Literature Review Plan & Outline

Topic: State-Sponsored Cyberterrorism in Global Politics

Introduction

The term 'cyberterrorism' describes a pre-meditated and politically motivated attack against information and computer systems (Veerasamy, 2020). According to Conway (2012), significant system or data disruptions need to occur for an attack to be considered cyberterrorism, although this is still an ongoing discussion in academic circles. As technology advances, and computers, as well as phones, tablets, and other computing devices, become more integral to the world's day-to-day life, the attack surface for, and the frequency of cyberterrorism has rapidly increased (Gao et al., 2021). There is no doubt about the devastating impact of such attacks, and some academics have gone so far as to label cyberterrorism the most important threat to national security (Petr, 2022; Singh, 2016).

In this review, we will discuss the history of cyberterrorism, as well as the current academic opinion and research that is being conducted in this field. In this review, we will focus on three major political powers - the United States of America, Russia, and China - and how they have used, or misused, IT systems for political gain in recent conflicts.

Theoretical Framework

Definition and Concepts

Theories of International Relations

Historical Context

Evolution of Cyberterrorism

Technological Advancements

Cyberterrorism has evolved beyond traditional definitions (Al Asyari, 2022), which in turn has caused ongoing academic discussions about the differences between cyberterrorism and cybercrime. Grobbelaar (2022) argues that there is no clear distinction between cyberterrorism, cybercrime, and the usage of the internet by terrorists.

Case Studies

Notable Incidents

Comparative Analysis

Impact Analysis

Global Politics and Relations

Economic Impact

Social and Ethical Considerations

Countermeasures and Policy Responses

International Cooperation

National Strategies

Challenges and Limitations

Future Directions

Emerging Threats

Recommendations for Policy and Practice

Conclusion

Summary of Findings

Implications

Areas for Future Research

Bibliography

Veerasamy, N. (2020) *Chapter 2 - Cyberterrorism - the spectre that is the convergence of the physical and virtual worlds.* Academic Press. DOI: https://doi.org/10.1016/B978-0-12-816203-3.00002-2 [Accessed 24 March 2024].

Conway, M. (2003) Cyberterrorism: The Story So Far. *Journal of Information Warfare* 2(2): 33-42. Available from: https://doras.dcu.ie/496/1/info_warfare_2_2_2003.pdf [Accessed 24 March 2024].

Gao, M., Dong, Y., Qiao, X. & Fan, S. (2021) The Study of the Plight of Cyberterrorism and Its Way Out. *The Frontiers of Society, Science and Technology* 3(1): 93-98. DOI: https://dx.doi.org/10.25236/FSST.2021.030115 [Accessed 24 March 2024].

Petr, K. (2022) Cyberterrorism as the Most Important Threat to the National Security of the Russian Federation and its Main Warnings. *National Security and Strategic Planning* 1(37): 23-28. DOI: https://www.doi.org/10.37468/2307-1400-2022-1-23-28 [Accessed 24 March 2024].

Singh, A. (2016) Spectre of Cyberterrorism: A Potential Threat to India's National Security. *Paripex Indian Journal Of Research* 5(3): 1-8. Available from: https://www.academia.edu/113887228/Cyberterrorism_A_Potential_Threat_to_Indias_National_Security?uc-sb-sw=38260598 [Accessed 24 March 2024].

Al Asyari, H. (2022) The Evolution of Cyberterrorism: Perspectives And Progress From The European Union And Association of Southeast Asian Nation. *Jurnal Hukum Ius Quia Iustum* 29(1): 1-23. DOI: https://www.doi.org/10.20885/iustum.vol29.iss1.art1 [Accessed 24 March 2024].

Grobbelaar, A. (2022) Cyberterrorism In Africa - Exaggerated Threat Or Worthy Foe? *Future, Research, and Expectations in Science, Knowledge, and Aspirations* 1(1): 257-266. DOI: https://doi.org/10.7251/ZNUBL2201257G [Accessed 24 March 2024].

Stafiniak, M. & Wodo, W. (2022) *State-sponsored Cybersecurity Attacks*. 2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University. Riga Technical University, Latvia. 14 November 2022. Available from: https://ieeexplore.ieee.org/document/9937131 [Accessed 23 March 2024].

Courtney, M. (2017) States of cyber warfare. *Engineering & Technology* 12(3): 22-25. Available from: https://ieeexplore.ieee.org/document/7895024 [Accessed 23 March 2024].

Jarvis, L., Macdonald, S. & Nouri, L. (2015) State Cyberterrorism: A Contradiction in Terms? *Journal of Terrorism Research* 6(3): 62-75. Available from: https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1162 [Accessed 23 March 2024].

Martin, J. J. (2020) Hacks Dangerous to Human Life: Using JASTA to Overcome Foreign Sovereign Immunity in State-Sponsored Cyberattack Cases. *Social Science Research Network* 121(1): 119-158. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542617 [Accessed 23 March 2024].

Ray, A. & Kaushik, A. (2017) State transgression on electronic expression: is it for real? *Information and Computer Science* 25(4): 382-401. Available from: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2016-0024/full/html [Accessed 23 March 2024].

Goldsmith, D. & Siegel, M. (2012) *Cyber Politics: Understanding the Use of Social Media for Dissident Movements in an Integrated State Stability Framework*. 2012 IEEE/ACM International Conferences on Advances in Social Networks Analysing and Mining. Istanbul, Turkey. 26-29

August 2012. Available from: https://ieeexplore.ieee.org/document/6425574 [Accessed 24 March 2024].