**Literature Review on State-Sponsored Cyberterrorism in Global Politics**

**Introduction**

This literature review examines the intricacies around the evolving and complex nature of state-sponsored cyberterrorism in relation to the framework of global politics. It examines the transition of cyberterrorism from a threat to it being state-sponsored – whereby states adopt it as a geopolitical tool for proxy warfare, threats and intimidation, or engendering international peace.

The review aims to highlight current policy statements and academic literature on the subject, in addition to generating an overview of what the subject entails. The review stems from insights gained from subject matter experts, industry stakeholders, policy experts, politicians, and academics who have vested interest in the subject matter.

**Aims and Audience**

This review is focused at exploring the many ways in which state-sponsored cyberterrorism is ideated, planned, and executed. It looks at the impact it has on international and intra-national relations, their motivation, and viable methods they adopt in executing these acts of cyberterrorism. This review aims to assess existing scholarly topics and arguments, identify key aspects of the subject matter, and highlighting areas of agreements and disagreements - with a view to adding my contribution to the body of knowledge within the subject matter. Dawson (2005) narrates that literature reviews aid continuity as it provides other researchers a good starting point on what has been left off by previous researchers. I agree with his view as I have used knowledge gained from previous research on the subject to build on mine.

The audience for this literature review will include (but not limited to) policymakers within the political science field, politicians, security experts, students of international relations, lawyers, political enthusiasts, students, and the body of academics. There is existing scholarship on the topic of state-sponsored cyberterrorism with deductions from Lee et al. (2025), Broeders et al. (2023), Gbormittah (2024), Iftikhar (2024), Durojaye and Raji (2024), Hunter et al. (2024), and Azubuike (2023).

**Conceptual Framework**

The review of literature highlights varying concepts relating to state-sponsored cyberterrorism.

* Lee et al. (2025) opined that the concept of state-sponsored cyberterrorism is seen in the prism of a proxy warfare tool. Their concept further adopts a realist view where the warfare is asymmetric – often with the use of non-state actors, and without a direct military engagement.
* Azubuike (2023) conceptualises cyberterrorism within the prism of securitisation, being politically construed to pose existential threat. This is drawn from the securitisation theory of Buzan et al. (1998) which explains how cyber threats are framed to be threats to human existence. Górka (2023) argues for securitisation whereby every public issue of existential threat is treated as a state of emergency – which must be dealt with decisively, and before other issues.
* Broeders et al. (2023) highlights cyberterrorism within the prism of censorship, international norm-setting, and surveillance - all wrapped around international diplomacy. This international diplomatic concept relates particularly to the United Nations Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG). He further argues against enabling ambiguities or vague representations within policy which aid nation-states suppressing dissent, and surveillance justification.
* Gbormittah (2024) systematically looks at cyberterrorism as cyberwarfare and state-sponsored hacking. He further suggested that appropriate emphasis be placed on the use of penetration testing in demystifying threat vectors, threat landscape and the tactics adopted by threat actors.
* Iftikhar (2024) provides an outlook on the impact of cyberterrorism, and offers countermeasures. He highlights the outcomes of cyberterrorism such as political instability, infrastructure disruption, public distrust and many more.
* Hunter et al. (2021) examines the motivations surrounding state-sponsored cyberterrorism with the use of statistical and descriptive analysis.

The common denominator from these literature is that the threat of cyberterrorism is rife, with both state and non-state actors latching onto its efficacy by reason of impact, spread, and seeming loopholes within certain policies. They also suggest that state-sponsored cyberterrorism is not a monolithic concept but hybrid in nature – often aided by strategy, technology, and a contest for existing norms.

**Critical Analysis/Synthesis**

The securitisation theory (Buzan et al., 1998) has been used extensively by industry experts in highlighting the existential threats posed by cyberterrorism. Nyman, (2013) advocates for the legitimisation of exceptional measures of collective actions. This will in turn enable problems to be categorised as being in need of urgent action.

McDonald, (2008) gives some historical intel as to the advent of the securitisation concept whereby its adoption and usage in immigration, health and politics particularly in the context of the post-2001 United States of America (USA) ‘war on terror’. As nation states grappled with the events heralding the September 11, 2001 (9/11) terrorist attack, it became imperative that terror was no longer a mirage, but an existential threat. Threat actors (either as nation states or non-state actors) became emboldened to its efficacy and sought to introducing and deploying cyberterrorism on a large scale to threatening others, or for political gains.

As conflicts have become almost a norm among nation states, the use of cyber-terrorism is becoming increasingly used as a vital tool in international conflict (Azubuike, 2023). This is also an argument posited by the Center for Strategic and International Studies (CSIS) who have provided some statistics to the incidents of cyberterrorism. They postulate that state-sponsored cyber-terrorism has increased by 65% over the last 5 years, with China, Russia, Iran, and North Korea as major culprits (CSIS, 2025). For example, the 2016 Russian interference in the United States presidential election and the recent Solar Winds cyberattack have underscored the potential impact of state-sponsored cyberattacks on democratic institutions and its impact on international relations (Janczewski and Colarik, 2017).

Beijing (Chine) sees the adoption of “informatisation of warfare” as critical to their sustainability (Pusztaszeri, *et al.* 2025). With China building its military as an ‘informationised military’ fully equipped to win ‘future informationised wars’ (Pusztaszeri, *et al.* 2025). This would seem that Beijing is adequately prepared to using the many tools available on the cyber space in gaining an edge on the international conflict stage.

The power dynamics among nation states is beginning to shift, with those wielding enormous cyber capabilities seen as big power players in the committee of nations. This is an argument espoused by Arquilla (2017) and further corroborated by Krekel *et al.* (2021) saying that the line of traditional warfare and cyber conflict have been blurred, forcing nations to adapt their strategies and alliances. In this battle of supremacy, any nation who does not ally with those wielding cyber power are literally trampled on during times of conflict. This is an argument I align with, as this portrays why many nations form alliances/blocks so they can be shielded from enemy attack. For example, the North Atlantic Treaty Organisation (NATO) paints a picture of alliances among nations. However, this does not prevent nations from carrying out cyber-attacks on others, but they mostly execute them subtly, with traceability not explicitly linked to an individual state.

The motivations of state-sponsored cyberterrorism is majorly to gain advantage over other countries within the international space. Additionally, Azubuike (2023) mentions that an intention to destabilise and undermine the security of the other nation is at the heart of the motivations of state-sponsored cyber terrorism. Election manipulation, damage to critical assets/infrastructure, espionage, theft of sensitive data are mostly deployed by attacking nations on victim nations.

Janczewski and Colarik, (2017) posit that nation states often adopt subtlety, deniability, and deception so not to be directly linked to the attack, and will often use third party actors, hacktivists, syndicates, and criminal elements to perpetrate their heinous crime. This further scuttles prosecution as it becomes difficult to apply legal, military, and diplomatic consequences on them.

**Evaluation of Methodology**

|  |  |  |
| --- | --- | --- |
| Study/Paper | Methodology | Key Strength |
| Hunters *et al*. (2021) | Quantitative and Descriptive Analysis | The adoption of statistical modelling which correlates power and the type of regime/administration with cyberterrorism or aggression. |
| Gbormittah, (2024); Iftikhar, (2024) | Systematic Literature Review | Consolidation of technical and geopolitical insights. |
| Azubuike (2023) | Content Analysis | Placing a premium on policy evaluation through an emphasis on securitisation theory. |
| Durojaye and Raji (2024); Iftikhar, (2024) | Survey and Case Study Analysis | Adoption of case studies in demystifying cyber-kinetic warfare. Examples of the Stuxnet and SolarWinds exemplify the core problems of state-sponsored cyberterrorism. |
| Broeders *et al*. (2023) | Discourse Analysis | Exploration of cyberterrorism and its framing in policy and law. It takes a cursory look at risk of vague definitions within global governance. |
| Lee et al. (2025) | Comparative Case Studies | The application of multi-theoretical analysis to the theories of realism and proxy warfare. |

These methodologies depict the very nature of cyberterrorism, being dynamic and evolving. The diversity in methodology suggests cyberterrorism being multi-disciplinary, and reveals breakups in data sources and analysis.

**Current Knowledge Overview**

State sponsored cyberterrorism is in a hybrid form which blends stealth operations, ideological warfare, and digital disruption. The various authors have shown knowledge in the subject in the context of its motivations, operational tactics, norms, legalities, and attribution.

Nation states adopt cyberterrorism being motivated by its potency to deter other nations or cause disruptions (Azubuike, 2023; Hunter et al., 2021). Additionally, Lee et al (2025) posit that nations who engage in cyberterrorism with others do so for proxy warfare and to align ideologically. Furthermore, they also engage in the act to change/preserve regime or gain domestic control (Broeders et al., 2023; Iftikhar, 2024).

Broeders *et al*. (2023) argues against vague definitions within policy, and that a consensus needs to be agreed on standard operating procedures. The vagueness in policies pose a risk for authoritarianism and the misuse of counterterrorism (Broeders et al., 2023; Iftikhar, 2024). Additionally, the legal framework across national boundaries to curtail the menace of state-sponsored cyberterrorism are inadequate (Iftikhar, 2024).

In terms of operational tactics, nation states adopt the use of Advanced Persistent Threats (APTs) and deploy malware to attack others (Gbormittah, 2024). The Stuxnet attack of 2010 is an example of cyber-worm deployed which affected the Iranian nuclear facility, infecting over 60,000 computers, and affecting countries like India, Indonesia, China, South Korea, Malaysia, United Kingdom, and the United States (Farwell and Rohozinski, 2011). The SolarWinds attack which started in 2020 affected more than 300,000 customers worldwide, with the United States being majorly impacted, and Russia suspected to be the perpetrator (Tran, 2021).

These attacks mainly focus on state infrastructures such as energy grid, hospitals, network installations and so on (Durojaye and Raji, 2024). Often exploiting zero-day vulnerabilities and social engineering (Iftikhar, 2024), and needing penetration testing insights regarding attack vectors (Gbormittah, 2024).

State sponsored cyberterrorism is attributed to be difficult to trace to the actual state who has perpetrated the terror (Hunter et al. 2021; Broeders et al. 2023), as these perpetrators adopt the use of proxies, third parties and false flags (Lee *et al*. 2025).

**Gaps**

As the scholarship on this subject is vast and growing, there still remain some gaps which in my opinion need to be addressed in support of the battle against state sponsored cyberterrorism.

One of such gap is the limited integration of cyber threat intelligence with geopolitical analysis (Gbormittah, 2024; Hunter et al. 2021). The synergy and handshake between nations in integrating intelligence is inadequate. Additionally, the role the private sector plays in the complicity is not properly studied. What is the level of involvement of the private sector technological firms in acting as enablers to these terror attacks? Furthermore, there is underrepresentation within Africa, Latin America, and the Southeast Asia on providing local intelligence to combating the menage (Iftikhar, 2024). Lastly, there needs to be a deep-dive on how cyberattacks translate into physical consequences (Azubuike, 2023; Gbormittah, 2024).

The resolution of these gaps will provide an opportunity to developing international norms, safeguarding digital rights, and putting in place standards to institute harmonious coexistence.

**Conclusion**

State sponsored cyberterrorism is multi-pronged, offering a hybrid approach which intersects global security, cyber administration/governance, and the normal practice of politics. Insights into strategy, operations, methodology have been garnered from the reviewed literature. This has provided knowledge on the tactics and methodology adopted.

It is therefore pertinent for policy makers to eschew ambiguity, uphold human rights in this digital age, and promote fairness within international relations. Future research should bridge any existing gaps, expand on the current knowledge, develop opportunities on regional case studies, and critically examine the role of the private sector (especially technology companies) in the menace of state-sponsored cyberterrorism.

**Reference**

Azubuike, C. (2023). *Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks*. Nnamdi Azikiwe Journal of Political Science, 8(3), pp.101–114.

Broeders, D. *et al.* (2023). *Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy*. Studies in Conflict & Terroris, 46(12), pp.2426–2453.

Buzan, B. *et al.* (1998). *Security: Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers.

Dawson, C. (2005). *Projects in computing and information systems: a student's guide*. Harlow: Pearson Education.

Durojaye, H. and Raji, O. (2024). *Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure*. Bournemouth University Research Paper.

Farwell, J. and Rohozinski, R., (2011). *Stuxnet and the future of cyber war*. Survival, 53(1), pp.23-40.

Gbormittah, E. (2024). *A Systematic Literature Review on Cyberwarfare and State-Sponsored Hacking: Penetration Testing Insights*. TechRxiv, [online] Available at: https://doi.org/10.36227/techrxiv.172373675.55159205/v1

Górka, M. (2023). *Conceptualising securitisation in the field of cyber security policy*. Journal of Modern Science, 53(4), pp.263-290.

Hunter, L. *et al*. (2021). *Factors That Motivate State-Sponsored Cyberattacks*. Cyber Defence Review, Spring 2021, pp.111–126.

Iftikhar, S. (2024). *Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures*. PeerJ Computer Science, 10:e1772. Available at: <https://doi.org/10.7717/peerj-cs.1772>

Janczewski, L. and Colarik, A. (2017). *Cyber Warfare and Cyber Terrorism*. Springer.

Lee, B. *et al*. (2025). *State Sponsored Terrorism as a Tool for Proxy War*. Journal of Terrorism Studies, 7(1), pp.1–17.

McDonald, M. (2008). *Securitization and the Construction of Security.* European journal of international relations, 14(4), pp.563-587.

Nyman, J. (2013). *Securitization theory. In Critical approaches to security* (pp. 51-62). Routledge.

Pusztaszeri, A. *et al.* (2025). *A Playbook for Winning the Cyber War*. Center for Strategic and International Studies.

Tran, C. (2021). *The SolarWinds attack and its lessons*. E-International Relations.