Framing Cyberterrorism: A Content Analysis of The New York Times

Norshahida Noor Zeri[1]
Noor Nirwandy Mat Noordin[2]

Centre for Media and Information Warfare Studies
Faculty of Communication and Media Studies
Universiti Teknologi MARA (UiTM)
40450 Shah Alam, Selangor, Malaysia

[1]hshahida.zeri@gmail.com
[2]nirwandy3493@salam.uitm.edu.my

Received Date: 20/2/2017 Accepted Date:30/5/2017 Published Date: 27/6/2017

ABSTRACT

The threat posed by cyberterrorism has grabbed the attention of the mass media. Concerned assessments of the cyberterrorism threat highlight infrastructural and sociopolitical vulnerabilities at risk of exploitation by appropriately resourced and intentioned actors. Approached thus, combined with figurative language within the framing of this threat cyberterrorism, emerges as a relatively straightforward danger of potentially catastrophic significance. This study aims to identify news related to cyberterrorism in The New York Times; to investigate issues highlighted which the term cyberterrorism is constructed; and, to determine types of cyberterrorism threats reported by the news media. This study applies quantitative content

ISSN 1985-563X

analysis method by using descriptive research design. A distinguishing characteristic of content analysis is its quantitative aspect. Quantitative content analysis consists of tabulating the occurrences of content units. Content analysis aims at statistical formulations, directed toward empirical problems and its statistical character is one of its most distinctive attributes. This study sketches some of the key developments within the coverage–or construction–of cyberterrorism and its threat in the New York limtedTimes between 2010 and 2016. This study believed that news framing of cyberterrorism issue was reasonably had shaped concerned thoughts amongst Americans and formed varying levels of anxiety, stretching from the concerned to the sceptical; different conceptions of the identity of would-be cyberterrorists.

Keywords: *News Framing, Cyberterrorism, Threats, Cyberterrorist, Content Analysis*

1.0 INTRODUCTION

Integral infrastructure systems such as power stations, hospitals, air traffic control networks, for example, heavily relies on computing devices nowadays. Therefore, a large portion of our infrastructure becomes susceptible to cyberterrorism attacks. Instead of directly targeting to ultimately harm the physical system, in a cyber attack, the attacker instead attempts to imperil the crucial computing devices to either indirectly seize control over the system, or acquire the ability to disrupt system operations.

Given that computing networks are increasingly confederated in interconnected systems, attackers further acquire the ability to deploy cyber-attacks remotely, without ever physically accessing any of the targeted infrastructure. Illustrations of computer viruses or worms, such as Stuxnet or Flame, that have substantially disrupted critical functions signify that the threat of cyber-attacks is not only real but that the consequences of carefully coordinated cyberterrorist attacks by hostile parties can be severe. The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach

targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure [1].

The threat posed by cyberterrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry [1]. Journalists, politicians, and experts in various fields constantly warns about an event in which sophisticated cyberterrorists electronically break into networks that control dams or air traffic control systems, bring about havoc and endangering not only millions of lives but national security itself.

Potential impetuous cyberterrorist attack enjoy periodic emergence within the global news media. A 2013 article in *The Washington Post,* for example, asked 'Is the U.S. Prepared for Cyberterrorism?' [2]; returning to subjects raised by Fox News two years earlier:'10 Years After 9/11, Are America's Cyberdefenses Weaker?' [3]. The UK's Daily Mail reported related concerns in light of an accessive reliance on cyber-technology, inside the British national security architecture: 'Cyber terrorists could inflict 'fatal' attack on Britain because Armed Forces rely so heavily on computers, MPs warn' [4]. Meanwhile, also in 2010, *The Australian* similarly cautioned: 'Cyber terrorism threat 'not taken seriously enough'' [5].

Headlines such as these demonstrate a widespread solicitude with the danger postured by cyberterrorism to various referents. In reality, as few authors have contended, the news media has been one of the most eminent sites in which this danger has been securitized. Gabriel Weimann in 2004, for example, connotes that, 'much of the discussion of cyberterrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms'. In addition, Maura Conway in 2008 [6], alludes that with 'the add of the mass media, cyberterrorism came to be viewed as the "new"security threat *par excellence'*.

In some ways, it is strange that print, broadcast and different types of journalism are every now and again blamed for overstating dangers. Endless attempts and endeavors at securitizing cyberterrorism are particularly interesting, nonetheless, however, is that they operate in the absence of two conditions that might increase their plausibility: (i) some measure of scholastic consensus that cyberterrorism does in fact represent a critical security risk and (ii), certain form of substantiating factual evidence.

1.1 Problem Statement

In spite of the fact that cyberterrorism shows recent addition to our security imaginaries, an expanding scholastic writing has now started to rise around this phenomenon. Concerned assessments of the cyberterrorism threat highlight infrastructural and sociopolitical vulnerabilities at risk of exploitation by appropriately resourced and intentioned actors. Approached thus, combined with figurative language within the framing of this threat cyberterrorism, emerges as a relatively straightforward danger of potentially catastrophic significance [7].

As with terrorism discourse more broadly [8], metaphors were employed to make sense of cyberterrorism work to (re)produce that to which they appear to refer, often with tangible discursive and political implications. According to Steuter and Wills [9], words are chosed from within a dominant system or frame of metaphor that offers a specific lexicon of language, that defines words in certain specific ways, and shapes both the 'what' and the 'how' of our communication. The most common metaphors helps to understand problems and conflicts in certain ways, offering certain available responses, and negating or obscuring others.

On the other hand, there exists a number of very different understandings of cyberterrorism within academic and other literature on this concept. Several authors, for instance, prefer a graduated approach, distinguishing between 'pure' and other types of cyberterrorism. In these cases, the former is often used most sparingly to refer only to attacks on digital targets via digital means, while the latter, in contrast, may incorporate activities such as propagandizing or fundraising online [10]; [11].

Cyberterrorism, in other words, might be thought of as a social construction rather than an extra-discursive reality: its existence is a product of meaning-making practices associated, variously, with political rhetoric, popular culture, cyber-security corporations, or the news media [6]. As Francois Debrix [12] argues, the language of cyberterrorism mobilized by the media and its so-called experts is quite technical . 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.

This study is aimed to study how cyberterrrorism is framed and constructed in news media by which The New York Times were chosen accordingly. Furthermore, studies on New York Times'coverage on cyberterrorism has been limited.

2.0 REVIEW OF LITERATURE

Literature review section provides a brief general idea and indication of numerous literature and keywords pertaining to the study of agenda-setting and news framing of cyberterrorism. This section particularly discusses several aspects that are related to the study. They are (i) Framing Theory, and; (ii) Priming.

2.1 Theory of Framing

In social theory, a 'frame' consists of a schema of interpretation, collection of anecdotes, and stereotypes that individuals rely on to understand and respond to events [13]. In communication, framing defines how news media coverage can shape mass opinion by using these specific frameworks to help guide their reader to understanding [14].

There is a relationship between news coverage and the media agenda, and a theory that comes into place is a theory of framing. 'Frame' is defined by Tankard & Severin [15] as an idea arrangement for news contents that provide context and suggestion of what issues that need to be given extra attention through selection, pressure, no involvement and elaboration. Theoretical foundation of framing theory asserts that the media tell people

both what is important in the world around them and how to think about the events and people who inhabit that world [16]. Framing is based on the assumption that how an issue is characterized in news reports can have an influence over how it is comprehended by audiences [17]. Framing theory in the context of agenda setting is a process through media pressure towards certain definite aspects while displaying other aspects as well. Framing exists through observation to certain subtopics ranging from size, space for story items, narrative presentation or intonation and depth of media coverage [18].

Watson and Hill [19] defined framing as a process by which the media place reality "into frame". These scholars added that framing consists of a narrative device and therefore whatever that is not on the page of a newspaper or news magazine is considered "out of frame". While Gitlin [20] on the other hand explained that news frame allow audiences to manage and comprehend reality to choose appropriate repertoires of cognition and action, but framing devices are also the ways journalists and editors routinely organize news discourse. Gitlin further contended that these framing devices are "persistent patterns of cognition, interpretation, and presentation, of selection, emphasis and exclusion" [20].

Semetko and Valkenburg [21], identified five news frames: 'conflict', 'human interest', 'attribution of responsibility', 'morality' and 'economic consequences'. The conflict frame emphasizes conflict between individuals, groups, institutions or countries. The human interest frame brings a human face, an individual's story, or an emotional angle to the presentation of an event, issue or problem. The responsibility frame presents an issue or problem in such a way as to attribute responsibility for causing or solving to either the government or to an individual or group. The morality frame interprets an event or issue in the context of religious tenets or moral prescriptions. The economic consequences frame, finally, presents an event, problem or issue in terms of the economic consequences it will have on an individual, group, institution, region or country. The study found that the attribution of responsibility frame was the most commonly used followed by the conflict and economic consequences frames based on an analysis of national print and television news [21].

2.2 Priming

Priming can be used in conjunction with stereotype because of the way people process messages in the news. Mass media content can have temporary effects on the way audience members process messages for a short time after exposure [22];[23]. Priming theory suggests that when people see, hear, or read about something, other ideas in memory that have similar meaning are activated for a short time afterward. Those thoughts then activate other thoughts and action tendencies related to the words associated with what was read, seen, or heard, causing a spreading activation [24]. This cognitive process is thought to be unconscious and/or automatic.

Therefore, connections to these related ideas are activated whether or not the individual believes them, provided that they exist in the person's associative network. The individual does not necessarily control the cognitive process; the connections to related ideas are automatic. Thus, priming theory can be used in conjunction with stereotype activation. Individuals effected by the prime will be more likely to apply these stereotypes in their interactions with the target group, even when the task at hand should be irrelevant to the priming experience [25].

3.0 METHODOLOGY

This study applies quantitative content analysis method by using descriptive research design. A distinguishing characteristic of content analysis is its quantitative aspect. Quantitative content analysis consists of tabulating the occurrences of content units. Content analysis aims at statistical formulations, directed toward empirical problems and its statistical character is one of its most distinctive attributes [26]. For this study, content analysis will attempt to characterize the meanings in a given body of discourse in a systematic and quantitative fashion. The selection of the online media to be analyzed is based on purposive sampling.

An international news magazine namely *The Times* from US were selected for a number of reasons; first the United States is a major superpower and an important player in the role of combatting cyberterrorism, particularly after the September 11 attacks. US also represent the supremacy of the

western world in terms of social, political and military and their media have been made as reference by other countries. *The Times* were considered an elite magazine and among the largest media outlets in terms of circulation.

A key word search was conducted around the terms <cyberattack>, <cyberterrorism>, <cyberterror>, <cyberwarfare> and <cyberthreat> for selected news outlet, to generate 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 –and special reports or other features using this terminology.

The data collected will be analyzed using descriptive statistics to observe the categories of news potrayal while the qualitative analysis came up with codes and themes. Variables identified were of types of news, objective of news, cyberterrorism issues, representation of cyberterrorists and types of cyberterrorism threats while news orientation was studied interpretatively. Interpretative analysis was applied to studying news orientation which was classified as engagement, understanding and level of concern the news exhibit. The categories that were studied are followings:

TABLE 1

Categories of Studies

Types of News	Special Reports and Features, Editorials, News in Brief, Culture and Arts, Business News, Opinion Pieces, World News, Technology News, Current Affairs, Profile and Caricature
Objective of News	To inform, to educate, to persuade, to explain, to deny, to accuse and to counter attack
Cyberterrorism issues	All related news, features, photo focus on main issues
Types of cyberterrorism threats	Types of cyberterrorism threats reported by the news media
Representation of Cyberterrorists in news	Professionals, Hackers, Unskilled, Non-state actors, Hacktivists, Presented as non-existent
Engagement	Degree of engagement with concept of cyberterrorism
Understanding	Particular understandings of cyberterrorism
Level of Concern	Concerned, Concerned with elements of scepticism, Balanced, Sceptical, Sceptical with elements of concern

4.0 FINDINGS AND DISCUSSION

Findings of the study are presented in this chapter according to study's research objectives. An array of news framing are presented with statistical data from the codings sheets that contains news reports of *The Times* that reported cyberterrorism. Findings of the study are derived from the coding sheet that was developed to categorize collected data.

Based on the data collection strategy conducted in the web archive of www.nytimes.com, there were 161 news reports in *The Times* that obviously reported the issue of cyberterrorism within the timeframe of 317 weeks and 2 days, from June 1, 2010 to June 30, 2016.

RQ1: Which types of news item were the most common in reporting cyberterrorism within the timeframe of study?

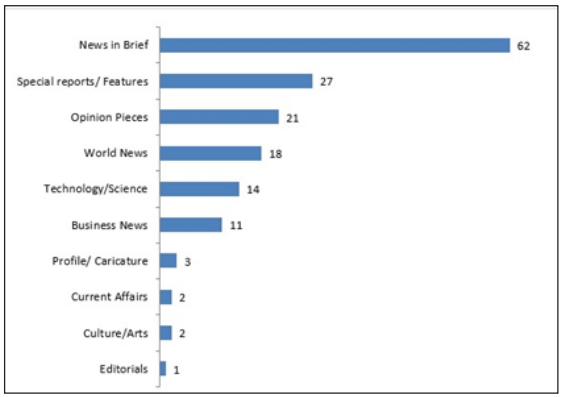

Chart 4.1 Types of News

Chart 4.1 breaks down the 161 news reports, separating them into ten types of piece. Cyberterrorism were commonly reported in "News in Brief" section with 62 news and least mentioned in Profile/Caricature, Business and Editorials section.

Chart 4.1a shows the total number of news reports in *The Times* over the course of research timeframe. As this indicates, there was significant

variation in the coverage of cyberterrorism. The top five on the chart accounted for 142 of the 161 items (equivalent to 88% of the total). The bottom five, in contrast, account for just 19 items (12%).

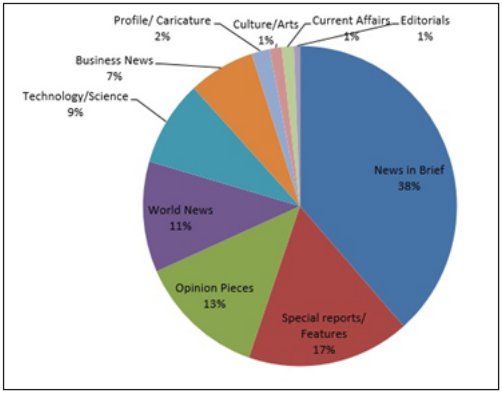

Chart 4.1a Variation of Coverage

RQ2: What are the objectives of news item in reporting cyberterrorism?

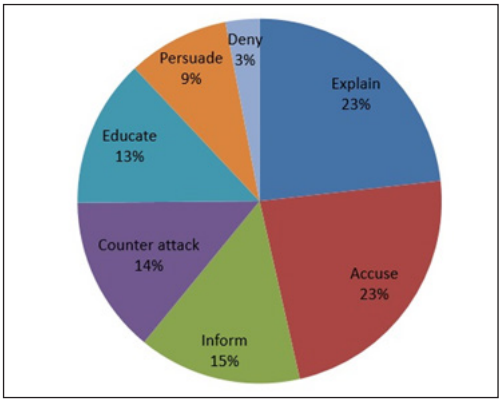

Chart 4.2 Objective of news

RQ3: What are the news frames employed by The New York Times?

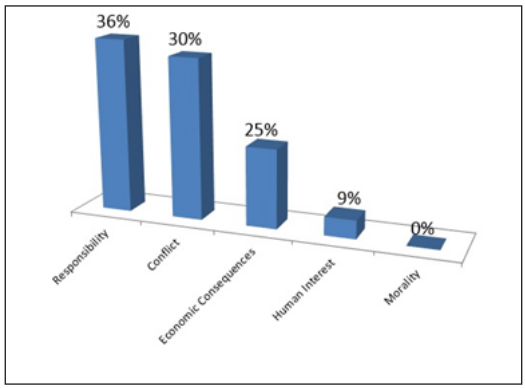

Chart 4.3 Types of news frames

Chart 4.3 demontsrated news frames that were used by *The New York Times* in reporting cyberterrorism. A high percentage (36%) on the attribution of responsibility scale indicated that the story suggests that some level of government has the ability to alleviate, or is responsible for causing, a certain issue or problem whilst the next highest percentage (30%) on the conflict scale indicated that the story reflects disagreement between parties or groups or countries or refers to two or more sides of an issue. A moderate percentage (25%) on the economic consequences scale indicated that the story mentioned financial losses or gains or the degree of expense involved.

76 news items in *The New York Times* fell into "attribution of responsibility" news frame based on measures that were taken by the government to alleviate or retaliate on cyberattacks. Among the items are *White House Weighs Sanctions After Second Breach of a Computer System* by Micheal D. Shear and Scott Shane, published on June 12, 2015, and U.S. Cyberattacks Target ISIS in a New Line of Combat by David E. Sanger, published on April 24, 2016 that clear illustrate the specified frame. Below are the excerpts from the first news reports, White House Weighs Sanctions After Second Breach of a Computer System.

> "Mr. Obama signed the executive order after the attack on Sony Pictures'computer network, an intrusion that American officials believe was carried out by the government of North Korea. The order gives the administration the ability to freeze assets in the United States, bar Americans from doing business with groups that sponsor cyberattacks, and cut the groups off from American goods and technology." (Para. 11)

Secondly, the news report of U.S. Cyberattacks Target ISIS in a New Line of Combat by David E. Sanger and appeared in the web archive of *The Times* on April 24, 2016 in Politics section.

> "While officials declined to discuss the details of their operations, interviews with more than a halfdozen senior and midlevel officials indicate that the effort has begun with a series of "implants" in the militants' networks to learn the online habits.

The second highest frame "conflict" garnered 71 news items from various sections. This frame explained the tendency of *The Times* to report disagreement between parties or groups or countries or refers to two or more sides pertaining to cyberterrorism. Among news items that fell into this are listed as follows. They were (1) China Blasts Hacking Claim by Pentagon by Keith Bradsher, May 7, 2013; and, (2) China Won't Cut Its Cyberspying by Grey Austin, February 20, 2013.

China Blasts Hacking Claim by Pentagon

> "From the president down, people in the United States have leveled accusations, and China has already many times answered those accusations." (Para. 5)

China Won't Cut Its Cyberspying

> "Chinese military planners believe that they would only launch a cyberattack on U.S. critical infrastructure in the event of an imminent large scale military clash with the United States over Taiwan. While

> Americans cannot have equal confidence, and their concern is legitimate, it is the Chinese perception that shapes China's responses (Para. 13)
>
> "The American case is not helped by its blurring of the two distinct complaints: I.P.R. theft and national security threats. This confusion comes about because some in the United States have assessed that China has an explicit policy of eroding American national economic power through largescale cyberespionage. This is presented as a form of economic warfare — an argument that many American analysts dispute.." (Para. 14)

RQ4: What are the issues highlighted in the news item of cyberterrorism?

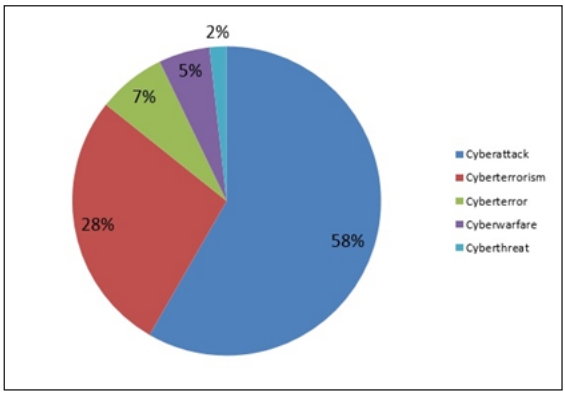

Chart 4.4 Issues in news items

A key word search was conducted around the terms <cyberattack>, <cyberterrorism>, <cyberterror>, <cyberwarfare> and <cyberthreat> for selected news outlet, to generate relevant items. Chart 4.4 indicates that *The New York Times* commonly adapt the term "cyberattack" as part of cyberterrorism with 98 items (58%) rather than reporting it using the term "cyberterrorism" itself. Other results as follows.

RQ5: What level of concern did the news items exhibit?

The next stage of the analysis coded and places each news items into one of the following six categories: skeptical; skeptical with elements of concern; concerned with elements of scepticism; balanced or, concerned.

A story was coded as concerned or sceptical if it was characterized by a clearly identifiable stance on the threat posed by cyberterrorism, offering no space for consideration of alternative perspectives. On the other hand, 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. Balanced coverage was characterized by the presence of competing narratives over the cyberterrorism threat and the absence of any definitive conclusion about the plausibility of these. The results of analysis are displayed in Chart 4.5.

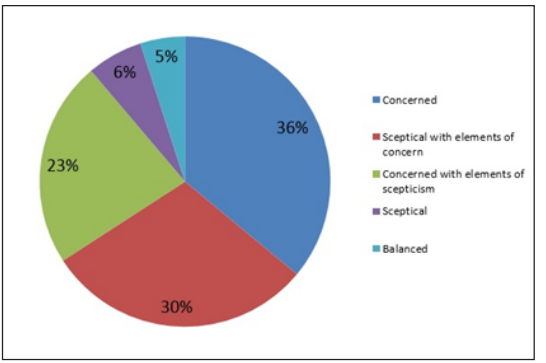

Chart 4.5 Level of Concerns

RQ6: What were the different levels of focus on, and understandings of, cyberterrorism in the news items?

The analysis of the tone 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 accprding to whether cyberterrorism was their primary focus, their secondary focus, or a topic mentioned in passing without any detailed discussion or analysis. As Chart 4.6 shows, a total of 80 items (50% of the

dataset) had cyberterrrorism as their primary focus, with a further 53 items (33%) having it as their secondary focus. There were 28 items (17%) that mentioned cyberterrorism without examining the concept in detail.

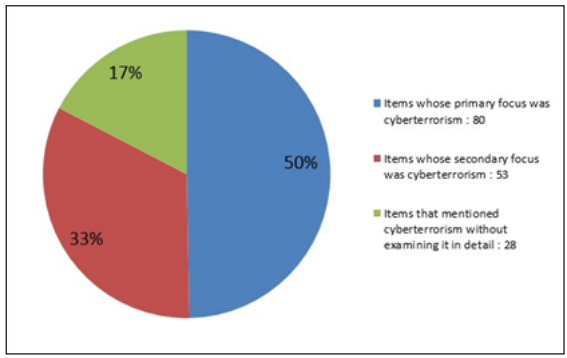

Chart 4.6 Level of engagement

Particular understandings of cyberterrorism were evident in 161 items. The breakdown of these understandings as follows:

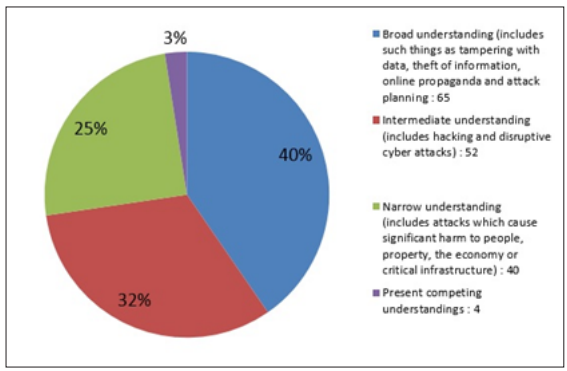

Chart 4.6a Level of understanding

RQ7: What are the types of cyberterrorism threats reported in the news items?

Chart 4.7 shows the total number of news items that mentioned one or more cyber events over the course of research timeframe. As this indicates, there was significant mention on cybersecurity policy, law or superior

directive from US President or Officers in charge. The most commonly mentioned were as follows:

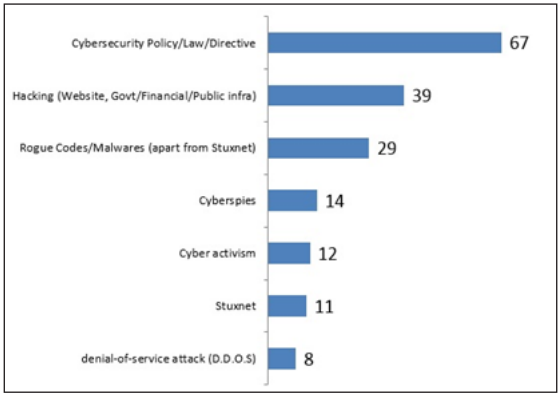

Chart 4.7 Types of threats

Meanwhile, 14 items mentioned one or more past events, cyber or non-cyber. The most commonly mentioned were as follows:

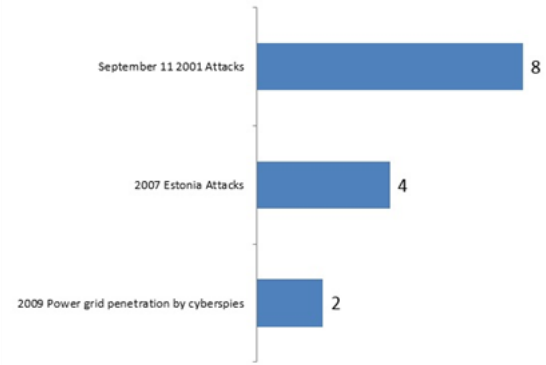

Chart 4.7a Types of past threats

RQ8: How were cyberterrorists represented?

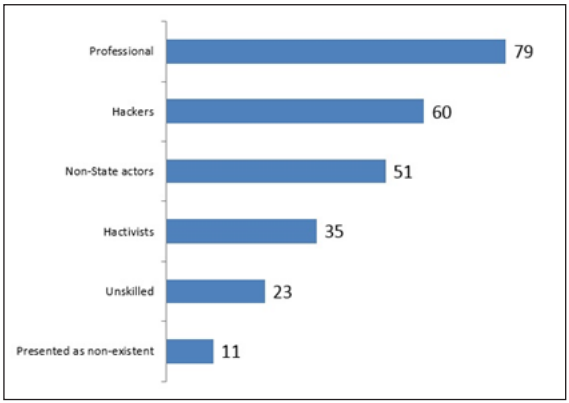

Chart 4.8 Representation of Cyberterrorists

The 161 news items offered specific representations of the identity of cyberterrorists. Five distinct identity types were present in the dataset: hackers; hacktivists; professionals; unskilled; non-state actors; and presented as non-existent. When an item contained more than one of these representations, they were included multiple times.

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 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.

Whilst the term hacker was used to refer to individuals, the term hacktivist refers to coverage of groups or their members who self-identify as collectives with a shared objective, such as Anonymous.

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. 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. As Chart 4.8 demonstrates, cyberterrorists were commonly potrayed as professionals with 79 (30%) followed by hackers 60 (23%) and non-state actors at with (20%) of the news items. A further 35 (14%) of the items potrayed cyberterrorists as hactivists, 23 (9%) of the items potrayed as unskilled and 11 (4%) of the news items potrayed cyberterrorists as non-existent.

5.0 CONCLUSION

This study sketches some of the key developments within the coverage–or construction–of cyberterrorism and its threat in *The New York Times* between 2010 and 2016. 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 content that focuses on cyberterrorism: a phenomenon that some (although not all) academic researchers argue has yet to occur [1]. 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. 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' [27]. 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 [28] wrote, 'is not an objective condition'. 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' [29].

Findings of this study suggested that *The Times* was enthusiastic to highlight cyberthreats and cyberattack through its news reports. Based on quantitative media content analysis conducted, study had stipulated five themes to categorize news reports of on *The Times* newspaper based on five news frames identified by Semetko and Valkenburg [21]. They were Conflict frame, Human interest frame, Economic consequences frame and Morality frame.

Responsibility and Conflict frames were the most significant and were paralleled to the manifesto by President Barack Obama to the Congress to pass broad legislation to bolster cybersecurity across the United States government and private industry, working to capitalize on concern about recent high¬profile computer breaches to counter an escalating threat.

The newspaper also could be proved to form 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.

Future research will seek to build on the analysis presented here by exploring more specific aspects of findings from this study. 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. Additionally, a study of semantics could be conducted to understand thoroughly the meaning of cyberterrorism words or concepts, as well as to examine the usage distinction of terrorism-related words or concepts in an array of media through a comparative study.

6.0 REFERENCES

[1] Weiman, G. (2004). Cyberterrorism. How Real Is the Threat, United States Institute of Peace, Washington.

[2] Eskew, C. "Is the U.S. prepared for cyberterrorism?," The Washington Post, March 29 2013, accessed December 15 2016, http://www.washingtonpost.com/blogs/post-partisan/wp/2013/03/29/is-the-u-s-prepared-for-cyberterrorism/.

[3] Quain, J. "10 Years After 9/11, Are America's Cyberdefenses Weaker?," Fox News, September 10 2011, accessed December 15 2016, http://www.foxnews.com/tech/2011/09/10/10-years-after-11-are-americascyberdefenses-weaker/.

[4] Drury, I. "Cyber terrorists could inflict 'fatal' attack on Britain because Armed Forces rely so heavily on computers, MPs warn," Mail Online, January 9 2013, accessed December 15 2016, http://www.dailymail.co.uk/news/article-2259374/Military-cyber-attack-threat-Armed-Forces-rely-heavily-computers-MPs-warn.html.

[5] Foo, F. "Cyber terrorism threat 'not taken seriously enough'," The Australian, September 14 2010, accessed November 15 2016, http://www.theaustralian.com.au/technology/cyber-terrorism-threat-not-taken-seriously-enough/story-e6frgakx1225921434904nk=8348714490b52fe465d858bc0dc812e2.

[6] Conway, M. (2008). The media and cyberterrorism: A study in the construction of 'reality. The politics of securing the homeland: Critical infrastructure, risk and securitisation, pp. 43–44.

[7] Jarvis, L., Macdonald, S., & Whiting, A. (2016). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat.

European Journal of International Security.

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

[9] Steuter, E., & Wills, D. (2009). At war with metaphor: media, propaganda, and racism in the war on terror. Lexington Books.

[10] Malcolm, J.G. (2004). 'Testimony of Deputy Assistant Attorney General John G. Malcolm on Cyberterrorism', before the Senate Judiciary Committee Subcommittee on Terrorism, Technology, and Homeland Security, February 24, Washington, DC.

[11] Anderson K (2009) Hacktivism and politically motivated computer crime. Encurve. http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Accessed 3 June 2016, pp.1–15.

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

[13] Goffman, E. (1974). Frame analysis: An essay on the organization of experience. Harvard University Press.

[14] Cissel, M. (2012). Media Framing: a comparative content analysis on mainstream and alternative news coverage of Occupy Wall Street. The Elon Journal of Undergraduate Research in Communications, 3(1), pp. 67-77.

[15] Severin, W. J., & Tankard, J. W. (2001). Communication theories: Origins, methods, and uses in the mass media. Pearson College Division.

[16] Brown, J. D. (2002). Mass media influences on sexuality. The Journal of Sex Research, 39(1),pp.42-45.

[17] Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. Journal of communication, 57(1), pp.9-20.

[18] Miller, K. (2000) Communication Theories: Perspective, Processes and Context. Boston.

[19] Watson, J. & Hill, A. (2000). Dictionary of media & communication. 5th ed. London: Arnold Publishers, pp.117.

[20] Gitlin, T. (1980). The whole world is watching: Mass media in the making and unmaking of the new left. In Blood, R.W. (2002). A qualitative analysis of the reporting and portrayal of mental illness in the Courier Mail and Sunday Mail, December 2001 to February 2002. School of Professional Communication, University of Canberra, Canada.

[21] Semetko, H. A., & Valkenburg, P. M. (2000). Framing European politics: A content analysis of press and television news. Journal of communication, 50(2), 93-109.

[22] Berkowitz, L. (1986). A survey of social psychology (3rd ed.). New York: Holt Rinehart and Winston.

[23] Devine, P.G. (1989). Stereotypes and prejudice: Their automatic and controlled components. Journal of Personality and Social Psychology, 56, 5-18.

[24] Jo, E., & Berkowitz, L. (1994). A priming effect analysis of media influence: An update. In J.Bryant & D. Zillmann (Eds.), Media effects: Advances in theory and research. Hillsdale, NJ: Erlbaum. pp. 43-60.

[25] Sherman, S.J., Mackie, D.M. & Driscoll, D.M. (1990). Priming and the differential use of dimensions in evaluation. Personality and Social Psychology Bulletin 16, 405–418.

[26] Janis, Irving L. and Raymond H. Fadner. 1942. "A Coefficient of Imbalance for Content Analysis." Experimental Division for the Study of War Time Communications, Document No. 31, Nov. 1. Washington, DC: Library of Congress.

[27] Macdonald, S., Jarvis, L. & Chen, T. (2013) A Multidisciplinary Conference on Cyberterrorism: Final Report, Cyberterrorism Project Research Report. A Multidisciplinary Conference on Cyberterrorism. Swansea University.

[28] Campbell, D. (1998). Writing security: United States foreign policy and the politics of identity. U of Minnesota Press.

[29] Jackson R et al (2011) Terrorism: a critical introduction. Palgrave, Basingstoke.