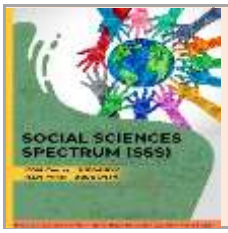


Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-0427 **P-ISSN:** 3006-0419
Volume 03, **Issue** 04, 2024
Web link:https://sss.org.pk/index.php/sss

Check for updates

Media Framing of Digital Threats: A Critical Analysis of Cyberterrorism in Pakistani News Discourse

Roshni Arshad
Lecturer, Department of Communication and Media Studies, University of Sargodha, Sargodha-40100, Punjab, Pakistan
Correspondence: roshniarshad21@gmail.com

Ahsan Raza
Lecturer, Department of Communication and Media Studies, University of Sargodha, Sargodha-40100, Punjab, Pakistan
Email: ahsanraza163@gmail.com

Malik Farrukh Naeem
M.Phil Alumnus, Department of Communication and Media Studies, University of Sargodha, Sargodha-40100, Punjab, Pakistan
Email: farrukhnaeem4321@gmail.com

Article Information [YY-MM-DD]

Received 2024-11-25 **Accepted** 2024-12-28

Citation (APA):

Arshad, R., Raza, A & Naeem, M, F. (2024). Media framing of digital threats: A critical analysis of cyberterrorism in Pakistani news discourse. *Social Sciences Spectrum*, *3*(4), 505-514. https://doi.org/10.71085/sss.03.04.247

Abstract

Cyberterrorism's novelty has garnered mass media attention from the beginning. Evaluations of the cyberterrorism threat point to sociopolitical and infrastructure weaknesses that well-resourced and well-intentioned individuals could exploit. The study aims to investigate how cyberterrorism is framed or constructed by prominent Pakistani News Media outlets. Using the quantitative content analysis approach, the researcher has identified five major frames utilized by news organizations. Findings reveal that the "Growing Threat" is most framed, highlighting public concern over the rising dangers of cyberterrorism. The analysis also identifies the "Administrative" frame as the most dominant, emphasizing the need for national preparedness against cyberattacks. However, the study uncovers a crucial issue: the media's portrayal often conflates cyberterrorism with cybercrimes, blurring the lines between distinct threats. This ambiguity necessitates a call to action for policymakers and news media to adopt precise terminology and enhance public understanding of the diverse nature of cyber threats.

Keywords: Cyberterrorism, Framing, News Media, Content Analysis, Cybercrime.

Content from this work may be used under the terms of the Creative Commons Attribution-Share-Alike 4.0 International License that allows others to share the work with an acknowledgment of the work's authorship and initial publication in this journal.

Copyright (c) 2024 Arshad, Raza & Naeem

1. Background

The landscape of cyberterrorism is constantly shifting, making it a difficult domain to track and understand. (Clarke & Knake, 2010; Kello, 2013; Lindsay, 2013). This environment encourages misinterpretation and calculation, threatening stability and increasing the possibility of unintentional or deliberate crisis escalation (Buchanan, 2020; Buchanan & Cunningham, 2020; Jervis, 2017). Cyberterrorism can be seen as the intersection of terrorism and cyberspace. The term itself was first coined in the 1980s by Collin and Copper (2012), referring to violent attacks achieved through the internet. While widely used by policymakers, politicians, law enforcement, academics, and media, the term carries significantly different meanings depending on the context.

Dorothy Denning's (2000) definition of cyberterrorism, which defines it as "illegal attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" is arguably the most influential. The illegality of the conduct and the intention to compel or threaten social or political ends are highlighted in this description. Although Denning's definition covers a broader variety of activities than Collin's, both emphasize the deliberate use of cyberspace to fulfill one's goals or desires.

Data breaches, attacks on critical infrastructure, ransomware, and cybercrime victimization are gaining a worrying surge. Malicious actors constantly develop sophisticated tools and techniques to bypass security measures, infiltrating systems more easily. Modern cyberattacks are more destructive and often carried out by well-resourced hacker groups. Some groups are allegedly state-sponsored, as seen in the Colonial Pipeline and Solar Winds hacks, while others may have links to terrorist organizations (Bastug, 2021a, 2021b). These attacks can devastate, disrupting essential services, causing significant financial losses, and eroding public trust in digital infrastructure. The rise of these threats necessitates robust defense strategies. Increased investment in cyber-defenses, international cooperation on cybercrime, and public awareness campaigns are crucial to mitigate these growing risks.

However, cyberterrorism is also a major threat to a sustainable future, as outlined by the UN’s Sustainable Development Goals (SDGs), and it faces a silent but growing threat: cyberterrorism. These malicious attacks go beyond stealing data; they can cripple essential services like power grids and water treatment, jeopardizing access to clean water and sanitation (SDG 6) and affordable and clean energy (SDG 7). Healthcare systems crippled by cyberattacks can leave entire communities vulnerable, hindering progress towards good health and well-being (SDG 3). Cybercrime, often linked to cyberterrorism, siphons resources away from developing economies, hindering efforts to eradicate poverty (SDG 1). This fear and instability can erode public trust in institutions (SDG 16), jeopardizing the very foundation of peaceful societies (SDG 16). By proactively addressing cyber threats, we can safeguard critical infrastructure, protect healthcare systems, and strengthen institutions - all crucial steps towards achieving the interconnected goals of the SDGs. It is the need of the hour to work together to build a digital world that fosters, not hinders, sustainable development.

2. Literature Review

The Idea of Cyberterrorism research dates back to the late 1900s (Littleton, 1995; Nelson et al., 1999; Ogren & Langevin, 1999). In the early 2000s, the idea began to garner more and more scholarly attention. The primary goals of the early research were to characterize the phenomena that were only beginning to emerge (Gordon & Ford, 2002; Veerasamy, 2009) and to evaluate the threat (Embar-Seddon, 2002; Thomas, 2003; Weimann, 2004). A review of the early research

indicates that some researchers anticipated the emergence of a digital threat and saw cyberspace as a force multiplier for terrorist activity. Other researchers took a more pessimistic view of cyberterrorism and contended that the media exaggerated the threat, especially (Debrix, 2001; Weimann, 2004, 2005).

People can obtain instant information from various media outlets, and communication literature includes two categories of media content: print and television (Cho et al., 2003). Additionally, it seems that terrorist groups want media coverage of their acts in order to spread their political ideologies to a larger audience (Nacos, 1996, 2003; Schmid & Graff, 1982). Terrorist attacks indeed garner media attention. As a result, there is controversy around the relationship between the media and terrorism (Onat et al., 2021). According to Comer and Kendall (2007), the media's portrayal of terrorist attacks also fuels societal unease and terror, which is advantageous for different terrorist organizations.

Cyberterrorism is a social construction instead of an extra-discursive reality because it results from meaning-making processes connected to political discourse, popular culture, cyber-security companies, or the media (Conway, 2002). The terminology of cyberterrorism deployed by the media and its purported specialists is highly sophisticated (Debrix, 2001). Thanks to the taxonomy and technical vocabulary used by the media, the public can perceive that cyberterrorism poses a threat, conveying the message that there will be significant casualties among the populace.

Research on "how different media outlets framed cyberterrorism" has examined how the media contributes to the propagation of fear about this phenomenon. Jarvis et al. (2015) explored how the news media constructs cyberterrorism as a security concern by analyzing news items about the phenomenon that were published in seven different nations between 2008 and 2013. As mentioned previously, many of the stories conveyed concern regarding the threat of cyberterrorism. The research examined how the media reported this issue and defined the referents of the media discourse concerning cyberterrorism (Jarvis et al., 2017). Within the scope of coverage, they found that the nation-state is the primary actor purportedly at risk from cyberterrorism, along with critical infrastructure and the business sector.

This analysis focuses on cyberterrorism coverage in three leading newspapers of Pakistan: The Dawn, The News International, and The Nation. These newspapers have considerable circulation and serve as an important source of information for the public regarding how incidents of cyberterrorism are reported in Pakistan tentatively and what narrative is built around them.

3. Theoretical Framework

According to Goffman (1974), a ‘frame’ in social theory is a set of criteria, stories, and a framework that one uses to act and understand the activity happening around him or her. Framing refers to another communication concept in which journalists use specific frames to help guide readers' understanding and shape their perception of the news (Cissel, 2012).

There is a connection between the media agenda and news coverage; one notion that takes hold is the framing theory. Severin and Tankard (2001) define “frame” as an idea arrangement for news contents that offer context and recommendations for concerns that require additional attention through selection, pressure, lack of involvement, and elaboration. According to the theoretical underpinnings of framing theory, people are informed by the media about what matters in the world and how to interpret the events and people that take place in it (Brown, 2002). Framing is predicated on the idea that news broadcasts’ portrayals of a topic might affect how readers understand it (Scheufele & Tewksbury, 2007). In agenda-setting, framing theory refers to a method wherein the media pushes particular features while simultaneously showcasing others. Framing

occurs through monitoring specific subtopics, such as media coverage depth, narrative presentation or intonation, size, and space for story components (Miller, 2000).

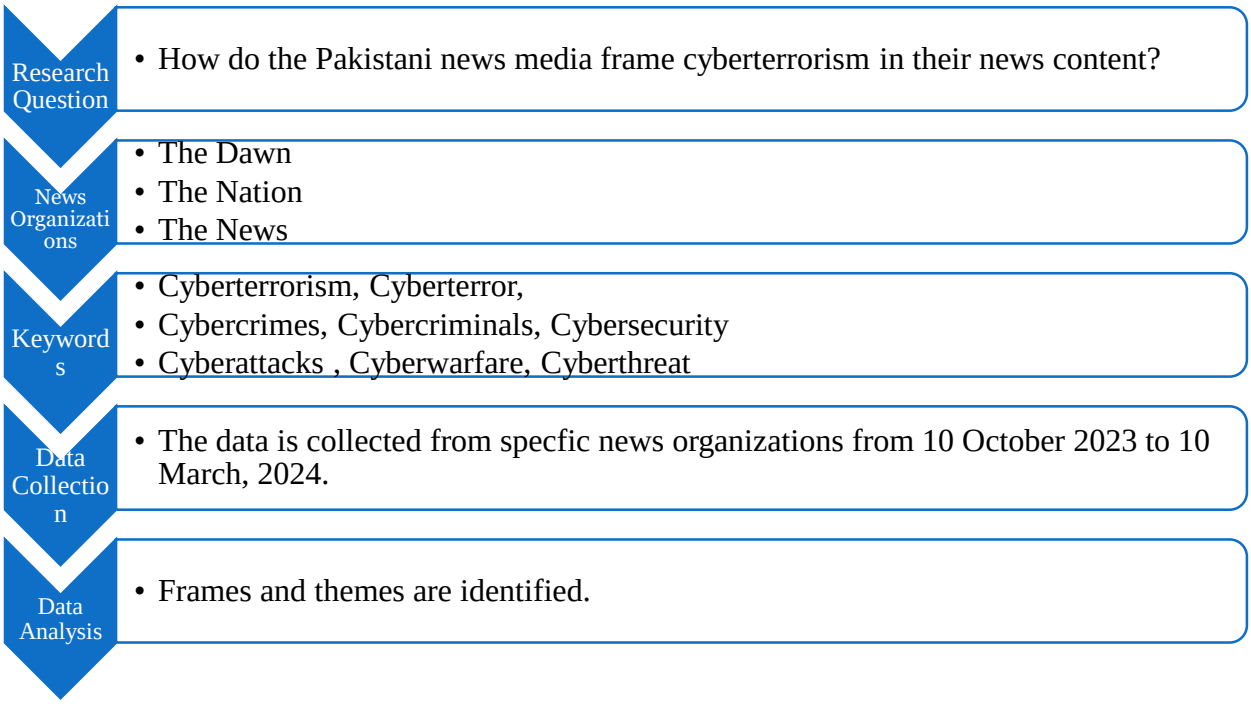
According to Watson and Hill (2000), framing is the process by which the media "frames" reality. According to these academics, framing is a narrative device; everything not on a newspaper or news magazine page is therefore deemed "out of frame." On the other hand, Gitlin (1980) clarified that news frames enable viewers to control and understand reality to select suitable thought and action repertoires; yet, framing devices are also how journalists and editors regularly arrange news discourse. These framing strategies are "persistent patterns of cognition, interpretation, and presentation, of selection, emphasis, and exclusion" (Gitlin, 1980). However, this research intends to answer the question: "How do the Pakistani news media frame cyberterrorism in their news content?"

4. Methodology

The quantitative content analysis method and a descriptive research methodology are both used in this study. The quantitative aspect of content analysis sets it apart from other methods. The quantitative content analysis process involves tabulating content unit occurrences. The statistical aspect of content analysis, which focuses on statistical formulations centered on empirical challenges, is one of its most distinctive features (Janis & Fadner, 1942). The goal of this study's content analysis is to carefully and quantitatively describe the meanings found within a certain language corpus.

Three of Pakistan's most prominent English newspapers (The Dawn, The News, and The Nation) were selected for analysis based on their circulation and readership. The time frame of the study was from October 2023 to 10 March 2024. A keyword search was conducted to gather news content from these news organizations' online archives. The keywords are cyberterrorism, *cyberterrorist, cybercrimes, cybercriminals, cyberattacks, and cyberwarfare*, which are used to gather news content from particular news organizations. The news items include news stories, columns, and editorials.

The data collected from each news organization is then analyzed through descriptive analysis to gain insight into each type and category of news content. Conversely, qualitative analysis has been employed to discover underlying themes and frames.



5. Findings

The data gathered through the specific keywords have a certain number of duplicate news content removed from the sample to maintain the data quality. The news is the same news content was published by two or more newspaper organizations. Then the researcher considered the source that appeared first. Table 1 reveals the number of news items from each news organization in our data sample.

Table 1: *Number of Article from Each Newspaper*

Newspaper	Number
The Dawn	18
The Nation	20
The News International	13
Total	51

The data is analyzed using a thematic content analysis strategy. A list of the themes or frames has been identified by Bastug et al., 2023. The themes were Growing threats, National Preparedness, Administrative (policies, orders, laws), cyber-threats from terrorist groups, State-linked groups, Cyber doom scenarios, Critical infrastructure, Criticism, and Consequences. However, our study results in just five frames, and their description are given in table 2.

Table 2: *Conceptualization of Frames of the Study*

Frames	Description
Growing Threat	The news content highlights cyber-terrorism as most daunting or eminent threat.
National Preparedness	The news content highlights the importance of national preparedness against cyber terrorism.
Cybercrime Scenarios	The news content highlights cybercrimes cases, reports, Proceedings
State linked Cyber Threats	The news content highlights overall state linked cyber threats from militant groups.
Administrative (policies, orders, laws etc.),	The news content highlights administrative actions, polices, orders etc.

The very first frame of our study is 'Growing Threat', in which the news content highlights cyber terrorism or crimes as a growing threat. An example of this is extracted from our data sample 'The Nation newspaper' as follows:

"*Experts of the global cyber security and digital privacy company Kaspersky have revealed that the number of overall cyber threats in Pakistan has increased by 17% in 2023 as compared to 2022*."

The second frame of the study is 'National Preparedness', which highlights the need for national preparedness against cyberattacks at the national level. The statement made by the federal minister is as follows:

"Caretaker Federal Minister for Information Technology and Telecommunication Dr. Umar Saif Wednesday said that the protection of Pakistan's cyberspace under the PECA Act is very important."

'The Cybercrime Scenario' frame includes the cybercrime that has been done or its looming implication in the news content. The terrifying incident of cybercrime reported by 'Dawn News' is:

"*The case followed a typical pattern for cybercrime, in which "kidnappers" tell a victim to isolate and provide pictures of themselves as if being held captive — photos that are then sent to the victim's family to extort payment*."

Another study frame is 'State-Linked Threats' in which the news content highlights state-level state-levels or threats by threats state or militant groups. The extract for this frame is from 'Dawn News':

"*State-backed hackers from Russia, China, and Iran have been using tools from Microsoft-backed Open AI to hone their skills and trick their targets, according to report published on Wednesday*."

'The Administrative frame' involves news content that gives information about administrative tasks such as laws, policies, strategies, orders, etc. The news content discusses an organizational setup for catering to cyberterrorism:

"*The National Cyber Crime Investigation Agency (NCCIA) is being established to check increasing cybercrimes while stringent measures were being taken to control smuggling, said Rai Ijaz Ahmad, Director Federal Investigation Agency (FIA).*"

Table 3: *Analysis of Frame Categories*

Frame	Number (N)
Growing Threat	13
National Preparedness	4
Cybercrime Scenarios	10
State linked Cyber Threats	5
Administrative (policies, orders, laws etc.),	19

The number of news content corresponding to each frame is demonstrated in Table 3. Our analysis shows that the most dominant frame in the Pakistani news media landscape is Administrative, with a count of 19, followed by Growing threat and cybercrime scenarios. However, the Administrative frame focusing on the administrative issues regarding cyberterrorism highlighted the policy recommendations, budget allocation and cybersecurity issues regarding cyberterrorism in Pakistan. Additionally, the growing threat frame is the second most dominant frame and should be taken more seriously to address the increasing concern about cyberterrorism. Cybercrime scenarios are also prevalent, giving us insight into the ongoing type and frequency of cybercrimes or attacks. Sate-linked cyber-threat and National Preparedness are the least observed frames.

6. Conclusion and Discussion

The terrifying fact of modern times is the rise of cyberterrorism. It is even scarier than conventional terrorism since its repercussions are mostly unknown to the public. People's concerns about this emerging threat appear partly fueled by the recent cyberattacks and the media's coverage. Our qualitative investigation revealed that cyberterrorism is frequently presented as an expanding issue threatening society. This is hardly shocking given the constant evolution of cyber threats and the rise in companies and people targeted by cyberattacks.

The findings show that the Administrative frame is the most common. The Pakistani government established the National Cyber Crime Investigation Agency (NCCIA) to prioritize cybersecurity. As a result, new cybersecurity regulations have been the subject of numerous talks. The most noteworthy finding from our investigation relates to the definition and formation of the idea of cyberterrorism in the media. Our sample revealed five publications discussing cyberattacks or cyber threats from organizations with ties to the state.

The data demonstrates that when it comes to differentiating cyberterrorism from other cyber threats like cyberwarfare, the media is not always doing a good job. Our investigation also showed that how cyberterrorism is portrayed in the media differs from how it is primarily defined in cyberterrorism literature. Since cyberterrorism is a type of terrorism, an attack must meet the criteria for being labelled as cyberterrorist to be considered legitimate, including ideological motivation and psychological effects that extend beyond the immediate victims (Hoffman, 2018). Nonetheless, many cyberattacks with financial and illegal goals are mislabeled as cyberterrorism in the media. Due to this misperception, "cyberterrorism" has become an umbrella term used by the media for any cyber offense. These are misrepresented cyberattacks that do not reach the level of terrorism.

The research results require policymakers to explain the distinction as there are lots of terminologies involved in the media coverage of significant cyberattacks to avoid jargoning cyber catastrophes. As for the Pakistani media, the editorial committees should care more about how the words “cyberattack,” “cyber threat,” and “cyber terrorism” are used to educate the public properly. Moreover, the research did not evaluate how specific themes or stories impacted the selected participants' levels of terror. In the future, more research could be done on the emotional response caused by cyberterrorism news.

References

Bastug, M. F. (2021a). Cyber evolution of terrorist groups. Orion Policy Institute. https://orionpolicy.org/orionforum/58/cyber-evolution-of-terrorist-groups

Bastug, M. F. (2021b). Rethinking cybersecurity after colonial pipeline hack. Orion Policy Institute.https://orionpolicy.org/orionforum/8/rethinking-cybersecurity-after-colonial-pipeline-hack

Bastug, M. F., Onat, I., & Guler, A. (2023). Threat construction and framing of cyberterrorism in the U.S. news media. *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(1), 29-44. http://doi.org/10.52306/KPIO9808

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

Buchanan, B. (2020). *The hacker and the state: Cyber-attacks and the new normal of geopolitics.* Cambridge, MA: Harvard University Press.

Buchanan, B., & Cunningham, F. S. (2020). Preparing the cyber battlefield: Assessing a novel escalation risk in a Sino-American crisis. *Texas National Security Review, 3*(4), 54–81.

Cho, J., Boyle, M. P., Keum, H., Shevy, M. D., McLeod, D. M., Shah, D. V., & Pan, Z. (2003). Media, terrorism, and emotionality: Emotional differences in media content and public reactions to the September 11th terrorist attacks. *Journal of Broadcasting & Electronic Media, 47*(3), 309-327.

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), 67-77.

Comer, J. S., & Kendall, P. C. (2007). Terrorism: The psychological impact on youth. *Clinical Psychology: Science & Practice, 24*(3), 179–212.

Conway, M. (2002). What is cyberterrorism? *Current History, 101*(659), 436.

Debrix, F. (2001). Cyberterror and media-induced fears: The production of emergency culture. *Strategies: Journal of Theory, Culture & Politics, 14*(1), 149-168.

Denning, D. E. (2000). Cyberterrorism: The logic bomb versus the truck bomb. *Global Dialogue, 2*(4), 29.

Embar-Seddon, A. (2002). Cyberterrorism: Are we under siege? *American Behavioral Scientist, 45*(6), 1033–1043.

Gitlin, T. (1980). *The whole world is watching: Mass media in the making and unmaking of the new left.* University of California Press.

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

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers & Security, 21*(7), 636-647.

Hoffman, B. (2018). *Inside terrorism.* Columbia University Press.

Janis, I. L., & Fadner, R. H. (1942). A coefficient of imbalance for content analysis. *Experimental Division for the Study of War Time Communications, Document No. 31.* Washington, DC: Library of Congress.

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing cyberterrorism as a security threat: A study of international news media coverage. *Perspectives on Terrorism, 9*(1), 60-75.

Jervis, R. (2017). *Perception and misperception in international politics: New edition.* Princeton University Press.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security, 38*(2), 7–40.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404.

Littleton, M. J. (1995). *Information Age Terrorism: Toward Cyberterror* [Master's Thesis]. *Naval Postgraduate School.*

Miller, K. (2000). *Communication theories: Perspective, processes, and context.* Boston.

Nacos, B. L. (1996). *Terrorism and the media.* Columbia University Press.

Nacos, B. L. (2003). The terrorist calculus behind 9-11: A model for future terrorism. *Studies in Conflict and Terrorism, 26*(1), 1–16.

Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning." *Parameters, 33*(1), 112.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyberterror: Prospects and implications. *White Paper.* Naval Postgraduate School.

Ogren, J. G., & Langevin, J. R. (1999). Responding to the threat of cyberterrorism through information assurance [Master's Thesis]. *Naval Postgraduate School.*

Onat, I., Guler, A., Kula, S., & Bastug, M. F. (2021). Fear of terrorism and fear of violent crimes in the United States: A comparative analysis. *Crime & Delinquency.* Advance online publication.

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

Schmid, A. P., & Graff, J. (1982). *Violence as communication: Insurgent terrorism and the western news media.* Sage.

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.

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

Veerasamy, N. (2009). A high-level conceptual framework of cyber-terrorism. *Journal of Information Warfare, 8*(1), 43-55.

Watson, J., & Hill, A. (2000). *Dictionary of media & communication* (5th ed.). London: Arnold Publishers.

Weimann, G. (2004). Cyberterrorism: How real is the threat? *United States Institute of Peace.* https://www.usip.org/sites/default/files/sr119.pdf

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism, 28*(2), 129-149.