ISSN (E) 3007-0376
ISSN (P) 3007-0368

Journal of Advanced Studies in Social Sciences (JASSS)

Vol.4, Issue 1 (January-June 2026)

Academy of Social Sciences
BAHISEEN Institute for Research & Digital Transformation
Street 14-G, Coral Town, Islamabad
Email: editor@jasss.pk, Website: https://jasss.pk

The Impact of the Cyber Crime Act, 2025, on Zambian Critical Information Infrastructure: A Scenario – Based Risk Assessment and Mitigation Framework

Towani Kawonga
School of Business and Information Technology, Texila American University - Zambia
Email: kawongatowani@gmail.com
Jacqueline Siwale
School of Business and Information Technology, Texila American University - Zambia
Email: jacquelinesiwale@gmail.com
Harrison Kalenga
School of Business and Information Technology, Texila American University - Zambia
Email: harrisonkalenga@gmail.com
Angelo Salasini
School of Business and Information Technology, Texila American University - Zambia
Email: angelosalasini8@gmail.com
Ulayi Owen
School of Business and Information Technology, Texila American University - Zambia
Email: ulayi.shiku@gmail.com
Olivier Gatete
School of Medicine, Texila American University-Zambia
Email: gatete10@gmail.com
DOI: https://doi.org/10.5281/zenodo.20780754

Abstract

The enactment of the Cyber Crime Act, 2025, represents a significant evolution in Zambia's legal framework for combating cyber threats. However, its specific implications for the protection of Critical Information Infrastructure (CII) remain unexplored. This paper presents a novel, scenario-based risk assessment framework to evaluate the impact of the new Act on Zambian CII sectors, including energy, finance, and telecommunications. The methodology involves a detailed analysis of the Act's provisions, the identification of key CII assets, and the development of plausible attack scenarios (e.g., ransomware attacks on the national power grid, SWIFT system compromises) to stress-test the regulatory environment. Our findings indicate that while the Act provides crucial legal tools for prosecution and information sharing, it introduces significant compliance burdens and potential operational complexities for CII operators. The study identifies critical gaps in incident response coordination and resource allocation. We propose a structured mitigation framework that integrates technical controls, governance policies, and public-private partnerships to enhance CII resilience. This research provides policymakers, regulators, and CII operators in Zambia with a proactive tool for navigating the new legislative landscape, ultimately contributing to greater national cybersecurity resilience.

Keywords: Cyber Crime Act 2025, Risk Assessment, Scenario-Based Analysis, Mitigation Framework, Zambia

1.0 INTRODUCTION

The digital transformation of national economies has inextricably linked national security and economic prosperity to the resilience of Critical Information Infrastructure (CII) [1]. In Zambia, sectors such as energy, finance, water, and telecommunications increasingly rely on interconnected digital systems, making them potential targets for sophisticated cyber-attacks [2]. Recognizing this threat, the Zambian government has undertaken substantial legislative reforms, beginning with the Cyber Security and Cyber Crimes Act No. 2 of 2021 and the Data Protection Act No. 3 of 2021 [3], [4]. The recent promulgation of the Cyber Crime Act, 2025, aims to further strengthen this legal arsenal by addressing emerging threats and harmonizing with international best practices [5].

While the introduction of the Cyber Crime Act, 2025, is a commendable step, its practical impact on the security posture of Zambian CII is not yet understood. Legislation can have dual effects: it can mandate necessary security measures and foster collaboration, but it can also create compliance overhead, vague liability standards, and operational challenges that may inadvertently weaken security if not implemented carefully [6], [7]. Existing research on Zambian cyber law has focused on the 2021 Acts [8], [30], but a dedicated study on the intersection of the new 2025 Act and CII protection is absent.

This paper addresses this gap by posing the following research questions:

i. What are the specific obligations and implications for Zambian CII operators under the Cyber Crime Act, 2025?
ii. What are the most critical risk scenarios facing Zambian CII in the context of this new legal regime?
iii. What mitigation strategies can be developed to enhance CII resilience while ensuring compliance?

To answer these questions, we develop and apply a scenario – based risk assessment framework. This approach moves beyond theoretical analysis to model real – world attack vectors, providing a pragmatic view of systemic vulnerabilities [9], [10]. The primary contribution of this work is a structured, actionable framework that enables Zambian stakeholders to proactively identify, assess, and mitigate risks to CII within the new legal environment established by the Cyber Crime Act, 2025.

The remainder of this paper is structured as follows; Section II reviews related work. Section III details the materials and methods. Section IV presents and discusses the results of the scenario analysis. Section V concludes the paper and suggests future research directions.

2.0 RELATED WORKS

This research sits at the intersection of cyber law, Critical Information Infrastructure Protection (CIIP), and risk assessment methodologies. The related literature is reviewed under these three themes.

a. Critical Information Infrastructure Protection (CIIP) Frameworks

Globally, the protection of CII is guided by established frameworks. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 provides a widely adopted voluntary framework for managing cybersecurity risk, emphasizing governance and supply chain security [11]. Similarly, the European Union Agency for Cybersecurity (ENISA) offers methodologies for identifying CII and managing cross-border risks [12], [8]. Theoharidou and Gritzalis [7] provide a comprehensive analysis of risk-based approaches to CIIP, arguing that a one-size-fits-all model is ineffective. In the African context, the

Southern African Development Community (SADC) has developed a Regional Critical Infrastructure Protection Programme Framework [13], and countries like Ghana [33] and South Africa [35] have advanced their own CII directives, offering valuable comparative case studies for Zambia.

b. Cyber Law and its Impact on CII

The relationship between legislation and CII security is complex. Muthuri and Kabanda [29] conducted a comparative analysis of cybercrime laws in the SADC region, highlighting disparities in legal definitions and enforcement capacities. Research by Chewe [30] on Zambia's earlier cyber laws pointed to challenges in implementation and capacity building. A key area of concern in legislation is the concept of intermediary liability and "duty of care" for service providers, which can impact how CII operators manage their networks [6]. Lewis [14] emphasizes that effective CIIP legislation must facilitate, not hinder, information sharing between the public and private sectors.

c. Scenario – Based Risk Assessment Methodologies

Traditional risk assessment methods are often static. Scenario-based planning and wargaming have emerged as dynamic alternatives for understanding complex cyber threats [9], [15]. Axelrod [16] demonstrates the utility of simulation for researching cyber conflict dynamics. Carin et al. [10] advanced cyber threat scenario modeling specifically for CII, focusing on cascading effects. In the African context, Tuyikeze and Abrahams [24] explored the application of attack graphs for proactive defense, underscoring the relevance of these techniques to the region's unique challenges.

While these works provide a strong foundation, none have applied a scenario-based methodology to analyze the impact of Zambia's specific and newly enacted Cyber Crime Act, 2025, on its CII. This paper seeks to fill this niche.

3.0 METHODS

This study employed a qualitative, scenario-based risk assessment methodology, structured in four phases, as illustrated in Fig. 1.

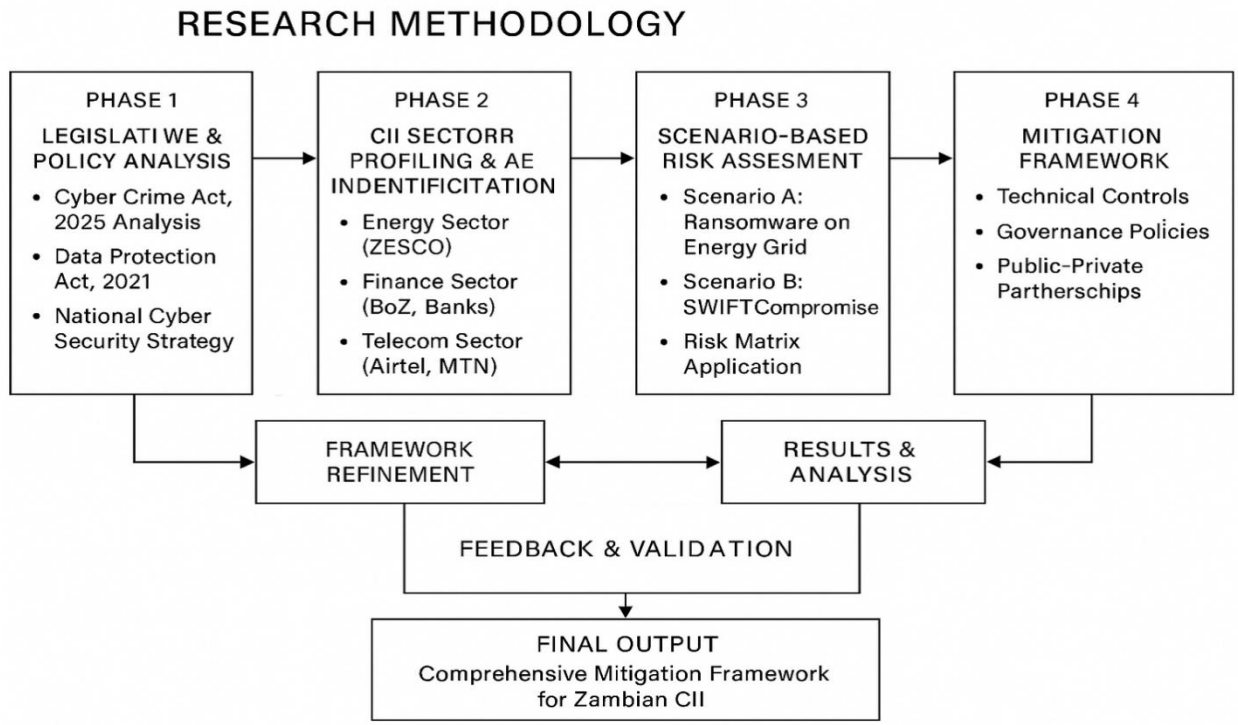

Figure 1: Research Methodology Flowchart (Phases 1-4)

a. Phase One, Legislative and Policy Analysis

The first phase involved a detailed document analysis of the primary legal texts governing cybersecurity in Zambia: the Cyber Security and Cyber Crimes Act No. 2 of 2021 [3], the Data Protection Act No. 3 of 2021 [4], the National Cyber Security Strategy (2024-2028) [2], and the seminal text for this study, the Cyber Crime Act, 2025 [5]. The analysis focused on extracting provisions directly relevant to CII operators, such as: Definitions of Critical Information Infrastructure. Mandatory security obligations and reporting requirements (e.g., for data breaches or significant cyber incidents). Powers granted to regulatory bodies like ZICTA, Liability and penalty clauses for non-compliance.

b. Phase Two, CII Sector Profiling and Asset Identification

Based on the Zambian National Critical Information Infrastructure Policy Framework [31] and global standards [12], key CII sectors were selected for focus: Energy (e.g., ZESCO's grid control systems), Finance (e.g., Bank of Zambia's payment systems, commercial bank networks), and Telecommunications (e.g., core network infrastructure of major providers). For each sector, critical assets were identified through a review of public infrastructure reports and sector-specific guidelines, such as those from the Bank of Zambia [32].

c. Phase Three, Scenario Development and Risk Analysis

This core phase involved developing three high – impact, plausible attack scenarios designed to stress-test the legal and operational framework:

i. Scenario A (Energy Sector), a sophisticated ransomware attack encrypts the control systems of a major power generation facility, causing a multi-day regional blackout.
ii. Scenario B (Finance Sector), a coordinated SWIFT system compromise targets a major Zambian commercial bank, leading to fraudulent high-value international transfers.
iii. Scenario C (Telecommunications Sector), a state – sponsored DDoS attack disrupts a major mobile network operator's core system, affecting national communications.

For each scenario, we conducted a structured analysis using a risk matrix based on likelihood and impact [7]. The analysis evaluated the scenario's implications before and after the implementation of the Cyber Crime Act, 2025, focusing on legal preparedness, incident response coordination, and attribution capabilities.

d. Phase Four, Mitigation Framework Development

The findings from Phase 3 were synthesized to develop a multi – layered mitigation framework. This framework integrates technical, governance, and collaborative measures aligned with the NIST CSF 2.0 [11] and tailored to the requirements and gaps identified in the Zambian legal context.

4.0 . RESULTS AND DISCUSSION

a. Key Provisions of the Cyber Crime Act, 2025, Affecting CII

The analysis of the Act revealed several pivotal provisions. It provides a clearer, more expansive definition of CII, encompassing cloud – based control systems. It introduces a strict 24-hour mandatory reporting window for significant CII incidents to ZICTA, a significant reduction from the 72 hour window for personal data breaches under the Data Protection Act [4], [5]. The Act also grants ZICTA enhanced audit and inspection powers and establishes stronger provisions for national – level information sharing.

b. Scenario Analysis Results

The application of the scenarios yielded critical insights:

i. Scenario A (Ransomware on Energy Grid), the Act empowers a swift, centralized response led by ZICTA and the National CERT [5]. However, the 24-hour reporting mandate poses a severe challenge, as initial incident containment and assessment within such a short time frame may be technically infeasible for many operators [17], potentially leading to non-compliance penalties during a crisis. The framework in [11] would recommend isolating affected systems, but the legal pressure to report immediately could conflict with operational recovery priorities.

i. Scenario B (SWIFT Compromise), the Act's provisions for cross – border collaboration are crucial here, as financial crimes are inherently international [29]. The mandatory information sharing framework can help quickly disseminate threat indicators to other banks. However, concerns regarding liability and the protection of shared sensitive information could hinder full participation from private entities [6], [14]. The Bank of Zambia's guidelines [32] would need to be explicitly harmonized with the new Act.

ii. Scenario C (DDoS on Telecoms), the Act's recognition of attacks on telecommunications as a national security issue is a key strength. It provides a legal basis for invoking national security protocols and seeking international cooperation from bodies like INTERPOL [50]. The primary risk identified is the potential for unclear thresholds when does a disruptive event become significant enough to trigger the full CII response protocol? This ambiguity could lead to delayed escalation.

c. Proposed Mitigation Framework

To address the identified risks, we propose a mitigation framework with three pillars:

i. Technical and Operational Controls, CII operators must implement robust security measures aligned with the NIST CSF 2.0 [11] and sector-specific guidelines [32], [36]. This includes network segmentation, continuous monitoring, and regular scenario-based exercises [10], [15].

ii. Governance and Compliance, Organizations should develop clear internal policies that map legal obligations to operational procedures. This includes establishing precise internal reporting chains to meet the 24-hour mandate and conducting gap analyses against the new Act.

iii. Collaborative Public – Private Partnerships (PPPs), ZICTA should establish formal, trusted channels for information sharing, ensuring anonymity and liability protection where appropriate [14]. Regular table-top exercises involving government agencies and CII operators are essential for building trust and testing coordination under the new law.

5.0 CONCLUSION

This paper has presented a scenario – based risk assessment of the impact of Zambia's Cyber Crime Act, 2025, on the nation's Critical Information Infrastructure. The findings demonstrate that the Act is a double – edged sword it provides essential legal tools for a coordinated national response to serious cyber incidents but also introduces significant compliance and operational challenges for CII operators. The strict reporting timelines, while intended to ensure swift action, may be pragmatically difficult to meet and could disincentivize transparent reporting during a crisis.

The proposed mitigation framework offers a path forward, emphasizing the need for a holistic approach that combines technical security, clear governance, and strengthened collaboration. The successful protection of Zambian CII will depend not only on the letter of the law but on the effective, pragmatic, and collaborative implementation of these measures by all stakeholders.

Future work will involve quantitative modeling of the cascading effects of the identified scenarios and empirical research through interviews with Zambian CII operators and regulators to validate and refine the proposed framework.

REFERENCES

- World Bank, "Cyber-Resilience of Critical Infrastructure: A Guide for Regulators," Washington, D.C., 2022.
- Republic of Zambia, "National Cyber Security Strategy (2024-2028)," Lusaka: Ministry of Technology and Science, 2024.
- Government of the Republic of Zambia, "The Cyber Security and Cyber Crimes Act No. 2 of 2021," Lusaka: Government Printer, 2021.
- Government of the Republic of Zambia, "The Data Protection Act No. 3 of 2021," Lusaka: Government Printer, 2021.
- Government of the Republic of Zambia, "The Cyber Crime Act, 2025 (Act No. X of 2025)," Lusaka: Government Printer, 2025.
- P. Myerson, "Scenario-Based Planning: A Tool for Strategic Cybersecurity," Gartner Research, 2023.
- M. Theoharidou and D. Gritzalis, "Critical Infrastructure Protection: A Risk-Based Approach," in Handbook of Security and Privacy, Elsevier, 2021.
- ENISA (European Union Agency for Cybersecurity), "Methodologies for the Identification of Critical Information Infrastructure," Publications Office of the European Union, 2023.
- L. Carin, et al., "Advancing Cyber Threat Scenario Modeling for Critical Infrastructure," IEEE Transactions on Information Forensics and Security, vol. 18, 2023.
- D. Bodeau and R. Graubart, "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," MITRE Corporation, 2022.
- NIST (National Institute of Standards and Technology), "NIST Cybersecurity Framework (CSF) 2.0," U.S. Department of Commerce, 2023.
- NIST (National Institute of Standards and Technology), "NIST Special Publication 800-82 Rev. 3: Guide to Operational Technology (OT) Security," U.S. Department of Commerce, 2022.
- SADC (Southern African Development Community), "Regional Critical Infrastructure Protection Programme Framework," 2022.
- Ghana Cyber Security Authority, "Directive for Critical Information Infrastructure (CII)," Accra, 2023.
- South Africa, Department of Communications and Digital Technologies, "Draft National Critical Infrastructure Bill," Pretoria, 2024.

- J. Muthuri and S. Kabanda, "A Comparative Analysis of Cybercrime Legislation in the SADC Region," African Journal of Information and Communication (AJIC), no. 31, 2023.
- P. Chewe, "Zambia's Evolving Cyber Law Landscape: Challenges and Opportunities for CIIP," Zambia Law Journal, vol. 55, 2024.
- J. A. Lewis, "Assessing the Risk to Critical Infrastructure from Cyber Attack," Center for Strategic and International Studies (CSIS), 2024.
- R. Axelrod, Simulating Cyber Conflict: Using Wargames for Research and Education. RAND Corporation, 2021.
- C. J. Alberts and A. J. Dorofee, OCTAVE Allegro: Guide to the Information Security Risk Assessment Method. Software Engineering Institute, Carnegie Mellon University, 2023.
- T. Tuyikeze and L. Abrahams, "Applying Attack Graphs for Proactive Defence in African Critical Infrastructure," in Proceedings of the Southern Africa Cyber Security Conference, 2024.
- ZICTA, "National Critical Information Infrastructure Policy Framework (Draft for Consultation)," Lusaka: Zambia Information and Communications Technology Authority, 2023.
- Bank of Zambia, "Cyber Security Guidelines for Payment Service Providers," Lusaka, 2022.
- Y. Cherdantseva, et al., "A Systematic Review of Cyber Risk Assessment Tools for the Energy Sector," Energy Informatics, vol. 7, no. 1, 2024.
- INTERPOL, "Cybercrime Threat Landscape for Africa: 2025 Assessment," Lyon, 2025.
- R. Khan and P. Maynard, "Cybersecurity of Smart Grids: A Review of Vulnerabilities and Impacts," IEEE Power and Energy Magazine, vol. 22, no. 2, 2024.
- SWIFT Institute, "The Cyber Threat Landscape for Financial Market Infrastructures," 2023.
- T. Bessis, "Cyber Attacks on Healthcare Critical Infrastructure: Lessons from the COVID-19 Era," The Lancet Digital Health, vol. 4, no. 3, 2022.
- Humayed, et al., "Cyber-Physical Systems Security: A Survey for the Smart Grid," IEEE Internet of Things Journal, vol. 10, no. 5, 2023.
- Munyuki and A. Kallon, "State of Cybersecurity Preparedness in Southern African Critical Infrastructure Sectors," International Journal of Critical Infrastructure Protection, vol. 40, 2023.
- T. Moyo, Cybersecurity Governance in Africa: A Study of National CERTs. Institute for Security Studies (ISS Africa), 2022.
- Kenya National Computer Cybercrimes Coordination Committee, "Annual Report on Cyber Threats to National Infrastructure," Nairobi, 2024.
- SADC (Southern African Development Community), "SADC Model Law on Computer Crime and Cybercrime," 2023.
- African Union, "The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention): Status of Implementation Report," 2024.

- P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, 3rd ed. Oxford University Press, 2021.
- T. Rid and P. McBurney, "Cyber-Weapons and Critical Infrastructure: A Taxonomy of Effects," Journal of Cybersecurity, vol. 9, no. 1, 2023.
- G. C. Kessler and J. P. Craiger, "ICS/SCADA Cyber Incidents: A Longitudinal Analysis," Computers & Security, vol. 124, 2023.
- ISO/IEC, "ISO/IEC 27005:2022 - Information technology — Security techniques — Information security risk management," 2022.
- ISO/IEC, "ISO/IEC 63422:2024 - Cybersecurity — Framework for critical infrastructure protection," 2024.
- A. Cardenas, et al., "Big Data Analytics for Cybersecurity in Critical Infrastructures," ACM Computing Surveys, vol. 54, no. 1, 2021.
- K. Croom, et al., "Supply Chain Attacks Targeting Telecommunications Infrastructure," in Proceedings of the Workshop on Telecommunications Security, 2024.
- World Economic Forum, "Global Cybersecurity Outlook 2025," Geneva, 2025.
- ITU (International Telecommunication Union), "Global Cybersecurity Index (GCI) 2025: Country Profile for Zambia," 2025.
- PwC, "Zambia Economic Outlook: The Digital Economy and Regulatory Compliance in 2025," Lusaka, 2025.
- ZICTA, "Post-Enactment Review of the Cyber Crime Act, 2025: Initial Impact on CII Operators," Lusaka, 2025.
- Mulenga, "The First 100 Days: Analyzing the Enforcement of Zambia's Cyber Crime Act, 2025," Journal of African Law, vol. 69, no. 2, 2025.
- S. Mkandawire, "Bridging the Gap: Technical Implementation of the Cyber Crime Act, 2025 in the Zambian Financial Sector," Zambia Banking Journal, 2025.
- Gartner, "Hype Cycle for Cybersecurity, 2025," 2025.
- Verizon, "Data Breach Investigations Report (DBIR) - 2025 Edition," 2025.
- Symantec, a division of Broadcom, "Internet Security Threat Report (ISTR), Volume 30," 2025.