Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage

by Lee Jarvis, Stuart Macdonald and Andrew Whiting

Abstract

This article examines the way in which the English language international news media has constructed the threat of cyberterrorism. Analysing 535 news items published by 31 different media outlets across 7 countries between 2008 and 2013, we show that this coverage is uneven in terms of its geographical and temporal distribution and that its tone is predominantly apprehensive. This article argues that, regardless of the 'reality' of the cyberterrorism threat, this coverage is important because it helps to constitute cyberterrorism as a security risk. Paying attention to this constitutive role of the news media, we suggest, opens up a fresh set of research questions in this context and a different theoretical approach to the study of cyberterrorism.

Keywords: Cyberterrorism; Media; News; Terrorism; Internet; Threat; Security; Insecurity; Stuxnet

Introduction

This article reports findings of a research project on media constructions of cyberterrorism. Examining a total of 535 English language items published in 31 different news outlets across 7 countries between 1 January 2008 and 8 June 2013, the project sought to examine a range of issues, including: the volume and tone of media coverage of cyberterrorism; the geographical and temporal spread of this coverage; the imagery used; the level at which the coverage was pitched (e.g., was background knowledge needed?); whether sources were quoted, and if so which; the portrayal of cyberterrorists (e.g., as professionals, hackers, etc.); whether the coverage made reference to past (cyber or non-cyber) events, and if so which; and, who or what is said to be threatened by cyberterrorism [1]. The aims of the research project were: first, to add empirical depth to conceptual accounts of the importance of media reportage within cyberterrorism discourse [2]; and, second, to explore the processes by which the term cyberterrorism is constructed and given meaning within the mainstream news media.

In this article – the first of three reporting our findings – our focus is the volume and tone of the media coverage, and its geographical and temporal distribution. The article will show unevenness in terms of both the temporal spread of the news items (with a marked increase in coverage from October 2010 onwards) and their geographical distribution (with a greater number of items published in UK outlets than those located within other countries). By contrast, our research identified far greater consistency in the *tone* of this coverage, with many more items manifesting concern over the cyberterrorism threat than scepticism toward it. The article concludes by arguing that, by demonstrating the role the news media plays in constructing a discourse that presents cyberterrorism as a security threat, our findings open up a range of fresh research questions in this area.

Cyberterrorism and the International News Media

Recent scholarship on cyberterrorism has focused largely on questions of definition, threat assessment and response [3]. Whilst each of these issues has generated diverse opinions, these debates share a common underlying assumption: that claims about cyberterrorism should be assessed or critiqued for the accuracy with which they reflect or represent reality. In this article we point to a different theoretical approach–one

which recognises that news media has a constitutive rather than correspondential relationship to the 'reality' of cyberterrorism. Instead of asking whether media coverage of cyberterrorism accurately reflects reality, our concern is instead to explore the role of the news media in constructing cyberterrorism as a real security threat.

Methodology

This project is the first systematic study of this size that focuses specifically on cyberterrorism [4]. The 31 news outlets examined in our research were of three sorts: broadsheet newspapers, tabloid newspapers and the websites of media corporations [5]. A key word search was conducted around the terms <cyber terrorism>, <cyberterrorism> and <cyber terror> for each news outlet, generating a total of 535 relevant items. These items included a wide and varied spread of content, ranging from news stories relating to current affairs in the country of origin or abroad, technology news and discussion thereof, opinion pieces and editorial reflections, items related to culture and the arts–including reviews of movies with fictional representations of cyberterrorism [6]–and special reports or other features using this terminology. While all of the news stories generated from this key word search referred explicitly to cyberterrorism, it was not uncommon for other elements of the cybersecurity lexicon – cyberwar, cyberespionage, cybercrime, etc. – also to be present. Where such examples are cited in this article, this is not meant to imply they are synonyms for cyberterrorism. Instead, this reflects the lack of clear distinction between said concepts and the flexible manner in which many of these media outlets employed such terms.

The study focused on items published between 1 January 2008 and 8 June 2013. These dates were selected for two reasons. First, because this provided sufficient data through which to explore developments in reportage on cyberterrorism: a total of 1986 days of media content. An second, because this period incorporated key events of potential relevance to cyberterrorism and media coverage thereof. These included the 2008 cyberattacks on Georgia, the 2010 revelations of the Stuxnet attack, the 2010 publication of the UK's *National Security Strategy*, and the November 2011 release of the UK's *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. The 31 news outlets were selected for this research for reasons of accessibility and pluralism. These included: the provision of a searchable online archive; diversity of political perspective and type of media company; diversity of geographical origin to facilitate comparison across and beyond the Anglosphere; and, reasons of language, such that the news content was provided in the medium of English.

Geographical Distribution of Coverage and Focus

News outlet	Total number of items that mentioned cyberterrorism
The Guardian	50
The Telegraph	43
Fox News	39
Reuters	28
BBC	26
The Washington Post	25
The Independent	24
Financial Times	23
Russia Today	22
The Australian	21
CNN	20
The Sun	20
The Times of India	20
Australian Telegraph	19
Australian Financial Review	18
The New York Times	16
China Daily	15
The Wall Street Journal	14
The Sydney Morning Herald	14
Daily Mail	12
The Straits Times	11
Channel 4 News	10
Aljazeera	10
Sky News	9
ABC News	8
LA Times	6
South China Morning Post	4
USA Today	3
Boston Globe	2
The West Australian	2
The Herald Sun	1
Total	535

Table 1: Number of News Items by News Outlet

Table 1 shows the total number of news items that appeared in each of the news outlets over the course of our research timeframe. As this indicates, there was significant variation in the coverage given to this topic by each of these outlets. The top eight on the list accounted for 258 of the 535 items (equivalent to 48% of the total). The bottom eight, in contrast, account for just 35 items (7%). Also significant is the geographical distribution across this period of time: of the top eight outlets, four were UK broadsheet newspapers and another was the British Broadcasting Corporation's (BBC's) online news site. The same trend is apparent in Table 2, which shows the

number of news items published in each of the US, UK and Australian newspapers in our sample. A total of 313 items appeared in these 18 newspapers (61% of the total). Of these, more than half were published in a UK newspaper (55%).

UK		Australia		US	
Newspaper	Total number of items	Newspaper	Total number of items	Newspaper	Total number of items
The Guardian	50	The Australian	21	The Washington Post	25
The Telegraph	43	Australian Telegraph	19	The New York Times	16
The Independent	24	Australian Financial Review	18	The Wall Street Journal	14
Financial Times	23	The Sydney Morning Herald	14	LA Times	6
The Sun	20	The West Australian	2	USA Today	3
Daily Mail	12	The Sun Herald	1	Boston Globe	2
Total	172	Total	75	Total	66

Table 2: Anglophone Newspaper Items by Country of Publication

The geographical focus of media coverage of cyberterrorism was as uneven in its distribution as in its origin. As Table 3 shows, more items focused on the US than any other country. Indeed, the number of items that focused on the US, UK and Australia was more than double the number concentrating on all other countries combined (353 compared to 174). Table 4 probes this unevenness further by asking what proportion of the news items focused on their country of publication. So, for example, all seven of the news items that focused on Singapore were published in the Singaporean *The Straits Times*. Similarly, only one of the 39 news items that focused on Australia was not published in Australia. Yet whilst 87% of the items that focused on the UK were published there, only 52% of the items that focused on the US were published in the US. And the majority of items relating to cyberterrorism that focused on China (69%) and Russia (83%) were not published in these countries.

US	170
UK	144
Australia	39
China	29
South Korea	28
India	21
Israel	18
North Korea	18
Iran	10
Singapore	7
Russia	6
Pakistan	5
Mexico	4
Europe	3
Japan	3
Estonia	2
Ireland	2
Middle East	2
Algeria	1
Georgia	1
Hong Kong	1
Indonesia	1
Morocco	1
Palestine	1
Saudi Arabia	1
Somalia	1
Spain	1
Zimbabwe	1
General international focus	56
No geographical focus	12

Table 3: News Items by Primary Geographical Focus

(Several news items within our sample had a strong focus on more than one country. Where this was the case both countries have been included)

	Total number of items primarily focused on this country	Percentage of these items that were published in this country
US	170	52%
UK	144	87%
Australia	39	97%
China	29	31%
India	21	86%
Singapore	7	100%
Russia	6	17%

Table 4: Geographical Focus of News Items by Country of Publication

Content Analysis: Focus and Apprehensiveness of News Coverage

Our analysis of the tone of the coverage across this diverse media content began by examining the extent to which each story focused specifically on cyberterrorism. A threefold classification was employed, with items categorised according to whether cyberterrorism was their primary focus, their secondary focus, or a topic mentioned in passing without any detailed discussion or analysis. As Chart 1 shows, a total of 83 items (16% of the dataset) had cyberterrorism as their primary focus, with a further 317 (59%) having it as their secondary focus. There were 135 items (25%) that mentioned cyberterrorism without examining the concept in detail.

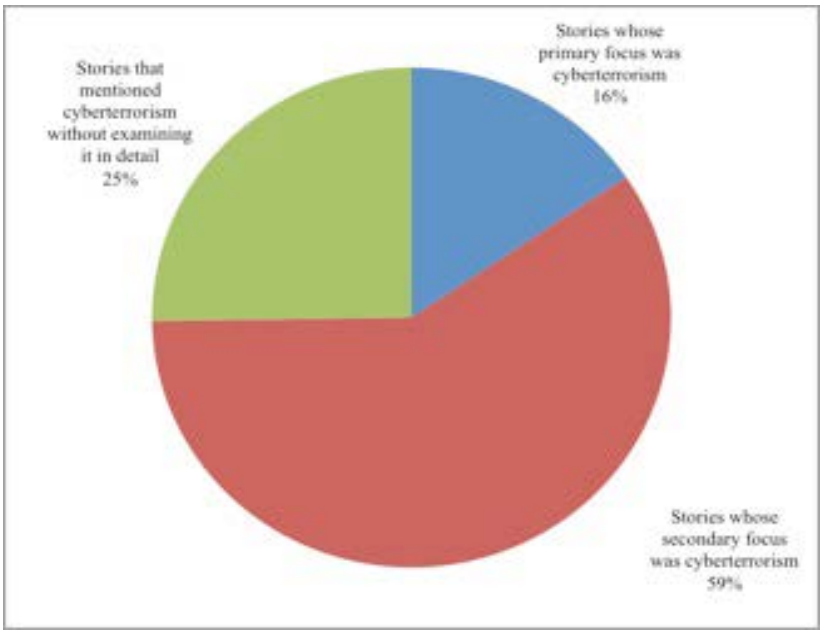

Chart 1: Proportion of News Stories with Cyberterrorism as their Primary or Secondary Focus

The next stage of the analysis concentrated on the 400 news items that had cyberterrorism as either their primary or secondary focus. Each story was coded and placed into one of the following six categories: concerned; concerned with elements of scepticism; balanced; sceptical; sceptical with elements of concern; or, neither (there were various reasons for placing a story in the last of these categories, such as the type of piece, with purely descriptive pieces not corresponding to any of the prior five categories).The results of this analysis are displayed in chart 2.

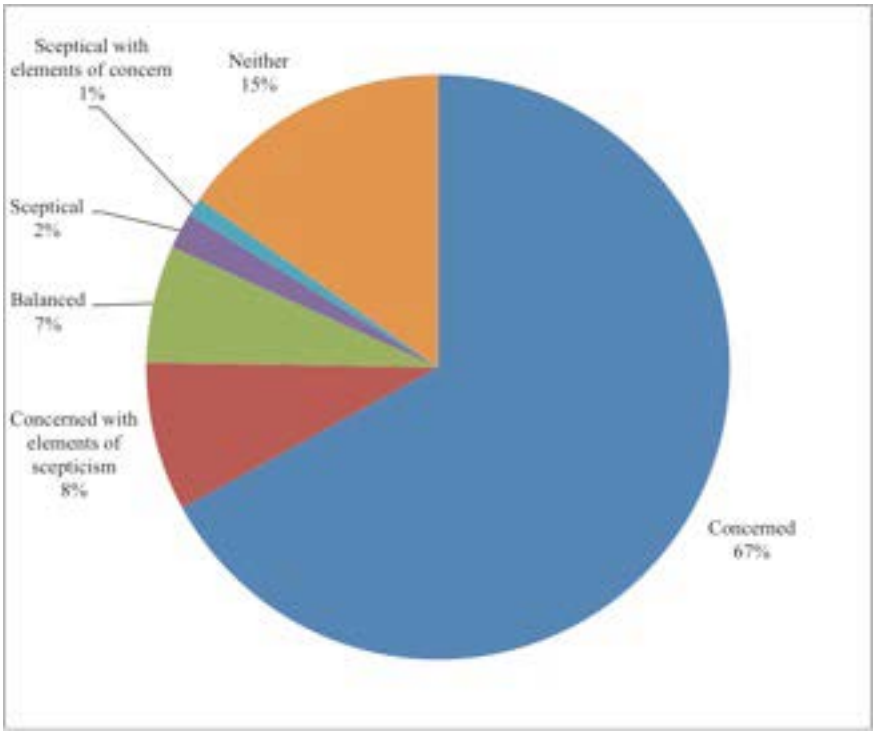

Chart 2: Proportion of News Stories that were Concerned, Sceptical, Balanced or Neither

A total of 268 news items – two-thirds of those with a primary or secondary focus on cyberterrorism – evidenced a marked concern with the threat posed by cyberterrorism. A further 33 items (8%) demonstrated concern with elements of scepticism: the second most fearful category within our schema. Equally striking are the small numbers of items that were sceptical about cyberterrorism posing any threat at all – only eight (or 2%) of the 400 analysed – sceptical with elements of concern (four in total; 1%) or balanced (26 in total; 7%). As this suggests, news coverage–at least within our sample–was predominantly apprehensive in tone throughout the five-year period on which we focused.

Table 5 investigates the tone of the news media coverage further by showing a breakdown of the items we explored by news outlet, by type of news outlet and by their origin in the Anglosphere or otherwise.

	Total number of news items which had cyberterrorism as a primary or secondary focus	Concerned	Concerned with elements of scepticism	Balanced	Sceptical	Sceptical with elements of concern	Neither
The Guardian	43	24 (56%)	9 (21%)	4 (9%)	3 (7%)	0	3 (7%)
Fox News	39	28 (72%)	1 (3%)	3 (8%)	0	0	7 (18%)
The Telegraph	30	21 (70%)	7 (23%)	1 (3%)	0	1 (3%)	0
The Washington Post	25	14 (56%)	0	0	1 (4%)	0	10 (40%)
BBC	23	15 (65%)	1 (4%)	2 (9%)	0	0	5 (22%)
The Independent	23	18 (78%)	0	0	0	0	5 (22%)
Financial Times	22	16 (73%)	0	1 (5%)	0	0	5 (23%)
CNN	20	9 (45%)	2 (10%)	2 (10%)	0	0	7 (35%)
The New York Times	16	7 (44%)	0	0	0	0	9 (56%)
The Australian	14	13 (93%)	1 (7%)	0	0	0	0
Russia Today	13	4 (31%)	2 (15%)	4 (31%)	0	2 (15%)	1 (8%)
The Wall Street Journal	13	10 (77%)	0	1 (8%)	1 (8%)	0	1 (8%)
Daily Mail	12	9 (75%)	1 (8%)	1 (8%)	0	0	1 (8%)

Reuters	11	8 (73%)	1 (9%)	1 (9%)	0	0	1 (9%)
The Sydney Morning Herald	11	5 (45%)	4 (36%)	2 (18%)	0	0	0
Australian Financial Review	10	9 (90%)	0	0	1 (10%)	0	0
The Sun	10	7 (70%)	1 (10%)	1 (10%)	0	0	1 (10%)
Channel 4 News	9	8 (89%)	1 (11%)	0	0	0	0
China Daily	9	6 (67%)	0	0	0	0	3 (33%)
The Straits Times	9	8 (89%)	0	1 (11%)	0	0	0
Australian Telegraph	8	8 (100%)	0	0	0	0	0
ABC News	6	3 (50%)	2 (33%)	1 (17%)	0	0	0
LA Times	6	4 (67%)	0	0	1 (17%)	0	1 (17%)
Sky News	5	4 (80%)	0	0	0	0	1 (20%)
The Times of India	4	4 (100%)	0	0	0	0	0
Aljazeera	3	1 (33%)	0	0	1 (33%)	1 (33%)	0
USA Today	3	2 (67%)	0	1 (33%)	0	0	0
Boston Globe	2	2 (100%)	0	0	0	0	0
The West Australian	1	1 (100%)	0	0	0	0	0
South China Morning Post	0	N/A	N/A	N/A	N/A	N/A	N/A
The Herald Sun	0	N/A	N/A	N/A	N/A	N/A	N/A

Tabloids	31	25 (81%)	2 (6%)	2 (6%)	0	0	2 (6%)
Broadsheets	240	163 (68%)	21 (9%)	11 (5%)	7 (3%)	1 (0%)	37 (15%)
News channels	129	80 (62%)	10 (8%)	13 (10%)	1 (1%)	3 (2%)	22 (17%)
Anglophone	362	245 (68%)	31 (9%)	21 (6%)	7 (2%)	1 (0%)	57 (16%)
Non-Anglophone	38	23 (61%)	2 (5%)	5 (13%)	1 (3%)	3 (8%)	4 (11%)
Overall total	400	268 (67%)	33 (8%)	26 (7%)	8 (2%)	4 (1%)	61 (15%)

Table 5: Concerned, Sceptical, Balanced or Neither, by News Outlet

A number of interesting points arise from this data. First, the five tabloid newspapers included in the sample were responsible for just 31 of the items identified in our research: a very modest average of 6.2 items per outlet over this period. This compares to averages of 14.1 items per broadsheet newspaper and 14.3 items per broadcaster. This indicates that if there is a dominant news media discourse on cyberterrorism it is not solely the product of tabloid hyperbole. At the same time, however, whilst the predominant tone of the entire sample was apprehensive, this tone was particularly acute in the tabloid newspapers. Of their 31 items, 25 (81%) were concerned and a further two (6%) were concerned with elements of scepticism. Moreover, none of the 31 tabloid items was sceptical or sceptical with elements of concern. Third, the proportion of items that were classified as concerned or concerned with elements of scepticism was lower for the broadcasters than for the broadsheet newspapers. In total, 70% of the items from broadcasters fell into one of these two categories, compared to 77% of those from the broadsheets. Moreover, the broadcasters had a higher proportion of balanced items (10%, compared to 6% for the tabloids and 5% for the broadsheets). Fourth, the non-Anglophone sources had a lower proportion of items that were concerned or concerned with elements of scepticism (66% in total), a higher proportion of items that were balanced (13%) and a higher proportion that were sceptical or sceptical with elements of concern about the threat posed by cyberterrorism (11%). The cumulative import of these findings is that Anglophone newspapers – particularly tabloids but broadsheets too – tended to strike a more apprehensive tone than broadcasters and non-Anglophone sources.

Chronological Analysis

Moving on to the temporal spread of the dataset, Chart 3 shows the number of news items that were published each month, from January 2008 to June 2013. As the chart shows, a far greater number of items were published in October 2010 (35 in total) than in any of the other months covered by our study. There were two factors that contributed to this large number of items. The first was the release of the UK's National Security Strategy on 18 October 2010, which identified international terrorism and cyberattack as two of the top tier threats facing the UK [7]. This was accompanied by the associated decision to invest an additional

£650m in cybersecurity at a time when cuts where being made to other aspects of the defence budget in the name of austerity. These developments generated a total of 22 news items mentioning cyberterrorism from 17-20 October 2010. As Table 6 shows, although most of these were published in the UK (17, 77%), there was also some media coverage from the US and Australia.

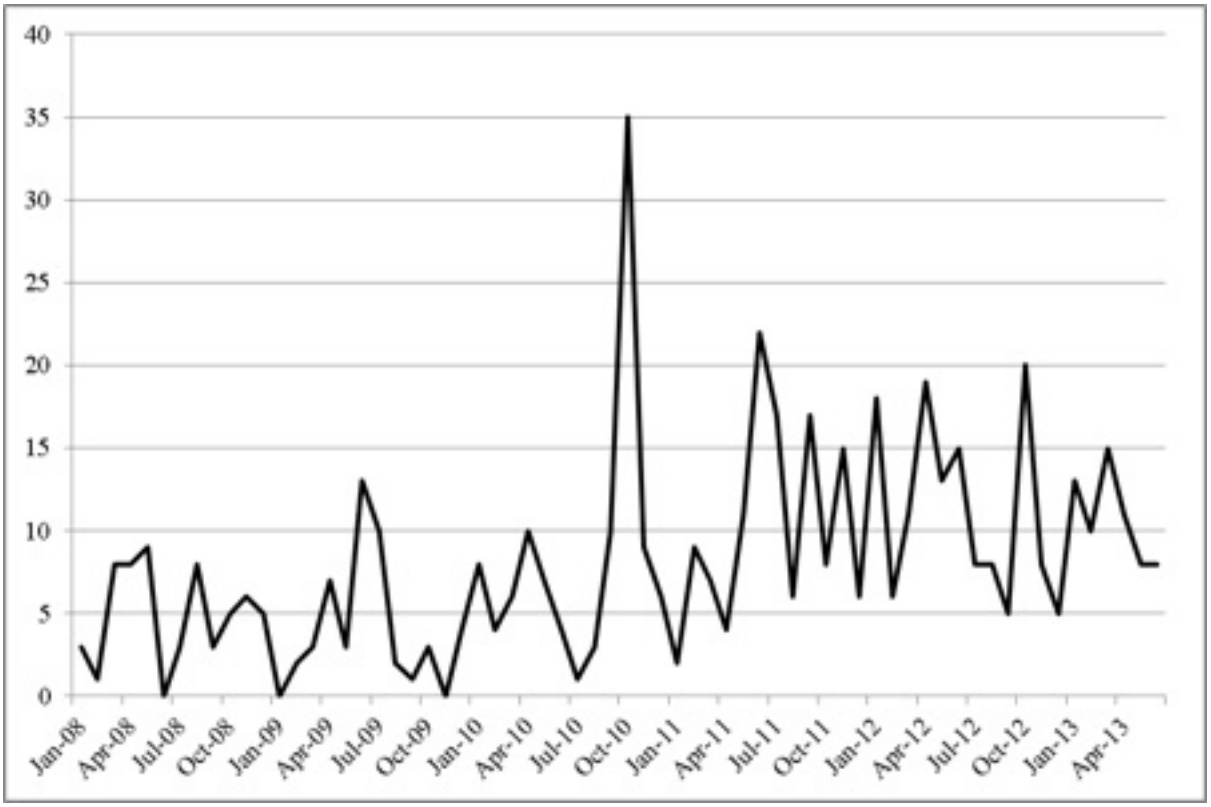

Chart 3: Number of News Items, by Month of Publication

Channel 4 News	4
The Telegraph	4
The Guardian	3
Aljazeera	2
Daily Mail	2
The Sun	2
ABC News	1
BBC	1
Fox News	1
The Independent	1
The Wall Street Journal	1
Total	22

Table 6: News Items 17-20 October 2010, by News Outlet

The general tone of these items is also significant. As Table 7 shows, of the 16 that discussed cyberterrorism in sufficient detail to enable classification within October 2010, none demonstrated a sceptical or balanced view of the threat posed by this phenomenon. On the contrary, a total of 13 items (81%) were classified as concerned and a further 2 (13%) as concerned with elements of scepticism. In fact, the tone of some of this coverage was dramatic. One headline published in the UK's most widely read newspaper warned of the need to, 'Fight

cyber war before planes fall out of sky' [8]. Another–headlined, 'Why Britain is desperately vulnerable to cyber terror'–presented a detailed description of a digital 'Pearl Harbour' in which:

> *Power cuts scythed through Britain, plunging cities into darkness … The nationwide panic meant supermarket shelves emptied and petrol stations ran out of fuel … There was no TV, no radio and no mobile networks. After a fortnight, there were riots, and the military, which was itself crippled by mysterious communications glitches, was called in [9]*

This was followed by the foreboding statement that 'This terrifying scenario may seem like a science fiction movie. But it is exactly the sort of possibility currently being considered at the highest levels in government as part of the National Security Strategy' [10].

	Number of news items
Concerned	13
Concerned with elements of scepticism	2
Balanced	0
Sceptical	0
Sceptical with elements of concern	0
Neither	1
Did not discuss cyberterrorism in detail	6
Total	22

Table 7: News Items 17-20 October 2010, by Concerned, Sceptical, Balanced or Neither

The second factor that contributed to the large number of items mentioning cyberterrorism in October 2010 was the revelations concerning Stuxnet. Stuxnet is of particular importance as one of the first known malwares to cause physical damage to critical infrastructure [11]. Allegedly developed by the CIA in cooperation with the Israeli Government, Idaho National Laboratory and other US agencies [12], it was introduced to the Natanz Uranium Enrichment Plan in Iran by USB flash drive causing 1000 centrifuges to fail. The first mention of Stuxnet in the 31 news outlets in our study came on 23 September 2010 in a piece published in the UK's *Financial Times*, headlined 'Warning over malicious computer worm'. In October 2010 there were a total of 11 news items that specifically mentioned this attack. As with coverage of the UK's National Security Strategy, discussion of Stuxnet was also characterised by considerable apprehensiveness of tone. A story on 1 October–headlined 'Security: A code explodes'–warned that Stuxnet had taken worries about cyber warfare to a different plane. The image accompanying this story was a picture of a grenade [13]. Three days later the same newspaper warned that comparing the cyber threat to the nuclear arms race was, if anything, 'a little too comforting' [14]. The story continued, this was because 'Anyone can play at cyber warfare. The tools can be bought on a local high street and the command-and-control bunker can be a spare bedroom' [15]. This time the accompanying image was a picture of three military tanks resembling computer mice.

During the same period, another newspaper published in Australia stated that half of all companies running critical infrastructure systems have reported politically motivated cyberattacks, adding, 'A global survey of such attacks – rarely acknowledged in public because of their potential to cause alarm – found companies estimated they had suffered an average of 10 instances of cyber war or cyber terrorism in the past five years at a cost of US $850,000…a company' [16]. Two days later this newspaper also quoted Eugene Kaspersky, who described Stuxnet as a 'turning point', arguing 'I am afraid this is the beginning of a new world' [17]. The *South China Morning Post*, meanwhile, even lamented the fact that 'Unlike Britain and the United States, neither the mainland nor Hong Kong has an established multi-agency government structure that could co-ordinate various agencies to react quickly to cyber terrorism' [18]. In fact, the first news item in our sample

that specifically mentioned Stuxnet and was classified as balanced was not published until June 2011: a story by the UK's BBC on the possible 'hacking' of the International Monetary Fund [19]. Up to that point, a total of 21 items had mentioned the attack in Iran, all of which were concerned (18 items) or concerned with elements of scepticism (3 items) about the threat posed by cyberterrorism.

While there were far more news items that mentioned cyberterrorism in October 2010 than any other month in the period of our study, the events reported during this month had a lasting impact on news media coverage of cyberterrorism. The change is twofold. First, as Chart 3 shows, following October 2010 there was a marked increase in the general level of items mentioning cyberterrorism. In the 33 months prior to October 2010 there was an average of 4.8 items per month. This more than doubled in the 32 months that followed, during which there was an average of 10.6 items per month. Second, in the period following October 2010 there was a marked increase in the number of news items published that demonstrated a concern with the threat of cyberterrorism. This is shown in Chart 4.

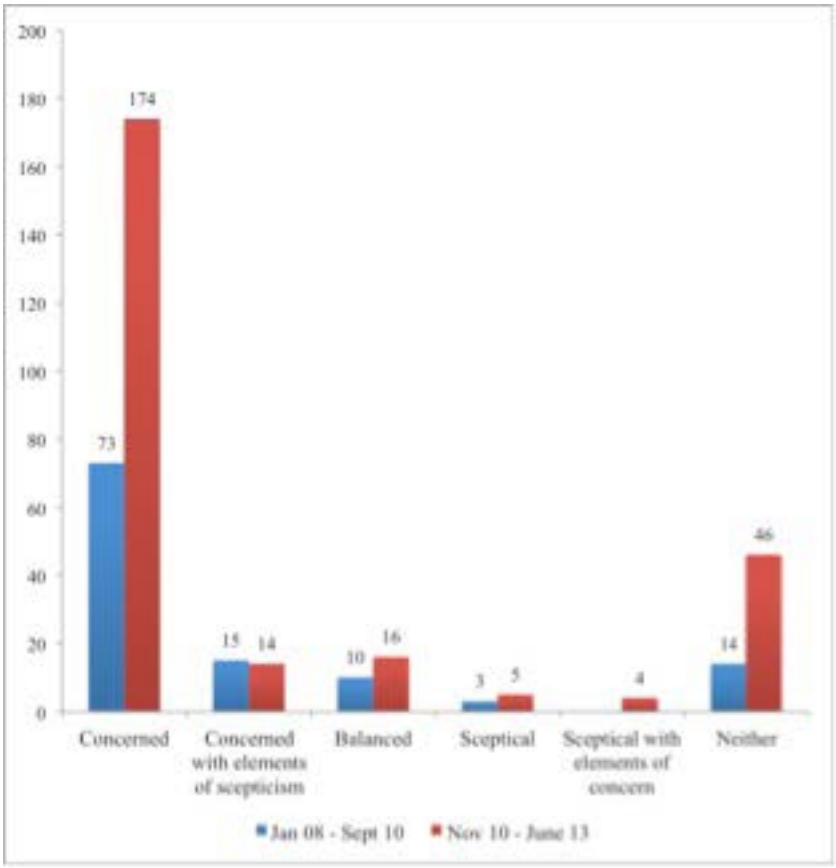

Chart 4: Number of Concerned, Sceptical, Balanced and Neither News Items before and after October 2010

As Chart 4 demonstrates, in the 33 months prior to October 2010 there were a total of 73 items that were concerned, an average of 2.2 per month. By contrast, in the 32 months that followed there were a total of 174 items that were concerned, an average of 5.4 per month.

Conclusion

The above discussion sketches some of the key developments within the coverage–or construction–of cyberterrorism and its threat in the English language international news media between 2008 and 2013. Two broad findings of importance to contemporary discussions of cyberterrorism emerge from this research. The first finding is that–in purely quantitative terms–there is a considerable amount of international media content

that focuses on cyberterrorism: a phenomenon that some (although not all) academic researchers argue has yet to occur [20]. In the deliberately narrow parameters of our research–whereby some variant of <cyber> and <terrorism> or <terror> had to be present in the story for its inclusion in our sample–an average of one story making reference to cyberterrorism was published every 3.7 days. As we have seen, the distribution of this coverage was far from uniform and many of the items we explored only mentioned cyberterrorism in passing. That said, this clearly evidences a significant amount of media interest in this new form of terrorism.

The second core finding is that much of the media coverage considered in our research expresses real concern over the current or future threat posed by this phenomenon. This concern contrasts with some of the more sceptical academic perspectives which frequently question whether would-be cyberterrorists have the means, motive or opportunity to engage in this type of activity [21]. It does, however, correspond rather more closely to a recent survey of researchers working on this topic in which 70% of those surveyed stated that cyberterrorism either does constitute, or potentially constitutes, 'a significant threat' [22]. This is important, we argue, because news coverage has a constitutive rather than corresponding relationship to the 'reality' of cyberterrorism: it is actively involved in the production of this potential security threat. Danger, as David Campbell wrote, 'is not an objective condition' [23]. It is a product of framing and interpretation, in which meaning is given to the world via language, images and other discursive practices: be they pictures of hand grenades, discussion of hypothetical 'doomsday' scenarios, or headlines about 'malicious computer worms'. Thus, whether or not there exists a 'real' threat of cyberterrorism (if such a question could ever, even, be answered), media (and other) depictions thereof are important in their own right. This is, not least, because when they become widely circulated and reproduced, dominant narratives of threat–around cyberterrorism, and, indeed, anything else–can, very quickly, take on the appearance of, 'an external "reality" which seems to confirm it as truth and commonsense' [24].

In our future research we will seek to build on the analysis presented here by exploring more specific aspects of findings from this project. This will include: first, looking at the voices of authority cited in news coverage of cyberterrorism in order to ask who is seen to speak the 'truth' about this threat and how such voices work to augment or mitigate it. Second, investigating how the figure of the 'cyberterrorist' is represented, and what types of target cyberterrorists are seen to threaten. And, third, looking at the use of historical and other metaphors in media attempts to make sense of this security challenge and how these connect to visual images in this coverage. Our hope in this article, however, is that by charting some of the ways in which English language news media has constructed cyberterrorism as a security threat we have demonstrated the importance of such a research agenda.

About the Authors:

Lee Jarvis *is Senior Lecturer in International Security at the University of East Anglia (UEA) and Director of the UEA's Critical Global Politics research group. His recent books include Counter-Radicalisation: Critical Perspectives (Routledge, 2015, edited with Christopher Baker-Beall and Charlotte Heath-Kelly); Critical Perspectives on Counter-terrorism (Routledge, 2015, edited with Michael Lister) and Security: A Critical Introduction (Palgrave, 2015, with Jack Holland).*

Stuart Macdonald *is Associate Professor in Law and Deputy Director of the Centre for Criminal Justice and Criminology at Swansea University. He is co-editor of* Cyberterrorism: Understanding, Assessment and Response *(New York: Springer, 2014) (with Lee Jarvis and Thomas Chen). His recent project on security and liberty was funded by the British Academy. He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney.*

Andrew Whiting *lectures in the Department of Criminology at Swansea University. He is currently completing his PhD which investigates the construction of cyberterrorism within Internet security industry discourse. Since undertaking his doctorate has had his work published on a range of topics that reflect his research interests including terrorism, cyberterrorism and radicalisation.*

Acknowledgments

We would like to thank Swansea University's College of Law and the Bridging The Gaps programme for their support for the research upon which this article is based. We 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.

Notes

[1] Chen, T., Jarvis, L., Macdonald, S. and Whiting, A. (2014). *Cyberterrorism and the News Media*. Cyberterrorism Project Research Report (No. 3). Available via: www.cyberterrorism-project.org.

[2] See, amongst others, Conway, M. (2008) 'The Media and Cyberterrorism: A Study in the Construction of 'Reality''. Available online at http://doras.dcu.ie/2142/1/2008–5.pdf (accessed 16 May 2013); Weimann, G. (2004) 'Cyberterrorism: How Real is the Threat?' United States Institute of Peace Special Report 119. Available at http://www.usip.org/publications/cyberterrorism-howreal-threat (accessed 15 May 2013); Stohl, M. (2006) '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): 223-238.

[3] Examples include Chen, T., Jarvis, L & Macdonald, S. (Eds.) (2014) *Cyberterrorism: Understanding, Assessment and Response*. New York: Springer; Jarvis, L., Macdonald, S. & Nouri, L. (2014) 'The Cyberterrorism Threat: Findings from a Survey of Researchers' *Studies in Conflict and Terrorism* 37(1): 68-90; Jarvis, L. & Macdonald, S. (2014) 'What is Cyberterrorism? Findings from a Survey of Researchers'. *Terrorism and Political Violence*. Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2013.847827 (last accessed 21 November 2014).

[4] The study by Bowman-Grieve examined a selection of 100 Anglo-American media sources published between 1996 and 2013, using the concept of moral panics: Bowman-Grieve, L. (2015) 'Cyber-terrorism and Moral Panics: A reflection on the discourse of cyberterrorism', in T. Chen, L. Jarvis & S. Macdonald (Eds.) *Terrorism Online: Politics, Law and Technology*. Abingdon: Routledge.

[5] The 31 sources selected were: ABC News, Al Jazeera, 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.

[6] For instance, cyberterrorism featured prominently in discussion and reviews on the twenty-third film in the James Bond franchise–Skyfall–that was released in cinemas internationally at the end of 2012.

[7] HM Government (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy* Cm 7953.

[8] *The Sun*, 19 October 2010.

[9] *Daily Mail*, 19 October 2010.

[10] *Daily Mail*, 19 October 2010.

[11] Farwell, J. P. & Rohozinski, R. (2011). 'Stuxnet and the Future of Cyber War'. *Survival* 53(1), pp. 23-40; Langner, R. (2013) *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington: The Langner Group.

[12] Gorman, S. (2012). 'US Team and Israel Developed Iran Worm'. *Wall Street Journal*, 1 June 2012.

[13] *Financial Times*, 1 October 2010.

[14] *Financial Times*, 4 October 2010.

[15] *Financial Times*, 4 October 2010.

[16] *Sydney Morning Herald*, 7 October 2010.

[17] *Sydney Morning Herald*, 9 October 2010.

[18] *South China Morning Post*, 1 October 2010.

[19] *BBC News*, 13 June 2011.

[20] Conway, M. (2004) 'Cyberterrorism: media myth or clear and present danger?', in: Irwin, J (Ed.) *War and virtual war: the challenges to communities*. Amsterdam: Rodopi, pp. 79–95.

[21] Conway, M. (2014) 'Reality check: assessing the (un)likelihood of cyberterrorism' in Chen T, Jarvis L, Macdonald S (Eds.) *Cyberterrorism: Understanding, Assessment and Response*. New York, NY: Springer; Denning, D. (2012) 'Stuxnet: What Has Changed?', *Future Internet*, 4(3). Available online via http://www.mdpi.com/1999-5903/4/3/672/pdf, (accessed 24/06/2014); Giacomello, G. (2004) 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism', *Studies in Conflict and Terrorism* 27(5): 387–388; Lewis, J. A. (2002) 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', *Center for Strategic and International Studies*, Available online via

http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (accessed 24/06/2014).

[22] Macdonald, S., Jarvis, L., Chen, T., and Lavis, S. (2013) *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1). Available online via: www.cyberterrorism- project.org.

[23] Campbell, D. (1998) *Writing Security: United States Foreign Policy and the Politics of Identity* (Revised Edition). Manchester: University Press, 1.

[24] Jackson, R., Jarvis, L., Gunning, J. and Breen Smyth, M. (2011) *Terrorism: A Critical Introduction*. Basingstoke: Palgrave, 144.