http://www.aljazeera.com/indepth/opinion/2012/10/20121023103237429854.html.

[123] Ibid.

[124] For an alternative, 'thinner' understanding, see Benjamin Banta, "Analysing discourse as a causal mechanism", *European Journal of International Relations*, Vol. 19, No. 2 (2012), pp. 379-402.

contributes to existing accounts of the media's importance in the framing of this 'threat' by adding empirical depth to this scholarship. Although some important related work exists, discussed above, this is the first study of its size focused, solely, on the construction of cyberterrorism.

The article's second, analytical, contribution was to highlight the importance of authority and analogy in media efforts to securitise cyberterrorism.[125] Authoritative voices, we argued, are called upon as 'witnesses'[126] both to validate and (less frequently) to contest threat scenarios in this context. This is, moreover, complemented by representations of 'expertise' in the framing of those voices and their importance. Analogies, as explained above, are widely used to help make sense of the consequences and likelihood of potential attacks. Such analogies draw upon 'real' historical events as well as hypothetical constructions of future scenarios. Neither, of course, are neutral, for - as with all rhetorical figures - reference to 9/11, Hurricane Katrina, Pearl Harbor work both to augment and to de-emphasise particular aspects of the events which are being discussed.

None of this is intended to suggest that audiences of cyberterrorism news media discourse automatically internalise dominant understandings, assumptions or analogies such as those considered above. Readers of texts such as these engage in active processes of decoding in which the meaning of such texts is negotiated, and any news story may be read

---

[125] On the former, see, for example, Dider Bigo, "Security and immigration: Toward a critique of the governmentality of unease", *Alternatives: Global, Local, Political*, Vol. 27, No. 1 - Supplement (2002), pp. 63-92.

[126] Atkins and Finlayson, *op. cit.*, p. 163.

more or less faithfully (hence the possibility of oppositional or aberrant readings).[127] This, we suggest, implies the scope for future research building on this work which could include analysis of the ways in which audiences consume cyberterrorism discourse in different media. On top of this there is clearly potential for comparative analysis of – and of intertextualities between – political and media discourse on cyberterrorism. News sources in languages other than English would offer a further point of comparison, allowing enquiry into the productivity of different languages in the construction of cyberterrorism. As, indeed, would engagement with social media discourse and non-written sources such as multi-media coverage on television or online. Such work, we suggest, would build upon this article's analysis of the role of analogy and authority within news media coverage of cyberterrorism, adding to our contribution of empirical depth to existing accounts of the importance of this site of discourse.

Acknowledgements

We express our gratitude to Swansea University's College of Law and Criminology, and to the Bridging The Gaps programme for their support for the research upon which this article is based. Thanks also to members of the University of East Anglia's Critical Global Politics

[127] See, amongst others, Stuart Hall, "Encoding/Decoding", in Meenakshi Gigi Durham and Douglas M. Kellner (eds.) *Media and Cultural Studies: Keyworks (revised edition)*. (Oxford, Blackwell: 2006), pp. 163-173; Colin Hay, "Narrating crisis: the discursive construction of the 'Winter of Discontent'", *Sociology*, Vol. 30, No. 2 (1996), pp.253-277; Douglas M. Kellner and Meenakshi Gigi Durham, "Introduction to Part II", in Meenakshi Gigi Durham and Douglas M. Kellner (eds.) *Media and Cultural Studies: Key Works (revised edition)*. (Oxford, Blackwell: 2006), pp. 91-98.

research group, at which an earlier version of this article was presented. We also gratefully acknowledge Jordan McErlean and Alicia Payne for their excellent research assistance, and David Mair and Lella Nouri for their helpful suggestions throughout the project.

About the Authors

Lee Jarvis is Reader in International Security at the University of East Anglia. He is an editor of *Critical Studies on Terrorism* and (co-) author or editor of nine books, including *Anti-Terrorism, Citizenship and Security* (with Michael Lister, Manchester University Press: 2015), *Security: A Critical Introduction* (with Jack Holland, Palgrave: 2015) and *Counter-Radicalisation: Critical Perspectives* (with Charlotte Heath-Kelly and Christopher Baker-Beall, Routledge: 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) and *Terrorism Online: Politics, Law and Technology* (Abingdon: Routledge, 2015) (both with Lee Jarvis and Thomas Chen). His recent project on security and liberty was funded by the British Academy.

Andrew Whiting is a Lecturer at Birmingham City University. He has had his work published on a range of topics including terrorism, cyberterrorism and radicalisation in *Perspectives on Terrorism,* as well as in edited volumes including *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer, 2014), *Counter-Radicalisation: Critical Perspectives* (Abingdon: Routledge, 2015) and *Researching Terrorism, Peace and Conflict Studies* (Abingdon: Routledge, 2015).

Contact details
Corresponding author: Lee Jarvis, School of Politics, Philosophy, Language and Communication Studies, Faculty of Arts and Humanities, University of East Anglia, Norwich Research Park, Norwich, UK, NR4 7TJ. Email: l.jarvis@uea.ac.uk Tel. +44 (0)1603 592 356.

Stuart Macdonald, College of Law, Richard Price Building, Swansea University, Singleton Park, Swansea SA2 8PP, Wales, UK. Email: s.macdonald@swansea.ac.uk Tel. +44 (0)1792 602411

Andrew Whiting, School of Business, Law and Social Sciences, Curzon Building, Birmingham City University, B4 7BD. Email: andrew.whiting@bcu.ac.uk Tel. +44 (0)121 300 4448.