Unpacking cyberterrorism discourse: Specificity, status and scale in news media constructions of threat

Abstract

This article explores original empirical findings from a research project investigating representations of cyberterrorism in the international news media. Drawing on a sample of 535 items published by 31 outlets between 2008 and 2013, it focuses on four questions. First, how individuated a presence is cyberterrorism given within news media coverage? Second, how significant a threat is cyberterrorism deemed to pose? Third, how is the identity of 'cyberterrorists' portrayed? And, fourth, who or what is identified as the referent – that which is threatened – within this coverage? The article argues that constructions of specificity, status and scale play an important, yet hitherto under-explored, role within articulations of concern about the threat posed by cyberterrorism. Moreover, unpacking news coverage of cyberterrorism in this way leads to a more variegated picture than that of the vague and hyperbolic media discourse often identified by critics. The article concludes by pointing to several promising future research agendas to build on this work.

Key words: Cyberterrorism; Discourse; Media; Construction; Threat

Introduction

Although it is a relatively new concept,[1] recent years have witnessed a significant growth of academic and political interest in cyberterrorism. Within the scholarly literature – in common with terrorism research more broadly[2] – two discussions have been particularly prominent. First, is the question of definition. Although Dorothy Denning's relatively narrow understanding of cyberterrorism remains the best-known and most widely-used,[3] considerable debate continues around the respective merits of

[1] 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, 13:2 (1997), pp. 15–18.

[2] For an overview of issues around the definition of terrorism, see Alex P. Schmid, 'The Definition of Terrorism', in Alex P. Schmid (ed.) The Routledge Handbook of Terrorism Research (Abingdon: Routledge, 2013), pp. 39-98. For recent contributions to debate on the definition of terrorism, compare: Anthony Richard, 'Conceptualizing Terrorism', Studies in Conflict & Terrorism, 37:3 (2014), pp. 213-236; Gilbert Ramsey, 'Why Terrorism Can, but should not be Defined', Critical Studies on Terrorism, 8:2 (2015), pp. 211-228. For an engaging discussion on the issues around the threat posed by terrorism, compare Mueller's 'six rather unusual propositions' article with the responses from Richard Betts, Daniel Byman and Martha Crenshaw in the same issue of *Terrorism and Political Violence*: John Mueller, 'Six Rather Unusual Propositions about Terrorism', Terrorism and Political Violence, 17:4 (2005), pp. 487-505.

[3] Denning described cyberterrorism thus: "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers,

restrictive and flexible conceptualisations of this term.[4] The second prominent debate relates to the threat posed by cyberterrorism to various referents including, *inter alia*, national security, corporations, and ordinary citizens.[5]

Concerned assessments of the cyberterrorism threat highlight infrastructural and socio-political vulnerabilities at risk of exploitation by appropriately resourced and intentioned actors. Approached thus, cyberterrorism emerges as a relatively

---

networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not". See: Dorothy E. Denning, *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives*. Washington, Washington D.C., May 2000.

[4] Compare, for example: Sarah Gordon, and Richard Ford, 'Cyberterrorism?', *Computers & Security* 21:7 (2002), pp. 636-647; Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'use' of the Internet', *First Monday*, 7:11 (2002); Dorothy Denning, 'A View of Cyberterrorism Five Years Later', in Kenneth Himma (ed.), Internet Security: Hacking, Counterhacking, and Society (London: Jones and Bartlett Publishers, 2007), pp. 123-140; Lee Jarvis and Stuart Macdonald, 'What is cyberterrorism? Findings from a survey of researchers', *Terrorism and Political Violence*, online first (2014), pp. 1-22.

[5] For an overview, see: Lee Jarvis, Stuart Macdonald, and Lella Nouri, 'The Cyberterrorism Threat: Findings from a Survey of Researchers', Studies in Conflict & Terrorism, 37:1 (2014), pp. 68-90.

straightforward danger of potentially catastrophic significance. Hyperbolic scenarios are widespread here, especially the risk of a 'Digital Pearl Harbour': 'a debilitating, full-scale digital assault - in which multiple attacks are launched against telecommunications networks, city power grids, and/or air traffic control systems, causing widespread destruction and possible loss of life'.[6] Such scenarios point, first, to the widespread construction of cyberterrorism as a generalised and homogeneous threat within this 'concerned' literature: a threat that remains insufficiently unpacked within academic – as much as media – analysis. And, second, to the importance of figurative language within the framing of this threat. As with terrorism discourse more broadly[7], metaphors employed to make sense of cyberterrorism work to (re)produce that to which they appear to refer, often with tangible discursive and political implications:

> Metaphors matter. We choose our words from within a dominant system or frame of metaphor that offers us a specific lexicon of language, that defines words in certain specific ways, and shapes both the "what" and the "how" of our communication. In this way, figuratively and often literally, through metaphor we make meaning. Our most common metaphors help us to understand problems and conflicts in certain ways, offering us certain available responses, and

[6] John D. Podesta and Raj Goyle, 'Lost in cyberspace? Finding American liberties in a dangerous digital world', Yale Law and Policy Review, 27:5 (2005), p. 516.

[7] See: Richard Jackson, Writing the War on Terrorism: Language, Politics and Counterterrorism (Manchester: Manchester University Press, 2005).

> negating or obscuring others. Metaphor operates in the realm of thought, but its workings reverberate in concrete, active, tangible ways.[8]

Less troubled analyses of the cyberterrorism threat, in contrast, tend to justify a more sceptical stance through cost-benefit analysis,[9] or via inductive reasoning from existing knowledge of the likelihood and consequences of offline terrorist attacks.[10] A common – although not universal – theme within these more sceptical assessments of the cyberterrorism threat is the importance of discursive renderings thereof. That is, for a number of authors, constructions of the danger posed by cyberterrorism themselves help to *constitute* or *create* this phenomenon as a significant and urgent security challenge. Cyberterrorism, in other words, might be thought of as a social construction rather than an extra-discursive reality: its existence is (at least in part) a product of

[8] Erin Steuter and Deborah Wills (2009) *At war with metaphor: Media, propaganda, and racism in the War on Terror*. Plymouth: Lexington Books, p. 3.

[9] Compare Giampiero Giacomello, 'Bangs for the buck: A cost-benefit analysis of cyberterrorism', Studies in Conflict & Terrorism, 27:5 (2004), pp. 387-408 with Turki Al-Garni and Thomas M. Chen, 'An updated cost-benefit view of cyberterrorism', in Lee Jarvis, Stuart Macdonald and Tom Chen (eds.), Terrorism Online: Politics, Law and Technology (Abingdon, Routledge, 2015), pp. 72-85.

[10] Maura Conway, 'Reality check: assessing the (un) likelihood of cyberterrorism', in Tom Chen, Lee Jarvis and Stuart Macdonald (eds.), Cyberterrorism: Understanding, Assessment and Response (Springer, New York, NY, 2014), pp. 103-121.

meaning-making practices associated, variously, with political rhetoric, popular culture, cyber-security corporations, or the news media.[11] As Francois Debrix argues, comparing contemporary representations of cyberterrorism with the 'techno-strategic' nuclear weapons discourse explored in Carol Cohn's[12] pioneering Cold War study:

> The language of cyberterrorism mobilized by the media and its so-called experts is quite technical for sure. But this technicality, far from de-realizing the threat, makes it possible. It realizes it in the mind/psyche of the public who is subjected to the simulated scenarios and mediations. The taxonomy of cyberterrorism and its technocratic language allow the public to recognize that there *is* a threat, and that this threat, as presented to them by the media, will surely cause serious casualties within the population.[13]

For Myriam Dunn Cavelty, more forcefully:

[11] 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 5 January 2016); Gabriel Weimann, 'Cyberterrorism: The sum of all fears?', Studies in Conflict & Terrorism, 28:2 (2005), pp. 129-149.

[12] Carol Cohn, 'Sex and death in the rational world of defense intellectuals', *Signs*, 12:4 (1987), pp. 687-718.

[13] Francois Debrix, 'Cyberterror and media-induced fears: the production of emergency culture', Strategies: Journal of Theory, Culture & Politics, 14:1 (2001), pp. 149-168, 164.

> While governments and the media repeatedly distribute information about cyber-threats, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory. In fact, menacing scenarios of major disruptive occurrences in the cyber-domain, triggered by malicious actors, have remained just that – scenarios.[14]

Analyses such as these are important for two reasons. First, they indicate the pervasiveness and prominence of (representations of) 'cyberterrorism' across diverse social, political and cultural sites – from Hollywood movies to political language, media coverage and beyond. Second, they also serve to open significant new research questions beyond those surrounding the issues of definition and threat noted above. These include questions around the content, framing and reception of (various) 'cyberterrorism' discourse(s), as well as the constitutive or causal power such discourses might possess.[15]

This article builds on this work on constructions of cyberterrorism, approaching representations of the definition, threat and characteristics of cyberterrorism as vital to its emergence as an object of knowledge. Specifically, it offers a detailed empirical

[14] Myriam Dunn Cavelty, 'Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate', Journal of Information Technology & Politics, 4:1 (2008), pp. 19-36, 20.

[15] See, for example: Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello, 'From 'cyberterrorism' to 'cyberwar', back and forth', in Johan Erikson and Giampiero Giacomello (eds.), International Relations and Security in the Digital Age (Abingdon: Routledge, 2007), pp. 57-82.

analysis of an original research sample of 535 items published by thirty-one international news media outlets between 2008 and 2013. This analysis extends this work above by focusing attention on the considerable – and often overlooked – variances in (news media) constructions of this threat and the importance of these via investigation of four research questions that emerge from the above debates on definition and danger. First, how individuated a presence does cyberterrorism occupy within news coverage making mention of this threat? For instance, does cyberterrorism receive sustained, differentiated analysis within relevant news items, or is it collocated with other cyber-security challenges or, indeed, other types of terrorism when it is discussed? Second, how significant a threat is cyberterrorism deemed to pose? Is the news media dominated by 'concerned' or 'sceptical' portrayals of this phenomenon, and are there variances across time or space? Third, how are 'cyberterrorists' identified within this coverage? Are they, for instance, portrayed as professional or amateur, as politically motivated, as non-state actors, and so on? And, fourth, who or what is positioned as the referent – the entity threatened by cyberterrorism? Does the perceived vulnerability of particular actors or infrastructures feature more prominently in the news media than others?[16]

[16] Research question two, three and four all involved coding the news stories for threat assessment, type of actor and referent object. This coding was done in relation to the particular emphasis of the news piece being analysed. This did mean that there was a certain degree of blurring between one

Our analysis of these questions is intended to make two immediate contributions to existing scholarship. The first is to add empirical detail to relevant literature on cyberterrorism and cybersecurity more broadly. Although numerous scholars have highlighted the importance of news media discourse in relation to this threat,[17] this study is the first of its size to be focused specifically on constructions of cyberterrorism. As detailed in the conclusion, our findings open considerable space for further research, including comparative analysis of different media. The article's second contribution is to add analytical depth to existing accounts of the content and framing of cyberterrorism discourse. To do this, we focus our analysis on three factors which, in our sample, intervened in media assessments of the threat posed by cyberterrorists. These are: (i) *specificity* – referring to the degree of individuated attention afforded to cyberterrorism within a particular news item; (ii) *status* – the type of actor positioned as a would-be

---

category and another and while objectivity was not possible as part of this process the categories do serve to highlight how threats are framed in news media coverage.

[17] Lorraine Bowman-Grieve, '"Cyber-terrorism and Moral Panics: A reflection on the discourse of cyberterrorism', in Tom Chen, Lee Jarvis and Stuart Macdonald (eds.), Terrorism Online: Politics, Law and Technology (Abingdon: Routledge, 2015), pp. 86-106; Maura Conway, 'Cyberterrorism: Media Myth or Clear and Present Danger?",' in Jones Irwin (ed.) War and Virtual War: The Challenges to Communities (Amsterdam: Editions Rodopi B.V., 2004), pp. 79-98; Michael Stohl, 'Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?', Crime, law and social change, 46:4-5 (2006), pp. 223-238.

cyberterrorist; and, iii) *scale* – the size of referent threatened by cyberterrorism. As demonstrated below, anxiety about the threat posed by cyberterrorism tends to increase with the level of individuated attention afforded to this phenomenon in a particular news item. Moreover, particular constructions of cyberterrorists – as either professional or unskilled actors – and geographically larger referents – especially 'the West' or the entire globe – are also associated with heightened levels of concern than their counterparts. As this suggests, our research points to a far more fractured, heterogeneous and variegated cyberterrorism discourse than is frequently identified by critics of media hyperbole in this context; a discourse in which variations matter a great deal. Indeed, as shown below, the most apprehensive media assessments of cyberterrorism tend to draw upon a very specific construction of cyberterrorism as the activity of either professionals or unskilled actors targeted at 'the West' or the entire world. These constructions also, importantly, typically differentiate cyberterrorism from other threats such as cyberwar, and draw heavily upon perceived sources of authoritative expertise from industry, politics or academia.

Constructing (cyber)terrorism

Recent years have witnessed the emergence of a diverse, broadly constructivist, literature which seeks to excavate, situate, and deconstruct the diverse ways in which

the phenomenon of terrorism has been discursively produced.[18] Associated with, but extending beyond, so-called 'critical terrorism studies',[19] this work has demonstrated the significance of film, television shows, video games, executive political speech, legislative debate, the news media, and much else besides to explore how terrorism: "as a social fact…comes into being within, and is dependent upon, the contextual, historical and political dynamics that structure its interpretation thus".[20] The point of this research, as Stump and Dixit argue, is not to question whether terrorism – or, here, cyberterrorism – exists. Rather, to shift the analyst's gaze from (cyber)terrorism as brute material reality to '(cyber)terrorism' as discursive production, in order: '…to study how representations of terrorism and their reality are socially produced through linguistic and non-linguistic practices.' As they continue, 'Explaining terrorism, to borrow from

[18] See, amongst many others: Richard Jackson, Writing the War on Terrorism: Language, Politics and Counterterrorism (Manchester: Manchester University Press, 2005); Stuart Croft, Culture, Crisis and America's War on Terror (Cambridge: Cambridge University Press, 2006); Carol K. Winkler, In The Name of Terrorism: Presidents on Political Violence (New York, NY: SUNY, 2006); Lisa Stampnitzky, Disciplining Terror: How Experts Invented 'Terrorism' (Cambridge: Cambridge University Press, 2013).

[19] Jeroen Gunning, 'A Case for Critical Terrorism Studies?', Government and Opposition, 42:3 (2007), pp. 363-393; Richard Jackson, Marie Breen Smyth, and Jeroen Gunning, (eds.) Critical terrorism studies: a new research agenda (Abingdon: Routledge, 2009).

[20] Richard Jackson, Lee Jarvis, Jeroen Gunning, and Marie Breen Smyth, Terrorism: A Critical Introduction (Basingstoke: Palgrave, 2011), p.119.

Jonathan Potter, is not a matter of 'denying the existence of tables' or terrorists, but rather a matter of 'exploring the various ways in which their reality is constructed and undermined'.[21]

In common with other constructivist work on security, it is the constitutivity of competing claims relating to terrorism that is emphasised within this literature.[22] The multitude of different definitions and understandings of terrorism that are observable across a wide array of discursive spaces have a productive effect as opposed to one that is merely reflective or descriptive. That is, the threat of terrorism, as well as the identity 'terrorist', are not made with reference to some extra-discursive, objective 'reality' of terrorism; they are, rather, created *through* such assertions (albeit with variable levels of stability). Importantly, such attempts to secure the meaning of terrorism are themselves also: situated in specific etymological and other genealogies; dependent on various intertextual relations; made manifest through identifications of similarity and difference between terrorism and other risks; and situated in a diverse range of (open, yet contested) social and cultural contexts. Terrorism and other security issues are,

[21] Jacob L. Stump and Priya Dixit, 'Toward a completely constructivist critical terrorism studies', International Relations, 26: 2 (2012), pp. 199-217, 210.

[22] 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, 19:3 (2013), pp. 399-519.

therefore, not a 'given'[23] but instead a discursive and social production. Any effort to define terrorism, or to assess the severity of the threat that it poses, do so at the expense of overlooking the constructed and contingent character of this phenomenon.[24] Approached thus, the task for analysts is not to explore the accuracy of dominant discourses on (cyber)terrorism, nor even to explore their causal impact upon policymaking in the 'real world'. Rather, it is to describe and unpack the material from which such discourses are created and to highlight moments of instability, paradox, contradiction and heterogeneity therein.[25]

This article furthers this research by presenting findings from a discursive analysis of a corpus of news media items on cyberterrorism published across a total of thirty-one different media outlets between 1 January 2008 and 8 June 2013. This sample included media hosted in Australia, China, India, Russia, Singapore, the United Kingdom, and the United States, and spanned broadsheet newspapers, tabloid

[23] See, for example, Mark B. Salter and Can E. Mutlu, "Securitisation and Diego Garcia", Review of International Studies, 39:4 (2013), pp. 815-834.

[24] Eva Herschinger, "A Battlefield of Meanings: The Struggle for Identity in the UN Debates on a Definition of International Terrorism", Terrorism and Political Violence, 25: 2 (2013), pp. 183-201, 184.

[25] See, Richard K. Ashley and Rob BJ Walker. "Conclusion: reading dissidence/writing the discipline: crisis and the question of sovereignty in international studies", International Studies Quarterly 34:3 (1990), pp. 367-416, p.384.

newspapers, and the websites of media production companies.[26] These media outlets were selected for a combination of purposive factors which included: accessibility to the researchers, including the presence of an internal online archive of content; diversity of political perspective and type of media corporation, given that concerns around privacy and liberty are particularly prominent within cybersecurity discourse; total size of readership, where possible favouring publications with the highest circulation figures; diversity of geographical origin in order to facilitate international comparison; and language, such that the news content was provided in the medium of English.[27] The corpus of news items identified across this sample was subsequently generated via a key word search for the terms <cyber terrorism>, <cyberterrorism> and <cyber terror> on

[26] The thirty-one sources 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.

[27] For explicit comparative analysis between media corporations and across national borders, please see Lee Jarvis, Stuart Macdonald and Andrew Whiting, "Constructing cyberterrorism as a security threat: a study of international news media coverage", Perspectives on Terrorism 9:1 (2015), pp. 60-75. and Lee Jarvis, Stuart Macdonald and Andrew Whiting, "Analogy and authority in cyberterrorism discourse: An analysis of global news media coverage", Global Society (2016).

the internal search engines of these sites, where possible.[28] This established a total of 535 relevant items for analysis. As detailed further below, these items varied considerably, and included news articles on current affairs, technology stories, opinion pieces, editorial discussion, and analysis of cultural events, including reviews of fictional depictions representations of cyberterrorism.[29]

2008 and 2013 were fixed as the parameters for this research for two reasons. First, because this provided us with sufficient data through which to explore developments within media discourse on cyberterrorism: a total of 1986 days of content. Second, because this period also incorporated a number of potentially relevant events that attracted considerable media interest as they unfolded.[30] These events included the cyber-attacks on Georgia that took place in the summer of 2008; the 2010 identification

[28] 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.

[29] 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.

[30] As one anonymous reviewer helpfully noted, there is certainly scope here for further research on news media coverage both prior and subsequent to our sample. Such research would incorporate reportage on other potentially relevant events such as the 2007 attacks in Estonia, or the 2015 attack against the French broadcaster TV5Monde.

of the Stuxnet attack against nuclear centrifuges in Iran; the 2010 publication of the UK's *National Security Strategy* in which cybersecurity threats occupied a place of prominence, and the subsequent release of the UK's *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* in 2011. Following data collection, each of the 535 news items was coded for relevant descriptive information and for thematic analysis.[31] These categories were generated from the project's research questions as well as iteratively via a preliminary reading of our data.

News media representations of cyberterrorism

[31] The descriptive information identified was as follows: (i) Publication title; (ii) Online only publication?; (iii) Date of publication; (iv) URL; (v) Country of publication; (vi) Article headline; (vii) Article length; and, (viii) Accompanying imagery? The thematic analysis involved coding for the following: (i) What type of piece is the news item (for example is it a discussion of current affairs or a technology blog)?; (ii) What is the geographical focus of the item?; (iii) What, if any, background knowledge around cyberterrorism or cyber-security is assumed?; (iv) Is a specific cyber event mentioned, and if so what?; (v) Is a specific non-cyber event mentioned, and if so what?; (vi) Is cyberterrorism the primary or secondary focus, or only mentioned in passing?; (vii) How is cyberterrorism depicted (for example, is a narrow or broad understanding evident)?; (viii) To what is cyberterrorism compared or contrasted?; (ix) Are sources cited, and if so whom or what?; (x) What referents are posited in the news item? (xi) How concerned is the item about the cyberterrorism threat?; (xii) How are cyberterrorists represented? (xiii) What subject position is the reader invited to inhabit?; (xiv) Is there any other information of interest or relevance?

As noted above, each of the 535 news items identified in our research sample was coded according to the extent of its focus on cyberterrorism as an individuated concern. 400 of these items had a primary or secondary focus on cyberterrorism (see Table 1). Items with a primary focus were those that concentrated exclusively or principally on the issue of cyberterrorism (however defined);[32] items with a secondary focus paid attention to this phenomenon without it constituting a main focus of the piece.[33] Those categorised as 'other' mentioned cyberterrorism at some point, but lacked any level of engagement with this concept sufficient for meaningful analysis.[34]

[Insert table 1 here]

[32] For example: Newscore, 'Al Qaeda's 'cyber jihad' to target social networking sites', Fox News, July 13 2011, available at: {http://www.foxnews.com/tech/2011/07/13/terrorists-announce-cyber-jihad-targeting-social-networking-sites-in-west.html} accessed January 5 2016.

[33] For example: Kevin Rudd, 'Just a mouse click away from war,' The Telegraph, September 19 2011, available at: {http://www.dailytelegraph.com.au/news/opinion/just-a-mouse-click-away-from-war/story-e6frezz0-1226140275845?nk=db62392fbe69ea158a1f9c79b4e30dd3} accessed January 5 2016.

[34] For example: Ted Regencia, 'Obama and Romney faulted for china-bashing', Aljazeera, October 22 2012, available at: {http://www.aljazeera.com/indepth/features/2012/10/2012102112493282290.html} accessed January 5 2016.

The 400 news items with cyberterrorism as a primary or secondary focus were subsequently categorised according to the level of concern each exhibited about the cyberterrorism threat. Six different levels of concern were identified following a detailed, immersive reading, characterised as: concerned; concerned, with elements of scepticism; balanced; sceptical; sceptical, with elements of concern; and, neither.

A story was coded as *concerned* or *sceptical* if it was characterised by a clearly identifiable stance on the threat posed by cyberterrorism, offering no space for consideration of alternative perspectives. Examples of the former include Jemima Kiss' article for the UK's *Guardian* newspaper, which cites Eugene Kaspersky's connection of the Stuxnet virus to 'three incidents of cyber-terrorism' and concludes that things 'are only going to get worse'.[35] Joseph S. Nye's 2011 article in *The New York Times*, similarly, cites ex-NSA director Mike McConnell's assessment that 'Sooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier',[36] without challenge from competing voices. As chart 1 demonstrates, two-thirds (67%) of the 400 news items in our study demonstrated a distinctively "concerned"

[35] Jemima Kiss, 'Future cyber attacks could prove catastrophic, say online security experts', The Guardian, January 21 2013, available at: {http://www.theguardian.com/technology/2013/jan/21/future-cyber-threats-catastrophic-dld-2013} accessed January 5 2016.

[36] Mike McConnell, cited in Joseph S. Nye, 'Cyberspace wars', The New York Times, February 27 2011, available at: {http://www.nytimes.com/2011/02/28/opinion/28iht-ednye28.html?_r=1&} accessed January 5 2016.

perspective on cyberterrorism. In stark contrast, only 2% of coverage across this time period took an explicitly sceptical stance toward this threat. Examples of these minority views included Duncan Campbell's 2009 piece in *The Guardian*, which approached Gary McKinnon's potential extradition to the United States as a product of misplaced fears over cyberterrorism in the post-9/11 period.[37] Another article in the same newspaper by Glenn Greenwald (writing prior to the Edward Snowden revelations) similarly sought to contest Leon Panetta's assertion that extremist groups armed with "cyber tools" could gain control of "critical switches" to cause catastrophic disruption, arguing:[38]

> This massive new expenditure of money is not primarily devoted to defending against cyber-aggressors. The US itself is the world's leading cyber-aggressor. A major purpose of this expansion is to strengthen the US's ability to destroy other nations with cyber-attacks.[39]

---

[37] David Campbell, 'If Labour can't protect people like Gary McKinnon, it really stands for nothing', The Guardian, available at: {http://www.theguardian.com/commentisfree/2009/jun/08/gary-mckinnon-hacker-court} accessed January 5 2016.

[38] Leon E. Panetta, 'Remarks by Secretary Panetta on Cybersecurity' (presentation, to the Business Executives for National Security at the, New York, NY, October 11 2012) available at: {http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136} accessed January 5 2016.

[39] Glenn Greenwald, 'Pentagon's new massive expansion of 'cyber-security' unit is about everything except defense', The Guardian, January 28 2013, available at:

Stories coded as either *concerned with elements of scepticism* or *sceptical with elements of concern* evidenced a dominant narrative while also providing space to a rival interpretation. 8% of items in our sample were concerned with elements of scepticism, with only 1% categorised as sceptical with elements of concern. An example of the former is Tim McDonald's 2010 piece for *ABC News Australia* which reports that governments are on alert for the threat of cyberterrorism.[40] Whilst reflections from the UK's former Foreign Secretary William Hague are cited to bolster this perspective,[41] the story concludes by citing Bill Gates' opinion that – with an appropriate governmental approach – cyberterrorism 'shouldn't be something that people will have to worry about'.[42] Karen Greenberg's 2012 piece for *Aljazeera*, in contrast, was clearly

---

{http://www.theguardian.com/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet} accessed January 5 2016.

[40] Timothy McDonald, 'Governments on alert for cyberterror threat,' ABC News Australia, October 19 2010, available at: {http://www.abc.net.au/news/2010-10-19/governments-on-alert-for-cyber-terror-threat/2303774} accessed January 5 2016.

[41] For sustained analysis of the use of 'expert' witnesses in this news media coverage, see Lee Jarvis, Stuart Macdonald and Andrew Whiting (2016).

[42] Timothy McDonald, 'Governments on alert for cyberterror threat,' ABC News Australia, October 19 2010, available at: {http://www.abc.net.au/news/2010-10-19/governments-on-alert-for-cyber-terror-threat/2303774} accessed January 5 2016.

sceptical about the significance of this threat, albeit while demonstrating elements of concern. This article's primary focus concerned how the language of cyber-defence (including the lexicon of counterterrorism) facilitates encroachment on civil liberties. At the same time, Greenberg does not reject the possibility of genuine cyber-threats outright, conceding that 'potential attacks, according to leading cyber experts, are possible'.[43]

Balanced coverage was characterised by the presence of competing narratives over the cyberterrorism threat and the absence of any definitive conclusion about the plausibility of these. For example, a *Russia Today* article from 2012 pays significant attention to the concerns of American security professionals about cyberterrorism before subsequently exploring the views of more sceptical 'experts'.[44] As chart 1 demonstrates, 7% of items across this time period took a balanced approach to the cyberterrorism threat. Finally, a story was categorised as *neither* if it discussed cyberterrorism but refrained from offering any clear assessment on the threat thereof. The UK's *Daily Mail*, for example, reported on Pakistan's introduction of new laws to combat

[43] Karen Greenberg, 'Will the apocalypse arrive online?,' Aljazeera, October 28 2012, available at: {http://www.aljazeera.com/indepth/opinion/2012/10/20121023103237429854.html} accessed January 5 2016.

[44] 'Is cyberwar hype fuelling a cybersecurity-industrial complex?', Russia Today, February 16 2012, available at: {http://rt.com/usa/security-us-cyber-threat-529/} accessed January 5 2016.

cyberterrorism without reflection on their need or utility.[45] 15% of items in our sample fit into this category.

[Insert chart 1 here]

As the above suggests, three-quarters of the news items examined in our research expressed concern toward the threat posed by cyberterrorism, with only a small proportion of these qualifying this with competing, sceptical perspectives. Importantly, as table 2 shows, the levels of concern about cyberterrorism varied according to the *specificity* of the coverage. Thus, 75% of the items which focussed primarily on cyberterrorism were concerned (compared to 65% for those with cyberterrorism as their secondary focus), and a further 11% were classed as concerned with elements of scepticism (compared to 8% for those with cyberterrorism as their secondary focus). In other words, levels of concern increased where there was a specific focus on cyberterrorism.

[45] Mail Foreign Service, 'Pakistan introduces death penalty for cyber terrorism crimes which 'kill or harm national security'', The Daily Mail, November 6 2008, available at: {http://www.dailymail.co.uk/news/article-1083627/Pakistan-introduces-death-penalty-cyber-terrorism-crimes-kill-harm-national-security.html} accessed January 5 2016.

[Insert table 2 here]

Who are the cyberterrorists?

Within the 400 news items that concentrated on cyberterrorism as their primary or secondary focus, 219 articles offered specific representations of the identity of cyberterrorists. Five distinct identity types were present in our sample: hackers; hacktivists; professionals; unskilled; and, unspecified non-state actors.[46] When an item contained more than one of these representations,[47] each of these was analysed separately.

The first four of these representations are distinguished by the actor's skill level and/or motivation. *Hacker* referred to depictions of cyberterrorists as individuals who are likely to employ computer techniques to cause disruption and interference to a particular target, but who lack either the skill or motivation to cause serious levels of

[46] The application of these labels was part of an iterative process. Not every story that made reference to cyberterrorists as "hackers" explicitly described them thus. However, articles were categorised under this heading where otherwise similar language was used to those which did employ this label.

[47] See, for example, Christopher Joye, 'It's global cyber war out there', Australian Financial Review, 2 January 2013, available at: {http://www.afr.com/f/free/national/it_global_cyber_war_out_there_94da3CY7Avufi9jp5d0JTI} accessed January 5 2016.

damage to the most critical systems. Website defacement and Distributed Denial of Service Attacks (DDoS) are techniques that were often associated with this representation of cyberterrorists, as opposed to the writing and dissemination of complex malware, for instance. A good example of this may be identified in a 2009 story written for *The Independent* that covered a recent 'cyber terror blitz' and the likelihood that 'Russian hackers' were to blame for temporarily shutting down Twitter and causing major slowdowns to Facebook and Livejournal through the use of DDoS.[48]

Whilst the term hacker was used to refer to individuals, the term *hacktivist* refers to refer coverage of groups or their members which self-identify as collectives with a shared objective, such as Anonymous, AntiSec and LulzSec. A 2012 *Russia Today* article, for example, in which cyberterrorists were categorised as hacktivist reported on the group Anonymous under the heading "Protesters or Terrorists?".[49] *Professionals* referred to stories focused on individuals with sufficient levels of knowledge of complex computer techniques to be able to target the most critical systems. For example, in a story outlining how the U.S. is looking to protect itself against future

[48] Jerome Taylor, 'Russia blamed for cyber terror blitz', The Independent, August 8 2014, available at: {http://www.independent.co.uk/news/world/europe/russia-blamed-for-cyber-terror-blitz-1769187.html} accessed January 5 2016.

[49] 'Anonymous: Protesters or terrorists? Fog of cyberwar obscures truth', Russia Today, February 21 2012, available at: {http://rt.com/usa/anonymous-freedom-cyber-wall-875/} accessed January 5 2016.

cyber-attack through the development of a virtual 'cyber city', Leon E. Panetta asserts that malicious actors (including terrorists) can target vulnerabilities in critical infrastructure to create destruction comparable to the September 11th 2001 attacks.[50]

Unskilled referred to representations of individuals who employed either already-available scripts or publically available platforms and software to commit acts deemed "cyberterrorist" in this coverage. A 2011 BBC article, for example, reported on two Mexican individuals who had sent out phoney tweets alleging that shootings and kidnappings were taking place at a local school. The actions entailed no technical expertise, yet the use of this social networking platform in this way caused panic and accidents, and was later labelled "Twitter terrorism".[51] Given the manner in which both state and non-state actors were deemed capable of cyberterrorism in much of this media, a final category – unspecified *non-state actors* – acknowledged representations that said

[50] Robert O'Harrow Jr., 'CyberCity allows government hackers to train for attacks', The Washington Post, 26 November 2012, available at: {http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html} accessed January 5 2016.

[51] Julian Miglierini, 'Mexico 'Twitter terrorism' charges cause uproar', BBC News, September 6 2011, available at: {http://www.bbc.co.uk/news/world-latin-america-14800200} accessed January 5 2016.

little about an individual's skill or motivation but explicitly identified the purported cyberterrorist as entirely unaffiliated with a state.[52]

As table 3 demonstrates, the most common representation of cyberterrorists in our sample was as professionals (n=118), followed by hackers (n=77). For the three most common representations, table 2 also shows subtotals for whether the cyberterrorist was presented as a state or non-state actor. These subtotals show that, even when represented as professionals, cyberterrorists were more likely to be portrayed as non-state, than state, actors.

[Insert table 3 here]

Table 4 builds on this analysis by examining whether levels of concern intensified when cyberterrorists were represented in a particular way. For each representation of the cyberterrorist, it shows the proportion of stories that fell within the six categories used to measure concern introduced above.[53]

[52] Joseph S. Nye, 'Preventing a cyber Pearl Harbour', The Australian, April 19 2012, available at: {http://www.theaustralian.com.au/news/world/preventing-a-cyber-pearl-harbour/story-e6frg6ux-1226331846976#} accessed January 5 2016.

[53] Table 3 does not include the representation of cyberterrorists as purely hypothetical. The story containing this representation was categorised as balanced. Note also that since some items contained

[Insert table 4 here]

Four findings of note emerge from this analysis of news media representations of the identity of cyberterrorists. First, levels of concern were higher when items contained discernible representations of cyberterrorists. For those items which included an explicit representation of this threat's identity, 84% were either concerned or concerned with elements of scepticism. This figure was 19% lower for those items which contained no such representation. So, again, greater specificity was associated with higher levels of concern.

Second, in addition to specificity, *status* also had an important bearing on concern levels. Of the four representations based on an actor's level of skill and motivation (hacker/hacktivist/professional/unskilled), "Professionals" was not only the most common but also the one with the greatest levels of concern. 75% of the stories representing cyberterrorists as professionals were categorised as concerned, with a further 12% classed as concerned with elements of scepticism. Indeed, none of the items representing cyberterrorists thus displayed any level of scepticism. Perhaps more surprisingly, the "Unskilled" representation also had above-average levels of concern.

---

more than one representation of cyberterrorists, some items appear more than once in this table and so the figures in the total column do not tally exactly with the figures in chart 1.

As with "Professionals", 87% of the items which portrayed cyberterrorists as unskilled were classified as either concerned or concerned with elements of scepticism. Unlike the "Professionals" construction, however, a small number of items containing the unskilled representation were classified as sceptical (5%).

Third, the small number of items (n=7) which represented cyberterrorists as "Unspecified non-state actors" were all classified as concerned. These items were all characterised by an attempt to locate the concept of cyberterrorism in the context of a wider threat setting which included either offline terrorist (and in our sample, specifically, jihadist) groups[54] – most frequently Al Qaeda[55] – hostile states,[56] or past

[54] Richard Norton-Taylor, 'Cyberwarfare defence spending to rise despite cuts', The Guardian, October 17 2010, available at: {http://www.theguardian.com/politics/2010/oct/17/cyberwarfare-defence-spending-increase-cuts} accessed January 5 2016.

[55] Associated Press, 'Al-Qaida in decline, but threat to US multiply', Fox News, January 31 2012, available at: {http://www.foxnews.com/us/2012/01/31/al-qaida-in-decline-but-threats-to-us-multiply/} accessed January 5 2016; Associated Press, 'Federal web sites knocked out by cyber attack', Fox News, July 9 2009, available at: {http://www.foxnews.com/story/2009/07/08/federal-web-sites-knocked-out-by-cyber-attack/} accessed January 5 2016; Graeme Wilson, 'Al-Qaeda's cyber jihad on Facebook', July 13 2011, available at: {http://www.thesun.co.uk/sol/homepage/news/3691372/Al-Qaedas-cyber-jihad-on-Facebook.html} accessed January 5 2016.

[56] Associated Press, 'Al-Qaida in decline, but threat to US multiply'.

examples of cyberattacks, particularly Stuxnet.[57] Because of this wider concern, only one of these seven items had a primary focus on cyberterrorism.

Fourth, items representing hacktivists as cyberterrorists had the lowest levels of concern. Only two of the six items containing this representation were classified as concerned, each of which featured industry expert Eugene Kaspersky.[58] In a 2012 article by Lee Taylor in The Australian Telegraph, for instance, Kaspersky asserts that

[57] Gordon Crovitz, 'The U.S. draws a line in the silicon', The Wall Street journal, May 23 2011, available at: {http://online.wsj.com/news/articles/SB10001424052748704816604576335300155742190} accessed January 5 2016; Joseph S. Nye, 'Preventing a cyber Pearl Harbour', The Australian, April 19 2012, available at: {http://www.theaustralian.com.au/news/world/preventing-a-cyber-pearl-harbour/story-e6frg6ux-1226331846976#} accessed January 5 2016.; Daniel Fineren, 'Energy assets in front line of cyber war', Reuters, May 31 2012, available at: {http://www.reuters.com/article/2012/05/31/us-cyber-attacks-energy-idUSBRE84U15E20120531} accessed January 5 2016.

[58] The three articles categorised as "neither" were neutral pieces reporting on a hack of the Arizona Department of Public Safety and other law enforcement institutions. See: Anna Rhett Miller and Alta Spells, 'Cyberattackers grab more info on Arizona agency employees', CNN, June 20 2011, available at: {http://edition.cnn.com/2011/CRIME/06/29/arizona.hackers/} accessed January 5 2016; John D. Sutter and Phil Gast, 'Group says it hacked 70 U.S. law enforcement sites', CNN, August 7 2011, available at: {http://edition.cnn.com/2011/CRIME/08/06/hacking.websites/} accessed January 5 2016; Rava Richmond, 'Hackers release more data from Arizona police', The New York Times, June 29 2011, available at: {http://bits.blogs.nytimes.com/2011/06/29/hackers-release-more-data-from-arizona-police/} accessed January 5 2016.

cyberterrorism is a logical progression for the "leaders" of hacktivist collectives such as Anonymous:

> Most hacktivists – not all of them – are just following orders from the leaders, but many of these leaders are professional people and this is really dangerous…[T]hey can grow to the terrorist level.[59]

The other item, in the *Australian Financial Review*, reported on how the Australian Security Intelligence Organisation (ASIO) has monitored 'with mounting alarm' groups such as Anonymous which have 'targeted Western nations and companies with disruptive attacks that foreshadow an apocalyptic fusion between cyber-capabilities and terrorism'.[60] In marked contrast was an article from *Russia Today*, which made use of the same representation of hacktivists as cyberterrorists but was classified as sceptical

[59] Eugene Kaspersky, cited in Lee Taylor, 'Cyber warfare technology bill be used by terrorists', The Australian Telegraph, May 23 2012, available at: {http://www.dailytelegraph.com.au/technology/cyber-warfare-technology-will-be-used-by-terrorists-says-eugene-kaspersky/story-fn7bsi21-1226363625940} accessed January 5 2016.

[60] Christopher Joye, 'It's global cyber war out there', Financial Review, January 2 2013, available at: {http://www.afr.com/f/free/national/it_global_cyber_war_out_there_94da3CY7Avufi9jp5d0JTI} accessed January 5 2016.

with elements of concern.[61] Depicting a perceived American preoccupation with cyber-threats as a thinly veiled grab for greater executive power, military spending and curtailing of civil liberties, this item included the following quote from independent journalist J.A. Myerson on the relationship between hacktivist dissent and terrorism in the eyes of the U.S. Government: "There is a deep insinuation that dissent is somehow connected to or an accessary to terror. That's a really horrifying prospect".[62]

Who or what is threatened by cyberterrorism?

Within the news items with cyberterrorism as a primary or secondary focus, a wide variety of referents were identified as that threatened by this newest incarnation of terrorism. As chart 2 indicates, the most common of these referents by some distance was the state itself, followed by critical infrastructures and then the private sector.[63]

[Insert chart 2 here]

[61] 'Anonymous: Protesters or terrorists? Fog of cyberwar obscures truth', Russia Today, February 21 2012, available at: {http://rt.com/usa/anonymous-freedom-cyber-wall-875/} accessed January 5 2016.

[62] J. A. Myerson, cited in 'Anonymous: Protesters or terrorists?'

[63] Where an item mentioned more than one threat referent both were included. As a result the total number of threat referents is greater than the total number of news items.

Table 5 examines how levels of concern about cyberterrorism varied depending on the threat referent.

[Insert table 5 here]

Three points emerge from the data presented in chart 2 and table 5. First, where specificity was linked to higher levels of concern in relation to the focus of news coverage and representations of cyberterrorists, the *scale* of particular referents also appears significant in our sample, at least. All-but-one of the items which presented 'the West' or 'developed states' as the referent threatened by cyberterrorism were categorised as concerned (with the other classed as 'neither'). These items contained numerous bold assertions, including: "Power and water and other vital services in the West could be crippled";[64] "The fear is that modern nations are so dependent on technology that widespread interference with systems could wreak havoc";[65] and, "the

[64] Christopher Williams, 'Stuxnet virus 'could be adapted to attack the West'', The Telegraph, July 27 2011, available at: {http://www.telegraph.co.uk/technology/news/8665487/Stuxnet-virus-could-be-adapted-to-attack-the-West.html} accessed January 5 2016.

[65] Patience Wheatcroft, 'Cyberterrorism is now seen as a real threat', The Wall Street Journal, June 30 2010, available at: {http://www.wsj.com/news/articles/SB10001424052748704103904575336703726142746} accessed January 5 2016.

western world has, almost overnight, found itself incredibly vulnerable".[66] Of these ten items, five focussed on al Qaeda's call for "cyber jihad",[67] whilst the remainder juxtaposed the West to countries such as Russia, China, North Korea and Iran by referring to past events including Stuxnet and the cyberattacks on Estonia and Georgia in 2007 and 2008.[68] Similarly, all seventeen of the items which presented "the globe" as

[66] Dylan Welch, 'Cyber soldiers', The Sydney Morning Herald, October 9 2010, available at: {http://www.smh.com.au/technology/technology-news/cyber-soldiers-20101008-16c7e.html} accessed January 5 2016.

[67] Newscore, 'Terrorists to target social networking sites in 'cyber jihad' against the West', The Australian, July 13 2011, available at: {http://www.theaustralian.com.au/news/latest-news/terrorists-to-target-social-networking-sites-in-cyber-jihad-against-the-west/story-fn3dxity-1226094159319} accessed January 5 2016; Newscore, 'Al Qaeda's 'Cyber Jihad' to Target Social Networking Sites'; Graeme Wilson, 'Al-Qaeda's cyber jihad on Facebook', The Sun, July 13 2011, available at: {http://www.thesun.co.uk/sol/homepage/news/3691372/Al-Qaedas-cyber-jihad-on-Facebook.html} accessed January 5 2016; Rod Moran, 'Jihad waged on digital battlefield', The West Australian, November 15 2010, available at: {https://au.news.yahoo.com/thewest/news/a/10806192/jihad-waged-on-digital-battlefield/}; Newscore, 'Al-Qaida plotting 'cyber jihad'', The Telegraph, July 14 2011, available at: {http://www.dailytelegraph.com.au/al-qaida-plotting-cyber-jihad/story-fn6e1m7z-1226094225380} accessed January 5 2016.

[68] Christopher Williams, 'Stuxnet virus 'could be adapted to attack the West'', The Telegraph, July 27 2011, available at: {http://www.telegraph.co.uk/technology/news/8665487/Stuxnet-virus-could-be-adapted-to-attack-the-West.html} accessed January 5 2016; Patience Wheatcroft, 'Cyberterrorism is now seen as a real threat', The Wall Street Journal, June 30 2010, available at:

the referent of the cyberterrorism threat were either concerned or concerned with elements of scepticism. These included a 2012 article in *Russia Today* following the discovery of the Flame malware which quoted Eugene Kaspersky as saying "I'm afraid it will be the end of the world as we know it … I'm scared, believe me"[69] and a 2009 article in *The Guardian* which reported on research conducted by the International Commission on Nuclear Non-proliferation and Disarmament under the headline "Terrorists could use internet to launch nuclear attack".[70] A recurring theme in this

---

{http://www.wsj.com/news/articles/SB10001424052748704103904575336703726142746} accessed January 5 2016; Dylan Welch, 'Cyber soldiers', The Sydney Morning Herald, October 9 2010, available at: {http://www.smh.com.au/technology/technology-news/cyber-soldiers-20101008-16c7e.html} accessed January 5 2016; 'Warning over Iran terror virus war', The Sun, December 6 2011, available at: {http://www.thesun.co.uk/sol/homepage/news/3979922/Warning-over-Iran-terror-virus-war.html} accessed January 5 2016; Christopher Joye, 'It's global cyber war out there', The Australian Financial Review, January 2 2013, available at: {http://www.afr.com/f/free/national/it_global_cyber_war_out_there_94da3CY7Avufi9jp5d0JTI} accessed January 5 2016.

[69] N.A. ''End of the world as we know it': Kaspersky warns of cyber-terror apocalypse", Russia Today, June 6 2012, available at: {http://rt.com/news/kaspersky-fears-cyber-pandemic-170/} accessed January 5 2016.

[70] Bobbie Johnson, 'Terrorists could use internet to launch nuclear attack: report', The Guardian, July 24 2009, available at: {http://www.theguardian.com/technology/2009/jul/24/internet-cyber-attack-terrorists} accessed January 5 2016.

coverage was the importance of transnational dialogue and cooperation around cyber-security,[71] including the need for international cyber-security treaties.[72]

Second, it is noteworthy that concern levels were higher when the referent was the private sector (85%) or critical infrastructure (74%) than when the referent was nation states (70%) or citizens (57%). This resonates with other research which suggests that there may be qualitative differences between cyberterrorism and its parent concept, terrorism. Whilst the latter is traditionally understood as constituted by serious levels of

[71] Chandni Vatvani, 'Experts warn of cyberterrorism threat', Fox News, May 21 2008, available at: {http://www.foxnews.com/printer_friendly_wires/2008May21/0,4675,TechBitMalaysiaCyberterrorism,00.html} accessed January 5 2016; Tova Cohen and Maayan Lubell, 'Nations must talk to halt "cyber terrorism": Kaspersky', Reuters, Jun 6 2012, available at: {http://in.reuters.com/article/2012/06/06/net-us-cyberwar-flame-kaspersky-idINBRE8550HM20120606} accessed January 5 2016; N.A. 'International co-operation against computer crimes is a worldwide issue', Russia Today, April 21 2010, available at: {http://rt.com/politics/international-cooperation-computer-crimes} accessed January 5 2016; NewsCore, 'Security expert warns of cyber world war', Fox News, November 1 2011, available at: {http://www.foxnews.com/tech/2011/11/01/expert-at-london-internet-security-conference-warns-cyber-war.html} accessed January 5 2016.

[72] Lee Taylor, 'Cyber warfare technology will be used by terrorists'; Claudine Beaumont, 'Global 'internet treaty' proposed', The Australian Telegraph, September 20 2010, available at: {http://www.telegraph.co.uk/technology/internet/8013233/Global-internet-treaty-proposed.html} accessed January 5 2016.

violence against people or property, this may not be the case for cyberterrorism.[73] For example, a 2011 opinion piece on Fox News by Judith Miller – which reported on an outage within the Research In Motion (RIM) network on which BlackBerry smartphones rely – opened as follows:

> Did you open your BlackBerry Wednesday or even Thursday morning and find – nothing? No new e-mails, or tweets. No new text messages. Just blackness and that familiar screen saver photo of your child, spouse or dog? Welcome to the world of cyber-terrorism vulnerability

From this starting point, the piece went on to warn that cyberattacks "could not only cause billions of dollars in damage to such vital systems, but endanger national security" (notwithstanding the fact that RIM had attributed the outage to a core switch failure).[74] Similarly, in 2011 a Reuters technology article covered a Sony shareholders' meeting. The meeting took place in the aftermath of the cyberattacks on the company earlier that year, in which hackers accessed personal information on 77 million PlayStation Network and Qriocity accounts. The piece quotes Sony's CEO Sir Howard Stringer as saying:

---

[73] Lee Jarvis and Stuart Macdonald (see note 4 above).

[74] Judith Miller, 'Welcome to the world of cyber-terror vulnerability', Fox News, October 13 2011, available at: {http://www.foxnews.com/opinion/2011/10/13/welcome-to-world-cyber-terror-vulnerability/} accessed January 5 2016.

> We believe that we first became the subject of attack because we tried to protect our IP (intellectual property), our content, in this case videogames … I think you see that cyber terrorism is now a global force, affecting many more companies than just Sony[75]

Third, the referents that were associated with the lowest levels of concern were: data (61%); citizens (57%); and, institutions (such as NATO,[76] the New York Stock Exchange[77] and the Church of Scientology[78]) (44%). For all three of these, a significant proportion of news items were concerned with elements of scepticism (22%, 29% and 22% respectively). As well as the fact that concern about these threat referents was more likely to be tempered in this way, it is also telling that, of the eight categories of

[75] Edmund Klamann et al, 'Sony says protecting content made it hackers' target', Reuters, June 28 2011, available at: {http://www.foxbusiness.com/technology/2011/06/28/sony-says-protecting-content-made-it-hackers-target/} accessed January 5 2016.

[76] N.A 'NATO chief: climate change, energy supply threats', CNN, July 21 2009, available at: {http://edition.cnn.com/2009/WORLD/europe/07/21/nato.scheffer.security/index.html?iref=mpstoryvie} accessed January 5 2016.

[77] Heidi N. Moore, '5 things we still don't know about the market plunge', The Washington Post, May 16 2010, available at: {http://www.washingtonpost.com/wp-dyn/content/article/2010/05/15/AR2010051500041.html} accessed January 5 2016.

[78] N.A. 'Masked protest over scientology', BBC News, February 11 2008, available at: {http://news.bbc.co.uk/1/hi/england/london/7237862.stm} accessed January 5 2016.

referent, institutions and citizens were the two least common. Only nine items identified institutions as a potential target for cyberterrorism, and even fewer identified citizens as one (n=7).

Lastly, table 6 examines whether concern levels varied depending on whether the geographical focus of a news item was its country of publication.[79] In other words, did concern levels drop when news items covered threats focused on other countries?

[Insert table 6 here]

Two interesting findings emerge from this data. First, for those items whose geographical focus was the country of publication, the proportion classified as concerned was only slightly higher than the equivalent figure for items whose focus was a country other than the one of publication. So levels of concern did not appear to drop to any significant extent when an item focussed on another country. This suggests an apprehension of the transnational and boundary-less nature of cyber threats. Second, the proportion of items which had an international focus that exhibited concern (76%) was significantly higher than in the concerned coverage which focused on specific countries.

[79] Items focusing on two or more countries where one was also the country of publication were added to the column "Items whose geographical focus was the country of publication".

This is consistent with our earlier finding that, in terms of referent, levels of concern are linked to the perceived *scale* of the threat.

Specificity, status and scale: constructing the perfect storm

It will already be apparent from the preceding discussion that multiple constructions of cyberterrorism are present within news media discourse. Cyberterrorists may be represented as hackers, hacktivists, professionals or unskilled actors. They may be represented as state or non-state actors. And, in addition, a range of referents are possible, from the entire world at one extreme to individual citizens at the other. In short, there is no homogeneous construction of cyberterrorism. In addition, these competing constructions of cyberterrorism can be presented in different ways. They may be presented as part of a wider threat environment which also encompasses offline terrorist groups and/or other types of cyber threat, or they may form the primary focus of a particular news item.

The analysis hitherto has examined the links between these different constructions and levels of concern about the threat that cyberterrorism poses. Some constructions – such as those in which cyberterrorists are represented as hackers or hacktivists, and where the referent identified is data, citizens or institutions – are

associated with below average levels of concern.[80] Other constructions, in contrast, are associated with above average concern levels. Based on the earlier analysis, these include representations of cyberterrorists as professionals or unskilled actors; and, stories where the threat referent is the private sector, critical infrastructure, the West or the entire globe. Moreover, news items with an international focus and concentrating primarily on cyberterrorism also appear to demonstrate an exaggerated conception of the cyberterrorism threat.

Of the 535 news items examined in this study, a total of ten match this "perfect storm" model. Four features of these items are worthy of note. First, the items did indeed display above average levels of concern. Eight of the ten items were categorised as concerned, and a further one as concerned with elements of scepticism.[81] Second, only one of the ten items was published in a tabloid newspaper. Of the other nine, six were published by broadcasters (Reuters (x2), Russia Today (x2), Fox News, Russia Today) and three by broadsheet newspapers. Indeed, the five tabloid newspapers in our sample were responsible for just 31 of the 400 news items that had cyberterrorism as their primary or secondary focus (6.2 items per outlet) compared to 129 from

[80] An example is the Sky News article on the efforts to extradite Gary McKinnon to the US, which included the US authorities' claim that McKinnon was a cyberterrorist: Mark White, 'NASA 'Nerd' Hacker Fights Extradition to US', Sky News, June 9 2009, available at: {http://news.sky.com/story/700207/nasa-nerd-hacker-fights-extradition-to-us} accessed January 5 2016.

[81] The tenth was classified as balanced.

broadcasters (14.3 items per outlet) and 240 from broadsheet newspapers (14.1 items per outlet). This would seem to refute suggestions that the dominant news media discourse on cyberterrorism (if, indeed, there is one) is solely the product of tabloid hyperbole.[82]

The third striking feature of these ten items is their reliance on other sites of discourse. All-but-two of the items report on meetings between policymakers, industry and academics. Two focus on the 2012 Tel Aviv Cyber Security Conference.[83] Two focus on the 2011 London Cyber Conference.[84] The four others focus respectively on the 2010 Cybersecurity World Summit,[85] the 2013 DLD Conference in Munich,[86] a

[82] Lee Jarvis, Stuart Macdonald and Andrew Whiting, (2015).

[83] ''End of the world as we know it': Kaspersky warns of cyber-terror apocalypse', Russia Today, June 6 2012, available at: {http://rt.com/news/kaspersky-fears-cyber-pandemic-170/} accessed January 5 2016; Tova Cohen and Maayan Lubell, 'Nations must talk to halt "cyber terrorism": Kaspersky', Reuters, Jun 6 2012, available at: {http://in.reuters.com/article/2012/06/06/net-us-cyberwar-flame-kaspersky-idINBRE8550HM20120606} accessed January 5 2016.

[84] Sam Kelly, 'Web Security Expert Warns of Cyber World War', Sky News, November 1 2011, available at: {http://news.sky.com/story/895510/web-security-expert-warns-of-cyber-world-war} accessed January 5 2016; N.A. 'Experts warn of cyber warfare', Sky News, November 1 2011, available at: {http://news.sky.com/story/895540/expert-warns-of-cyber-warfare} accessed January 5 2016.

[85] Ewen MacAskill, 'Countries are risking cyber terrorism, security expert tells first world summit', The Guardian, May 5 2010, available at: {http://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity} accessed January 5 2016.

2008 security conference organised by RUSI[87] and a 2008 meeting of Government and technology experts in Malaysia.[88] With headlines such as "Experts warn of cyberterrorism threat",[89] "Countries are risking cyber terrorism, security expert tells first world summit"[90] and "Web security expert warns of cyber world war"[91], these eight items are (almost entirely) descriptive overviews of speeches delivered at these events with relatively little express commentary or opinion. The "experts" quoted in these items include the UK Prime Minister David Cameron, the Malaysian Prime Minister Abdullah Admad Badawi, an Estonian defense ministry official, the former Director of the Pentagon agency responsible for computer networks, the Director-General of the

---

[86] Jemima Kiss, 'Future cyber attacks could prove catastrophic, say online security experts', The Guardian, January 21, available at: {http://www.theguardian.com/technology/2013/jan/21/future-cyber-threats-catastrophic-dld-2013} accessed January 5 2016.

[87] Mark Trevelyan, 'Security experts split on 'cyberterrorism' threat', Reuters, April 17 2008, available at: {http://uk.reuters.com/assets/print?aid=UKL1692021220080417} accessed January 5 2016.

[88] Julia Zappei, 'Experts warn of cyberterrorism threat', Fox News, May 21 2008, available at: {http://www.foxnews.com/printer_friendly_wires/2008May21/0,4675,TechBitMalaysiaCyberterrorism,00.html} accessed January 5 2016.

[89] Julia Zappei, 'Experts warn of cyberterrorism threat'.

[90] Ewen MacAskill, 'Countries are risking cyber terrorism, security expert tells first world summit', The Guardian, May 5 2010, available at: {http://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity} accessed January 5 2016.

[91] Sam Kelly, 'Web Security Expert Warns of Cyber World War'.

French network and information security agency, a former US advisor to the White House on cybersecurity and the Chief Research Officer at F-Secure. Moreover, the two items which are not primarily descriptive accounts of a conference or meeting but are instead discussion-based pieces which purport to assess the magnitude of the cyberterrorism threat also draw heavily on the opinions of "experts", including the Head of the US Department of Homeland Security Michael Chertoff, the Director of Research Programs at the Australian Strategic Policy Institute Anthony Bergin and various academics.[92] By far the most prominent voice, however, is that of Eugene Kaspersky. With warnings such as "[W]e are close, very close, to cyber terrorism. Perhaps already the criminals have sold their skills to the terrorists – and then … oh, God",[93] Kaspersky is quoted in all five items published from 2011 onwards. Whilst none of this is to suggest that the process of selecting, summarising and collating these views is an entirely objective, impartial one, the discourse in these news items is clearly rooted in and derived from other discursive sites.

[92] Rod Moran, 'Jihad waged on digital battlefield', The West Australian, November 15 2010, available at: {https://au.news.yahoo.com/thewest/news/a/10806192/jihad-waged-on-digital-battlefield/} accessed January 5 2016; Tom Allard, 'In cyberspace they can't hear you scream', The Sydney Morning Herald, April 19 2008, available at: {http://www.smh.com.au/news/technology/in-cyberspace-they-cant-hear-you-scream/2008/04/18/1208025480226.html} accessed January 5 2016.

[93] Sam Kelly, 'Web Security Expert Warns of Cyber World War'.

It is noteworthy, finally, that six of these ten items also culminate in calls for greater international cooperation to enhance cybersecurity and deal with cyber threats. The use of hyperbole in these items may therefore – to some extent, at least – be understood as an attempt to overcome inertia or resistance via securitization of this issue. This raises clear questions for future research projects, including the motives of the different actors involved in this coverage.

Conclusion

The analysis of international news coverage presented in this article has attempted to offer two primary contributions to existing literature. The first was to add empirical depth to existing accounts of media representations of this threat, and the importance thereof. As outlined above, academic literature on cyberterrorism tends to simplify and generalise in one of two ways. In the first instance, 'concerned' assessments of the danger it poses typically construct cyberterrorism as a monolithic, unitary security threat, rarely disaggregating it. 'Sceptical' threat assessments, in contrast, assume an equally homogeneous media discourse on cyberterrorism that is characterised by hyperbolic representations of imminent, exceptional threat. As demonstrated by our findings, however, media discourse on cyberterrorism is actually surprisingly heterogeneous. It is characterised, *inter alia*, by: varying levels of anxiety, stretching from the concerned to the sceptical; different conceptions of the identity of would-be

cyberterrorists; variable levels of focus on this particular phenomenon, and therefore different contexts into which cyberterrorism is inserted; and, a range of distinct referents deemed threatened by cyberterrorism. As we have shown, although two thirds of the coverage in our sample of 31 outlets across a five year period was concerned by the threat of cyberterrorism, dissenting voices were also identifiable. Similarly, while cyberterrorism is most frequently identified as the behaviour of professional actors or hackers, the label is also applied to a range of other actors including hacktivist collectives and unskilled individuals. And, in terms of referents identified – or constructed – in this coverage, there is considerable diversity from imaginary geopolitical spaces ('the West') through to individual beings (ordinary citizens) and inanimate entities (such as data). As this suggests, there is not one (singular, monolithic) news media discourse on cyberterrorism: this coverage is profoundly multiple and diverse.

The article's second contribution was to add analytical depth to existing work on the content and framing of cyberterrorism discourse by highlighting the importance of three – hitherto neglected – factors within articulations of this threat. First, as demonstrated above, *specificity* matters, whereby news coverage that affords greater priority to cyberterrorism specifically tends toward a more exaggerated level of concern with the threat that it poses. Moreover, articles containing an explicit representation of 'cyberterrorists', in our sample, also demonstrate heightened levels of concern.

Secondly, our analysis also pulled attention to the importance of *status*, demonstrating that particular portrayals of cyberterrorist actors led to heightened levels of concern. Of particular note here, however, was the nature of this correlation and the discovery that the impact of status on levels of concern applied at two divergent points across the capability spectrum. International news coverage reported fearfully both on cyberterrorists deemed to be 'professionals' (with knowledge of how to target the most critical systems) and, conversely, on those deemed 'unskilled' (with no expertise at all and often a reliance on publically available software). Given the article's desire '…to study how representations of terrorism and their reality are socially produced through linguistic and non-linguistic practices'[94] the application of the label "cyberterrorist" within international news coverage both to those deemed capable of destruction comparable to that of the events of 9-11 and to those who send out hoax "Tweets" is of great significance for the construction of cyberterrorism knowledge.

And, third, we have also shown the significance of *scale* in this coverage, in that larger referents such as 'the West' or 'the globe' tend to attract greater anxiety than states or individual citizens. This relation is not, however, perfect, as the private sector and critical infrastructure also emerge as referents of particular concern throughout our sample. Although it might appear intuitive that larger referents would correlate with

[94] Jacob L. Stump and Priya Dixit, 'Toward a completely constructivist critical terrorism studies', International Relations, 26: 2 (2012), pp. 199-217, 210.

greater anxiety, there are at least two noteworthy aspects that can be drawn from this finding. First, the emphasis on larger referents such as these evidences a move away from the state as the primary referent within international media coverage of cyberterrorism. Given the traditional centrality of the state within terrorism discourse,[95] its scaling up in this instance to entire swathes of the globe is perhaps reflective of a broader anxiety toward threats against interconnected and potentially vulnerable systems. As characterised by Thomas Homer-Dixon:

> We've realised, belatedly, that our societies are wide-open for terrorists. We're easy prey because of two key trends: First, the growing technological capacity of small groups and individuals to destroy things and people; and second, the increasing vulnerability of our economic and technological systems to carefully aimed attacks[96]

Still on the point of status a second noteworthy aspect relates to the prevalence of larger referents and what Lene Hansen and Helen Nissenbaum write about 'everyday security

[95] Richard Jackson, Lee Jarvis, Jeroen Gunning, and Marie Breen Smyth, Terrorism: A Critical Introduction (Basingstoke: Palgrave, 2011).

[96] Thomas, Homer-Dixon, 'The rise of complex terrorism', Foreign Policy, January/February: 128 (2002), p. 53.

practices'.[97] This particular grammar of cyber security, according to Hansen and Nissenbaum:

> …points to the way in which securitizing actors, including private organizations and businesses, mobilize "normal" individuals' experiences in two ways: to secure the individual's partnership and compliance in protecting network security, and to make hypersecuritization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life[98]

Issues of cybersecurity are often more relatable to the experience of the general citizenry and this link has aided securitizing actors in their ability to successfully complete securitizing moves. With this in mind one may expect the international news media to 'move down' the scale of referent objects and produce more stories with personal data or privacy rights as that which is under threat. However, what this article has found is that, *contra* Hansen and Nissenbaum, the international news media, far from covering stories with more personally relatable referent objects, in fact more frequently do the opposite and scale up the referent.

[97] Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', International Studies Quarterly, 53:4 (2009), p. 1165.

[98] Lene Hansen and Helen Nissenbaum, 'Digital disaster', p. 1165.

Moving away from these analytical contributions, this article also sought to connect the burgeoning literature on cyberterrorism with its focus on issues of definition and threat to a more established body of scholarship on the construction and framing of terrorism (and, indeed, security) more broadly. In this context, it is of considerable interest to note that more specific representations of cyberterrorism tend to be associated with heightened levels of concern, given a widespread assumption that generalised and ambiguous discourses on terrorism serve (for some, deliberately) to exaggerate the threat that terrorism poses.[99] As Debrix argues, discourses on cyberterrorism are in fact complex and internally divided, and – as the above hopefully demonstrates - much might be learned by breaking these down into their constituent parts:

> Cyberterrorism is not an evanescent, chaotic threat, even though the media would like to convey this image of it to the public. On the contrary, the media themselves have organized cyberterrorism into categories, strategies, typologies, and methodologies which make it possible to talk about it (as a threat, a fear, a virtual danger) and to produce more knowledge about it (mostly, an anticipated sense of emergency and planning).[100]

[99] Saree Makdisi, 'Spectres of 'terrorism,' Interventions, 4:2 (2002), pp. 265-278; Katie Rose Guest, 'The Ideology of Terror: Why We Will Never Win the "War"', The Journal of American Culture, 28:4 (2005), pp. 368-376.

[100] Francois Debrix, 'Cyberterror and media-induced fears: the production of emergency culture', Strategies: Journal of Theory, Culture & Politics, 14:1 (2001), pp.149-168,158.

These three contributions leave us with a discourse that looks very different when observed along various different points of the "threat spectrum". Media discourse – in its entirety – is characterised, as shown above, by enormous diversity and heterogeneity. At the same time, however, when we turn attention to the most apprehensive accounts within international media discourse we find something far more uniform and stable. The 'perfect storm' constructions considered at the end of the article are notable not only for their representing the most apprehensive and cohesive part of this news media discourse. They also evidence considerable similarities of form, especially in relation to the citing of 'expert' knowledge from industry and beyond.

Ultimately this article has sought to contribute to understanding of how the threat of cyberterrorism has been constructed by the news media in a range of different countries across the world. It has sought to describe and unpack more and less hyperbolic constructions of cyberterrorism as an effort to render visible often-neglected heterogeneities therein. Future research could profitably build on this work via comparative analysis with other media providers and types, including non-English language sources and citizen journalism. Other timescales both before and subsequent to that covered in our analysis would make a particularly interesting comparison, too, allowing exploration of the importance of particular events in the framing of coverage on cyberterrorism. More work might be done on the reception of news media discourse

by different audiences, and on the specific rhetorical devices employed in news coverage, including the role of metaphors, analogies, intertextualities and the like; as well as the significance of images therein. Such research would build on this article's provision of a fuller and more detailed picture of the granularities of cyberterrorism discourse and the importance thereof.

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. We also gratefully acknowledge Jordan McErlean and Alicia Payne for their excellent research assistance, and David Mair and Lella Nouri-Bennett for their helpful suggestions throughout the project. Finally, we would like to thank the three anonymous reviewers who offered valuable comments on an earlier version of this article as well as to the editors of the European Journal of International Security.