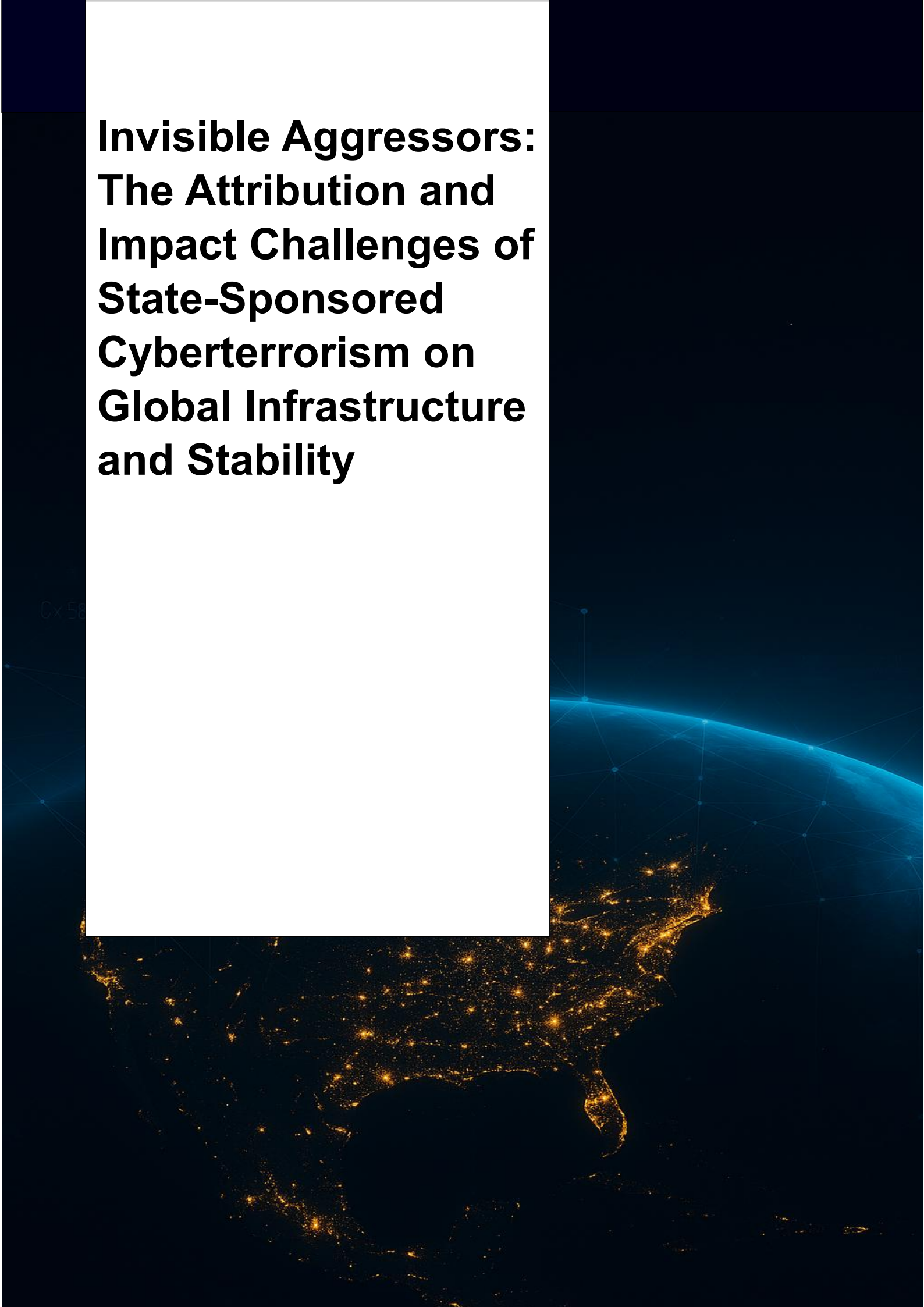
Invisible Aggressors: The Attribution and Impact Challenges of State-Sponsored Cyberterrorism on Global Infrastructure and Stability



Introduction

Nation-states use cyberterrorism to pursue strategic goals without open conflict. Unlike visible and attributable conventional terrorism, it operates through covert digital disruptions that can destabilise infrastructure and public trust (Campbell, 2022; Veerasamy, 2014). The WannaCry and SolarWinds incidents caused significant damage despite lacking definitive proof of state involvement (Henrico & Els, 2025; Iftikhar, 2024). These cases hinder law enforcement, reduce accountability, and complicate international cybersecurity efforts.

This review examines state-sponsored cyberterrorism, exploring conceptual ambiguity, attribution challenges, and infrastructure targeting and considers the broader implications for international security.

The central research question guiding this review is: What challenges does state-sponsored cyberterrorism pose to attribution, critical infrastructure security, and international stability?

Conceptual and Definitional Ambiguity

A significant difficulty in dealing with state-sponsored cyberterrorism is the lack of a single, widely accepted definition. Researchers differ in interpreting acts' purpose, techniques, and consequences (Iftikhar, 2024; Veerasamy, 2014). While conventional terrorism usually involves physical violence and clear political aims, cyberterrorism takes place through digital systems and may not cause immediate or visible damage. This divergence complicates both legal classification and the formulation of coherent policy responses (Banks, 2018; Hosford, 2025).

Veerasamy (2014) offers a structured cyberterrorism life cycle model, mapping the trajectory from ideological motivation to technical execution. However, this framework does not resolve deeper definitional inconsistencies. Campbell (2022) observes that law enforcement and academic discussions often conflate cyberterrorism with cybercrime, especially when incidents involve ransomware or data theft. Radoniewicz (2021) and Montsari (2023) both argue that this definitional instability allows the term "cyberterrorism" to be politicised, shaping legal and policy responses in ways that may prioritise state interests over clarity and accountability. The overlap is further complicated when protest-driven cyber actions, like hacktivism, cause public disruption or fear yet do not meet terrorism thresholds (Hosford, 2025).

The concept of state sponsorship introduces additional ambiguity. Some scholars define it narrowly as direct government control or funding, while others include indirect support, proxy networks, or state tolerance (Maurer, 2021). Iftikhar (2024) attempts to clarify this by identifying intent to destabilise as a key indicator, but the literature remains inconsistent. Henrico and Els (2025) argue that without precise legal language, states can deny involvement and exploit the lack of accountability.

There is also conceptual divergence in how harm is defined. Legal and technical studies focus on measurable outcomes like infrastructure failure but often overlook broader social impacts such as fear or instability (Islam et al. 2025). Ignoring these aspects can distort how threats are evaluated and may downplay the full scope of harm caused by state-connected cyber incidents.

Without a standard definition, aligning research and coordinating legal responses is challenging. A lack of a shared understanding of cyberterrorism and state sponsorship hampers effective regulation and response efforts.

Attribution Challenges

Attributing cyberattacks to state actors is one of the most persistent and complex challenges in cyberterrorism. The internet's technical design allows attackers to hide their identities, reroute traffic through multiple jurisdictions, and mimic the behaviours of other groups (Folkes, 2025; Veerasamy, 2014). Such deception allows states to act disruptively while maintaining plausible deniability, complicating legal responsibility and international responses (Iftikhar, 2024; Torres, 2024).

Veerasamy (2014) notes that attribution is critical in the cyberterrorism life cycle but acknowledges that anonymising tools and proxy networks significantly limit conclusive identification. Iftikhar (2024) highlights that despite strong circumstantial evidence in incidents like SolarWinds and WannaCry, states often avoid formal attribution due to high international evidentiary standards. Even when attribution is attempted, it is frequently contested, politicised, or withheld to avoid escalation (Maurer, 2021; Torres, 2024). Tsagourias and Farrell (2020) further argue that legal and technical attribution efforts lack uniform standards, leaving states free to frame attribution in ways that serve strategic goals rather than international consistency.

Henrico and Els (2025) examine this issue in South Africa, where legal frameworks lack mechanisms for pursuing foreign-based perpetrators. More broadly, legal systems typically require proof of intent and direct control, which is rarely available in digital operations. As a result, prosecutions are infrequent, and international accountability mechanisms remain weak. The paper also highlights a serious gap between technical detection and legal enforcement, particularly within international law frameworks that demand strong evidence.

Governments often assess political risk before publicly attributing cyberattacks. Torres (2024) explains that officials may deliberately avoid assigning blame to prevent diplomatic fallout or escalation when a suspected attacker is a powerful state. Conversely, ambiguous threats may be amplified or leveraged to justify domestic surveillance expansion or defence spending, irrespective of evidentiary clarity (Snider et al. 2025).

Efforts to close attribution gaps are still limited. Folkes (2025), in a Delphi study of cybersecurity experts, emphasises the lack of cooperation between public and private sectors in forensic analysis and intelligence sharing. Private companies often possess critical evidence but are reluctant to share it due to legal, security, and confidentiality concerns. This lack of transparency undermines effective attribution, making it harder to hold perpetrators accountable or prevent similar incidents.

This ambiguity lets hostile states act aggressively without facing direct consequences. Without stronger attribution, cyberterrorism remains a low-risk asymmetric tool (Vostoupal & Uhlířová, 2024).

Attacks on Critical Infrastructure

State-sponsored cyberterrorism often targets critical infrastructure because of its societal importance and the widespread disruption such attacks can cause. Sectors like energy, healthcare, and finance depend heavily on digital systems, making them particularly vulnerable to cascading failures (Iftikhar, 2024; Suorsa & Helo, 2025). These operations allow states to exert pressure or destabilise rivals while avoiding direct military confrontation, often staying below the threshold of armed conflict (Torres, 2024).

Iftikhar (2024) identifies healthcare, energy, and transport systems as common targets for politically motivated cyber actors. The WannaCry and SolarWinds attacks caused significant disruption to public and governmental services. Although conclusive attribution is lacking, many experts suggest these operations were state-backed. They illustrate how cyberattacks can apply pressure and cause instability without triggering traditional conflict. The energy sector has become a particularly strategic vulnerability. Suorsa and Helo (2025), in a case study of a European energy provider, show that state-linked attacks on operational systems can severely affect national supply chains. They argue that current risk-mapping tools often fall short of addressing the advanced tactics used by state-backed attackers. The EU's NIS2 Directive aims to strengthen resilience, but inconsistent implementation among member states reduces its effectiveness. Helyes (2021) notes that fragmented legal protections, especially in cross-border cases, leave critical infrastructure vulnerable as reliance on digital technologies increases.

Torres (2024) frames these attacks as instruments of indirect digital warfare used to destabilise adversaries without provoking an open military response. The strategic ambiguity of such incidents allows state actors to test systems, intimidate rivals, or undermine political confidence while avoiding direct accountability. Snider et al. (2025) further observe that cyberattacks on infrastructure often heighten public anxiety and increase support for expanded surveillance powers, outcomes that may serve aggressor interests.

Henrico and Els (2025) note that legal systems in regions like South Africa lack adequate tools to respond to cross-border attacks on infrastructure, leaving critical systems exposed. Even with regulations, enforcement is hindered by political and resource limits.

Despite their high impact, responses to infrastructure-targeted cyberterrorism remain fragmented and primarily national. Without international norms, infrastructure remains vulnerable.

Implications for International Stability

Cyberterrorism backed by nation-states quietly reshapes global security (Torres, 2024). It weakens trust between governments (Iftikhar, 2024), exposes loopholes in international law (Henrico & Els, 2025), and challenges long-standing expectations about how states should behave. These covert tactics bypass traditional military responses and erode governance (Torres, 2024).

Mott (2018) explains that some governments talk about cyberterrorism in ways that help them gain support for new surveillance laws or political action. This can distract from fundamental system flaws and complicate questioning or limiting those powers.

Henrico and Els (2025) argue that international legal frameworks cannot address state-linked cyber aggression. Instruments like the Budapest Convention address cybercrime broadly but lack provisions specific to cyberterrorism or state sponsorship (Alkharman & Hassan, 2023). Masyhar et al. (2023) highlight that legal systems often fail to align domestic law with international enforcement standards, undermining coordinated responses. These limitations are especially pronounced in Global South countries, where institutional and legal capacity gaps further weaken accountability (Henrico & Els, 2025). Karakhodjayeva (2023) also emphasises the need for harmonised legal frameworks, noting that state accountability in cyberspace remains fragmented, particularly as AI-driven threats complicate regulation.

Torres (2024) describes cyberterrorism as a form of asymmetrical statecraft that relies on digital operations to destabilise rivals while avoiding direct military

confrontation. The lack of clear attribution enables covert interference and allows states to evade responsibility, which fuels global uncertainty and makes coordinated responses more difficult. Differing definitions and policies lead to inconsistent threat handling, raising the risk of overreaction and escalation. According to Iftikhar (2024), many decisions reflect national agendas more than international agreements, making coordinated action much harder. This mismatch makes it difficult to coordinate across borders and reduces the strength of legal protections that should help prevent these kinds of attacks. According to Snider et al. (2025), countries use cyberattacks to justify new surveillance powers and cybersecurity laws, often with little public input. While these policies may enhance defence, they risk concentrating state power and undermining democratic freedoms (Maurer 2021; Torres 2024; Snider et al. 2025).

Efforts to strengthen international collaboration remain uneven. Folkes (2025), through a Delphi study, identifies expert consensus on the need for shared attribution protocols, coordinated response strategies, and cross-sector engagement. Still, progress is slow. Mistrust and national agendas often hinder collaboration. As a result, cyberattacks backed by governments continue to cause problems that law and diplomacy cannot keep up with. Without enforceable global rules, the internet will remain a space where powerful actors operate without consequence.

Gaps and Future Directions

Although research on state-sponsored cyberterrorism is expanding, the literature remains fragmented and marked by several important gaps. A core barrier is the persistent lack of definitional clarity across academic and legal contexts. The idea of state involvement is also unclear.

Some governments fund attacks directly, while others look the other way. Ambiguity hampers research, policy, and accountability (Henrico & Els, 2025; Iftikhar, 2024).

Attribution remains a significant challenge. Despite expert consensus, few practical solutions exist. Folkes (2025) notes that progress is slow partly because public and private groups do not always work together. On top of that, there are no shared systems to guide investigations or handle digital evidence consistently. If the way that data is collected and stored is unclear, it may not meet the standards needed in legal proceedings. This makes it harder to hold attackers accountable and slows down international cooperation.

The literature also reflects a geographical imbalance. Much of the research focuses on attacks and policies in the Global North, particularly Europe and the United States. As Henrico and Els (2025) illustrate, countries in the Global South face different legal, institutional, and infrastructural challenges that remain underexplored. This skew limits the global applicability of current findings and overlooks important variations in threat exposure and response capacity. Qudus (2025) and Yongsheng et al. (2024) argue that international cyber governance frameworks often reflect Global North priorities, leaving countries in the Global South with limited legal protections, technical support, and policymaking influence. Legal and governance gaps are also apparent. Although instruments like the Tallinn Manual and Budapest Convention offer normative guidance, they lack binding force and remain inconsistently adopted (Karakhodjayeva, 2023). Agreement on cyber accountability is limited.

Many studies explore state-sponsored cyberterrorism from a single perspective, such as law, technology, or politics, which restricts a comprehensive understanding

of the issue. Future research should take a more integrated approach to address the complexity of these threats better. It should also include core procedural elements for reliable digital investigations, such as continuity, chain of custody, and the credibility of evidence.

In addition, the literature has yet to fully explore how emerging technologies like generative AI and deepfakes may complicate attribution and escalate cyberterrorist strategies. The growing realism of synthetic content produced by generative adversarial networks (GANs) and diffusion models presents serious challenges for detection and verification (Amerini et al. 2025). Attribution becomes even more difficult when deepfake content cannot be reliably linked to specific generative models or actors (Khoo et al. 2021). Paterson (2024) notes that without coordinated frameworks between states and technology platforms, AI-driven threats are likely to outpace existing policy and regulatory mechanisms (Paterson, 2024). Even though these risks exist, there are no clear international guidelines for responding to or escalating cyber conflicts. In contrast, threats like nuclear or biological weapons are governed by established global norms. Addressing these challenges will require renewed research, more substantial political commitment, and greater international cooperation.

Conclusion

This review examined how definitional ambiguity, attribution difficulties, and infrastructure vulnerabilities limit effective responses to state-sponsored cyberterrorism. These problems make it more challenging to hold actors accountable and to build cooperation across borders. As these threats become more common, responses often remain slow and uncoordinated. A unified, cross-sectoral strategy

grounded in shared definitions, reliable attribution, and enforceable legal standards is essential to shift from reactive containment to proactive international resilience.

References List

Alkharman, J. A. & Hassan, I. (2023) Cyberterrorism and Self-Defense in the Framework of International Law. *Journal of Law and Sustainable Development* 11(8): 1-21. DOI: https://doi.org/10.55908/sdgs.v11i8

Amerini, I. (2025) Deepfake Media Forensics: Status and Future Challenges. *Journal of Imaging* 11(73): 1-42. DOI: https://doi.org/10.3390/jimaging11030073

Banks, W. (2018) Who Did It? Attribution of Cyber Intrusions and the Jus in Bello. *The Impact of Emerging Technologies on the Law of Armed Conflict*. DOI: https://doi.org/10.1093/oso/9780190915322.003.0009

Campbell, M. (2022) *Cybercrime and Its Relation to Cyberterrorism.* Unpublished MSc capstone project. Utica University. Available from: https://www.proquest.com/openview/bb5f49b149c574398facaa9decc18a9c/1?pq-origsite=gscholar&cbl=18750&diss=y [Accessed 10 May 2025].

Folkes, C.P.L. (2025) *Level of consensus for a forward-thinking cybersecurity model.* Doctoral dissertation. Purdue University Global. Available from*:* https://scholarworks.waldenu.edu/dissertations/17435/ [Accessed 11 May 2025].

Iftikhar, S. (2024) Cyberterrorism as a global threat: a review on repercussions and countermeasures*. PeerJ Compututer Science*. 10:e1772 DOI: http://doi.org/10.7717/peerj-cs.1772

Islam, E., Rudolph, C. & Oliver, G. (2025) Managing cyber harm: a survey of challenges, practices, and opportunities. *Information Security Journal: A Global Perspective.* DOI: https://doi.org/10.1080/19393555.2025.2484348

Helyes, M. (2021) Cyberterrorism and the protection of critical information infrastructures: A snapshot of the current state of certain regulatory issues. *Lélektan és hadviselés 3*(1): 51-68. https://doi.org/10.35404/lh.2021.1.51.

Henrico, S. & Els, S. (2025) Cyber Attacks in South Africa: Geopolitical and legal implications. *African Security Review*. DOI: https://doi.org/10.1080/10246029.2025.2489352

Hosford, K. (2025) Charting the scholarly waters of cyberterrorism and hacktivism research: A bibliometric analysis of academic output (2000–2020). *Information Security Journal: A Global Perspective.* DOI: https://doi.org/10.1080/19393555.2025.2459741

Karakhodjayeva, S. (2023) Navigating State Accountability in Cyberspace: Balancing Cyber-security, Artificial Intelligence, and Data Protection Conflict of Laws. *Uzbek Journal of Law and Digital Policy*. DOI: https://doi.org/10.59022/ujldp.64

Khoo, B., Phan, R.C.-W. & Lim, C.-H. (2021) Deepfake attribution: On the source identification of artificially generated images. *Wires Data Mining and Knowledge Discovery* 12(3): 1-21. DOI: https://doi.org/10.1002/widm.1438

Masyhar, A., Utari, I., Usman, U. & Sabri, A. (2023) Legal challenges of combating international cyberterrorism: the NCB Interpol Indonesia and global cooperation. *Uzbek Journal of Law and Digital Policy* 1(1): 1-11. DOI: https://doi.org/10.22219/ljih.v31i2.29668.

Maurer, T. (2021) States, Proxies, and (Remote) Offensive Cyber Operations. *The Oxford Handbook of Cyber Security*. DOI: https://doi.org/10.1093/oxfordhb/9780198800682.013.35

Montsari, R. (2023) *Countering Cyberterrorism. The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity.* Advances in Information Security. DOI: https://doi.org/10.1007/978-3-031-21920-7

Mott, G. (2018) *A Critical Reflection on the Construction of the Cyberterrorist Threat in the United Kingdom of Great Britain and Northern Ireland.* PhD thesis. Nottingham Trent University. Available from: https://irep.ntu.ac.uk/id/eprint/34122/ [Accessed 12 May 2025].

Paterson, M.J. (2024) 'AI deepfakes on the web: The wicked challenges for AI ethics', *The Web Conference 2024*. Singapore, 13–17 May. New York: Association for Computing Machinery. 4396-4406.

Qudus, L. (2025) Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges*. International Journal of Science and Research Archive* 14(1): 1146-1163. DOI: https://doi.org/10.30574/ijsra.2025.14.1.0225

Radoniewicz, F. (2021) 'Cyberspace, Cybercrime, Cyberterrorism', in: J. Kosiński (ed.) *Cybersecurity in Poland*. Cham: Springer. 33-53.

Snider, G.L.K., Hefetz, A., Shandler, R. & Canetti, D. (2025) Experimenting with Threat: How Cyberterrorism Targeting Critical Infrastructure Influences Support for Surveillance Policies, Terrorism and Political Violence. *Terrorism and Political Violence* 37. DOI: https://doi.org/10.1080/09546553.2025.2457746

Suorsa, M. & Helo, P. (2025) Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis. *Information Security Journal: A Global Perspective.* DOI: https://doi.org/10.1080/19393555.2025.2489421

Torres, K.A. (2024) *Assessing the New Type of Cyberwar: A Qualitative Exploratory Study of Technology Dependence Facilitating the Current Rise of Cyberterrorism.* PhD thesis. Colorado Technical University. Available from: https://www.proquest.com/openview/d2698fc7e46973464792f1a2f2467c96/1?pq-origsite=gscholar&cbl=18750&diss=y [Accessed 10 May 2025].

Tsagourias, N. & Farrell, M. (2020) Cyber attribution: technical and legal approaches and challenges. *European Journal of International Law* 31(3): 941-967. DOI: https://doi.org/10.1093/ejil/chaa057

Veerasamy, N. (2014) *CLC – Cyberterrorism Life Cycle Model.* PhD thesis. University of Johannesburg. Available from: https://www.proquest.com/openview/146ff232088b1e226620328581d0ef57/1?pq-origsite=gscholar&cbl=2026366&diss=y [Accessed 10 May 2025].

Vostoupal, J. & Uhlířová, K. (2024) Of Hackers and Privateers: The Possible Evolution of the Problem of Cyber-Attribution. *Masaryk University Journal of Law and Technology* 18(2): 169-214. DOI: https://doi.org/10.5817/MUJLT2024-2-2

Yongsheng, G., Isnaini. & Frensh, W. (2024) International Cyber Governance: Strategies And Practices Against Cybercrime. *ARBITER: Jurnal Ilmiah Magister Hukum* 6(2): 276-286. DOI: https://dx.doi.org/10.31289/arbiter.v6i2.5095