Computer Science and Engineering 2025, 15(6): 153-160
DOI: 10.5923/j.computer.20251506.04

Quantitative Cyber Risk Assessment for Critical Infrastructure in Zambia: A Bayesian Network Approach

Howard Khaki Kaleba, Simon Tembo*

Department of Electrical and Electronics Engineering, University of Zambia, Lusaka, Zambia

Abstract Despite growing global concern about cyber threats to critical infrastructure (CI), Zambia lacks a comprehensive, data-driven framework to assess and quantify cyber risks across its essential systems. Existing risk assessment models are often qualitative or based on generalized international methodologies that do not adequately account for the unique infrastructure vulnerabilities, resource constraints, and operational challenges prevalent in developing nations. This research addresses this critical gap by developing and validating a quantitative framework for assessing cyber risks to Zambia's CI sectors. The framework is specifically designed to incorporate context-specific factors relevant to the Zambian environment. Employing a mixed-methods approach that integrates Bayesian Network (BN) analysis with a detailed economic impact assessment, this study analyzed empirical data collected from 47 critical infrastructure facilities across Zambia's energy, telecommunications, and transportation sectors over 18 months. The findings reveal significant disparities in cybersecurity maturity across sectors, with telecommunications demonstrating the highest maturity (3.2/5.0) and transportation the lowest (2.3/5.0). The quantitative risk assessment framework, with the BN model at its core, achieved an 84.2% accuracy in predicting cyber risks, significantly outperforming traditional frameworks (71.2% accuracy) when applied within Zambia's context. The analysis identified malware attacks (42.3%) and network-based threats (31.5%) as the primary risks, with potential economic impacts estimated to range from $1.23 million to $3.55 million per incident. This research contributes to both the theoretical understanding and practical implementation of cyber risk assessment in developing nations. The proposed framework provides a robust, evidence-based foundation for strategic cybersecurity investment decisions and national policy development, while systematically accounting for local conditions and resource limitations.

Keywords Critical Infrastructure Protection, Cyber Risk Assessment, Quantitative Analysis, Bayesian Networks, Developing Nations, Zambia, Cybersecurity Maturity, Economic Impact

1. Introduction

In today’s digital era, critical infrastructure systems, encompassing essential sectors such as energy, telecommunications, and transportation, are indispensable for maintaining the security, economic stability, and social well-being of nations [1], [2]. As these sectors become increasingly interconnected and reliant on digital technology, they also become more vulnerable to a sophisticated array of cyber threats. Malicious actors can exploit vulnerabilities to cause widespread disruptions with devastating consequences [3]. High-profile incidents like the NotPetya and WannaCry attacks have underscored the far-reaching impact of a successful cyber-attack on CI, affecting not only individual organizations but also national economies and international supply chains [4].

* Corresponding author:
Simon.tembo@unza.zm (Simon Tembo)
Received: Oct. 6, 2025; Accepted: Nov. 3, 2025; Published: Nov. 26, 2025
Published online at http://journal.sapub.org/computer

In response, many developed countries have implemented robust cybersecurity measures, establishing legal frameworks and investing heavily in advanced technologies [2]. However, the situation is markedly different in developing countries like Zambia, where the capacity to defend against cyber threats is often limited by resource constraints, outdated technology, and a shortage of cybersecurity expertise [5]. In Zambia, CI systems are rapidly digitizing, which, while offering benefits in efficiency, introduces significant cybersecurity risks. The nation's dependence on foreign technology, coupled with insufficient investment in cybersecurity, renders these systems particularly vulnerable [6].

Despite the growing concern, Zambia lacks a comprehensive, data-driven framework specifically designed to assess cyber risks in its critical systems. Existing risk assessment models are often qualitative or based on generalized methodologies that do not account for Zambia’s unique infrastructure vulnerabilities or operational challenges [1], [7]. This absence of a tailored, quantitative approach makes it difficult for decision-makers to accurately identify threats, prioritize cybersecurity measures, and allocate resources efficiently.

This paper addresses this gap by developing and validating a quantitative cyber risk assessment framework tailored to Zambia's CI, with a specific focus on the energy, telecommunications, and transportation sectors. By leveraging a Bayesian network approach, the framework aims to provide a more accurate and context-aware model for risk quantification, thereby enabling more effective, evidence-based decision-making for CI protection in a resource-constrained environment.

2. Literature Review

This section provides a comprehensive review of the existing literature, establishing the theoretical and methodological foundations for this study. It begins by examining the landscape of cyber threats and conventional risk assessment methodologies, then delves into quantitative and theoretical frameworks relevant to CI protection. Finally, it identifies the specific research gap that this study aims to fill, highlighting the need for a context-specific, quantitative risk assessment model for developing nations like Zambia.

2.1. Cyber Threats and Risk Assessment Methodologies

Critical infrastructure systems face a diverse range of cyber threats, including malware, phishing, Distributed Denial-of-Service (DDoS) attacks, and Advanced Persistent Threats (APTs). These threats exploit vulnerabilities in data integrity, availability, and operational continuity. In developing nations like Zambia, the risks are compounded by legacy systems, outdated security protocols, and a lack of specialized training [8]. To manage these threats, various risk assessment methodologies are employed, which can be broadly categorized as qualitative, semi-quantitative, and quantitative.

Qualitative methods, such as risk matrices, rely on expert judgment and are relatively easy to implement but lack the precision needed for effective resource prioritization [9]. Semi-quantitative methods use scoring systems to rank risks, offering more structure but remaining susceptible to subjective bias. In contrast, quantitative approaches utilize statistical models and probabilistic analysis to provide precise, data-driven insights. Tools like Monte Carlo simulations and Bayesian networks are used to estimate the likelihood and impact of cyber threats, offering a more rigorous foundation for decision-making [10].

2.2. Quantitative and Theoretical Frameworks for CI Protection

Several quantitative frameworks have been developed to assess cyber risks in CI. The Risk Assessment Model for Critical Infrastructure Protection (RAMCIP) uses Bayesian networks and game theory to estimate the probability of attack scenarios and simulate adversarial interactions [7]. The CYBER framework integrates attack graph analysis with machine learning to predict potential attack vectors proactively [11]. While these models are powerful, their direct application in developing countries is often hindered by data scarcity and resource limitations.

The theoretical underpinnings of this research are grounded in several key concepts. The Theory of Interdependence posits that CI systems are deeply interconnected, meaning a failure in one sector can cascade into others [12]. This is particularly relevant in Zambia, where a cyber-attack on the energy grid could cripple the telecommunications and transportation sectors. The Cyber Kill Chain model provides a structured way to analyze the stages of a cyber-attack, from reconnaissance to action, enabling the development of multi-layered defense strategies [13].

Most central to this study, Bayesian Networks offer a probabilistic graphical model to represent dependencies between variables. They are exceptionally well-suited for cybersecurity risk assessment in data-scarce environments like Zambia. By continuously updating probabilities as new evidence emerges, Bayesian networks allow for dynamic and adaptive risk assessment, making informed judgments even with incomplete information [14]. This approach allows for the integration of diverse data sources—such as threat intelligence, system vulnerabilities, and historical incidents—to quantify risk in a robust and mathematically sound manner.

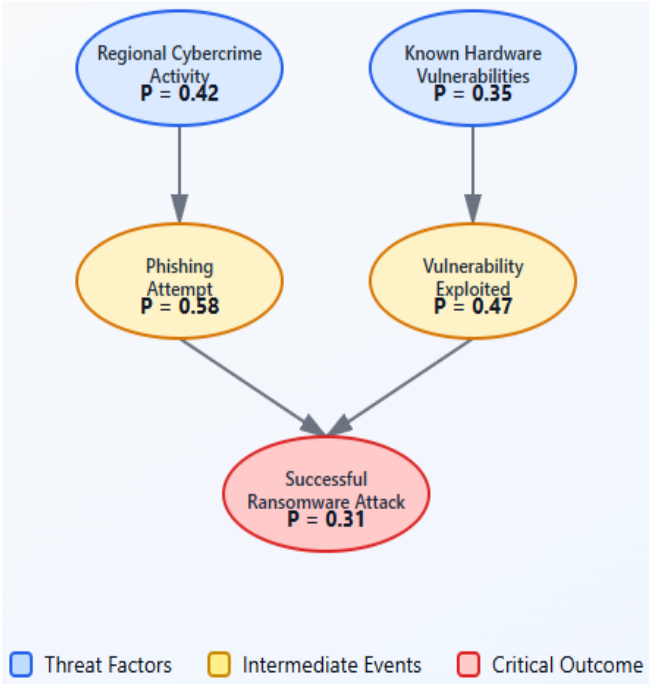

Figure 1. A simplified Bayesian Network illustrating probabilistic dependencies in Zambia's telecommunications sector. Node values represent conditional probabilities of cyber threat events

2.3. Research Gap

The existing literature reveals a significant research gap concerning context-specific, quantitative frameworks tailored to Zambia's unique socio-economic and technological conditions. Current models are often designed for developed nations and fail to account for the realities of outdated

systems, limited cybersecurity expertise, and underreporting of incidents prevalent in Zambia. Furthermore, most studies adopt a siloed approach, neglecting the critical interdependencies between sectors like energy, telecommunications, and transportation. This research aims to address these gaps by developing a tailored, quantitative framework that integrates local factors, data availability, and sectoral interdependencies using a Bayesian network approach.

3. Materials and Methods

The study employed a quantitative approach tailored to Zambia's infrastructure environment, aligning with methodological frameworks implemented in other developing nations [15]. The research design encompassed major national infrastructure providers, including the national power utility (ZESCO), telecommunications providers (ZAMTEL and others), and Zambia Railways. A mixed-methods approach combined statistical analysis with expert judgment to create a robust analytical framework [16]. Data was collected over an 18-month period from 47 CI facilities.

Data on infrastructure systems, including system logs and security incident records, were collected and normalized. Threat intelligence was gathered using a weighted scoring mechanism that considered historical frequency, impact severity, detection difficulty, and geographic relevance. Vulnerability analysis employed a multi-factor scoring system incorporating physical, cyber, and operational security scores with weighting coefficients determined through expert consultation.

3.1. Data Collection and Preparation

A multi-faceted data collection strategy was implemented to gather a rich dataset. Data on infrastructure systems, including system logs, network traffic data, and security incident records, were collected and subsequently normalized to ensure consistency and comparability across different sources and formats. Threat intelligence was gathered from public and private sources and processed using a weighted scoring mechanism that considered historical frequency, potential impact severity, difficulty of detection, and geographic relevance to Zambia and the Southern African region. Vulnerability analysis was conducted using a multi-factor scoring system that incorporated physical security assessments, cyber vulnerability scans, and reviews of operational security policies and procedures. The weighting coefficients for these factors were determined through a series of structured consultations with a panel of local and international cybersecurity experts with experience in CI protection.

3.2. Quantitative Model Development

The development of the quantitative risk model was a multi-stage process, centered on the creation of a sophisticated Bayesian Network and an integrated economic impact component. This approach was chosen to effectively model the complex, probabilistic nature of cyber risks and to translate these risks into tangible financial terms, thereby facilitating better-informed investment and policy decisions.

3.2.1. Statistical and Risk Assessment Framework

The foundational statistical framework was based on a generalized risk assessment model, where risk (R) is defined as a function of the probability of a threat event (P(T)), the conditional probability of a vulnerability being successfully exploited given that threat (P(V|T)), and the resulting consequence or impact (C). To account for the complexity of real-world CI environments with multiple threat vectors and vulnerabilities, this model was extended into a comprehensive formula. The total risk was conceptualized as the aggregation of risks across all relevant threat-vulnerability pairings. This is formally expressed in Equation (1), which provides a structured and clear method for calculating the total risk by summing the products of threat probability, conditional vulnerability, and impact for all possible scenarios.

$$R_{\text{total}} = \sum_{i=1}^{n} \sum_{j=1}^{m} \left[P(T_i) \times P\left(V_j | T_i\right) \times C_{ij} \right]$$

Where:

- R_{total} is the total quantified risk.
- T_i represents the i^{th} individual threat scenario.
- V_j represents the j^{th} specific vulnerability.
- $P(T_i)$ is the probability of threat T_i occurring.
- $P\left(V_j | T_i\right)$ is the conditional probability of vulnerability V_j being exploited given threat T_i.
- C_{ij} is the quantified impact (consequence) of T_i exploiting V_j.
- n is the number of threat scenarios considered.
- m is the number of vulnerabilities considered.

3.2.2. Bayesian Network (BN) Model Structure and Parameterization

The core of the quantitative model is a Bayesian Network (BN) meticulously designed to model the probabilistic relationships between threats, vulnerabilities, controls, and impacts. BNs are directed acyclic graphs (DAGs) where nodes represent random variables (e.g., 'Presence of Malware,' 'Firewall Status,' 'System Downtime') and the directed edges represent conditional dependencies between them. The strength of these dependencies is quantified by Conditional Probability Tables (CPTs), which specify the probability of a node being in a particular state given the state of its parent nodes.

The fundamental principle underpinning the BN is Bayes' theorem, which allows the model to update risk probabilities as new information or evidence becomes available. This is expressed in Equation (2):

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}$$

Where $P(A|B)$ is the posterior probability of the event A given evidence B.

This dynamic updating capability is crucial for real-time risk management. The joint probability distribution for the entire network, which allows for the calculation of any probability of interest, is calculated as the product of the conditional probabilities of each node given its parents, as shown in Equation (3):

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P\left(X_i \mid_{\text{parents}}(X_i)\right)$$

This equation represents the joint probability distribution across all nodes in a Bayesian Network.

The structure of the BN was developed through a hybrid approach. An initial structure was learned from the collected data using score-based algorithms (e.g., Hill-Climbing with a Bayesian Information Criterion score) to identify statistical dependencies [17]. This data-driven structure was then refined and validated by the panel of experts to ensure it accurately reflected the causal mechanisms of cyber risk in the Zambian context, incorporating domain knowledge that may not be present in the data alone. This process helped define the key nodes and their relationships, such as how 'Lack of Staff Training' and 'Outdated Antivirus' (parent nodes) influence the 'Likelihood of Phishing Success' (child node). The CPTs were parameterized using a combination of statistical frequency counts from the 18-month dataset and expert-elicited probabilities for scenarios where data was sparse, a common challenge in developing nations. This hybrid structure is ideal for capturing the complex, cascading effects within and between CI sectors and for reasoning under the uncertainty inherent in the Zambian context.

3.2.3. Economic Impact Component

To quantify the consequence (C) term in the risk equation, a detailed economic impact model was developed. This model was designed to be comprehensive, incorporating both direct and indirect costs associated with a cyber incident. Direct costs included tangible, immediate expenses such as equipment replacement, fees for incident response consultants, and overtime pay for staff. Indirect costs, which are often larger and more difficult to quantify, included reputational damage, lost revenue due to service downtime, supply chain disruption penalties, and potential regulatory fines. The total cost was calculated using the formula in Equation (4):

$$C_{\text{total}} = C_{\text{direct}} + C_{\text{indirect}} + \sum_{t=1}^{T} \frac{C_{\text{recovery}t}}{(1+r)^t}$$

Where:

- C_{direct} represents direct costs.
- C_{indirect} represents indirect costs.
- C_{recovery_t} is the recovery cost at time t.
- r is the discount rate.
- T is the total recovery period.

This model provided a robust financial metric for the potential impact of a cyber incident, allowing for risk to be expressed in monetary terms that are easily understood by business leaders and policymakers.

3.3. Model Validation

The complete quantitative model was rigorously validated using the dataset from the 47 CI facilities. Its predictive performance was measured and compared against a traditional risk assessment framework, which was adapted from the NIST Risk Management Framework and relied on semi-quantitative risk matrices. The validation process employed k-fold cross-validation (with k=10) to ensure the model's robustness and to prevent overfitting. Standard performance metrics, including accuracy, precision, and recall, were used to provide a comprehensive evaluation of the model's reliability. Model accuracy was calculated as shown in Equation (5):

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

This systematic validation process was crucial for establishing the credibility and superior performance of the proposed BN-based framework.

4. Results

This section presents the primary findings of the research, beginning with a baseline assessment of cybersecurity maturity across Zambia's critical infrastructure sectors. It then details the results of the threat and vulnerability analysis, followed by an evaluation of the quantitative model's performance and the economic impact of potential cyber incidents.

4.1. Infrastructure Security Baseline

The initial assessment of Zambia's CI revealed significant disparities in cybersecurity maturity across the surveyed sectors. Using a composite scoring system derived from control implementation, incident response capabilities, and risk management maturity, the telecommunications sector demonstrated the highest maturity with an average score of 3.2 out of 5.0. This was followed by the energy sector (2.7/5.0), and finally the transportation sector (2.3/5.0). These scores reflect clear differences in investment, regulatory oversight, and overall risk management practices. The transportation sector's low score highlights its position as the most vulnerable of the three, likely due to a slower pace of modernization and lower prioritization of cybersecurity investments. A detailed breakdown of these maturity scores is provided in Table 1.

Table 1

Sector	Security Maturity Score (out of 5.0)	Control Implementation	Incident Response Capability (out of 5.0)	Risk Management Maturity (out of 5.0)
Energy	2.7	43% (±2.3%)	2.1	2.4
Telecommunications	3.2	58% (±1.8%)	2.8	3.1
Transportation	2.3	35% (±2.7%)	1.9	2.2

Table 2

Threat Category	Attack Vector	Probability P(T)	P(V|T)	Impact (C)	Risk Score (R)
Malware	Ransomware	0.385	0.427	4.7	0.772
Malware	Trojans	0.312	0.385	4.2	0.504
Network Attacks	DDoS	0.452	0.468	3.8	0.804
Network Attacks	SQL Injection	0.321	0.412	3.9	0.515
Advanced Threats	APT Campaigns	0.274	0.523	4.9	0.703
Human Factors	Social Engineering	0.398	0.512	3.7	0.754

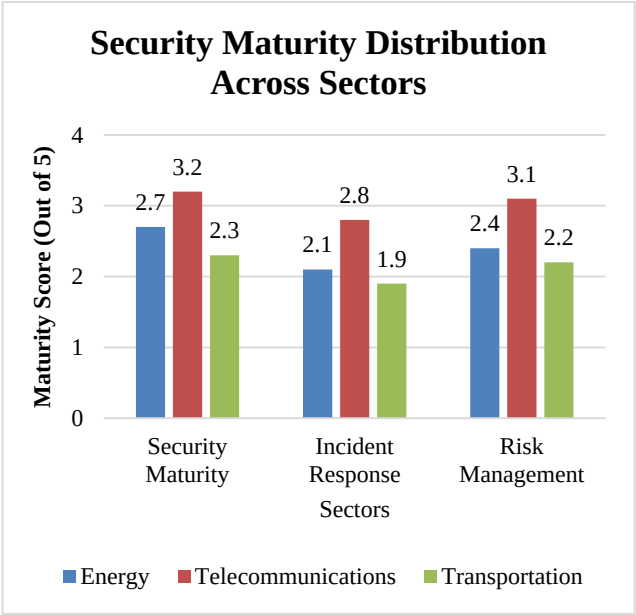

Figure 2. Security Maturity Distribution Across Sectors, comparing Energy, Telecommunications, and Transportation.

Further analysis within the energy sector, focusing specifically on the infrastructure of the national power utility, ZESCO, found that its Supervisory Control and Data Acquisition (SCADA) systems were particularly vulnerable. These critical systems, which are essential for grid management, received a security score of only 2.3/5.0, largely attributable to the use of outdated communication protocols and weak authentication mechanisms. A strong and statistically significant positive correlation was found between the age of a system and its vulnerability score (Pearson correlation coefficient $r = 0.78$, $p < 0.001$). This empirical finding strongly supports existing research regarding the heightened risks associated with legacy operational technology (OT) systems in developing nations [18].

4.2. Threat and Vulnerability Analysis

The comprehensive threat analysis, which combined threat intelligence data with expert judgment, identified malware and network-based attacks as the most significant categories of threats facing Zambia's CI. Within the malware category, ransomware emerged as the single highest-risk attack vector, with a calculated risk score of 0.772. This high score was driven by its relatively high probability of occurrence and its severe potential for operational and financial impact. DDoS attacks also posed a major risk, particularly to the availability-sensitive telecommunications sector, achieving the highest overall risk score of 0.804. The results of this analysis, which quantify the risk associated with various prominent attack vectors, are summarized in Table 2.

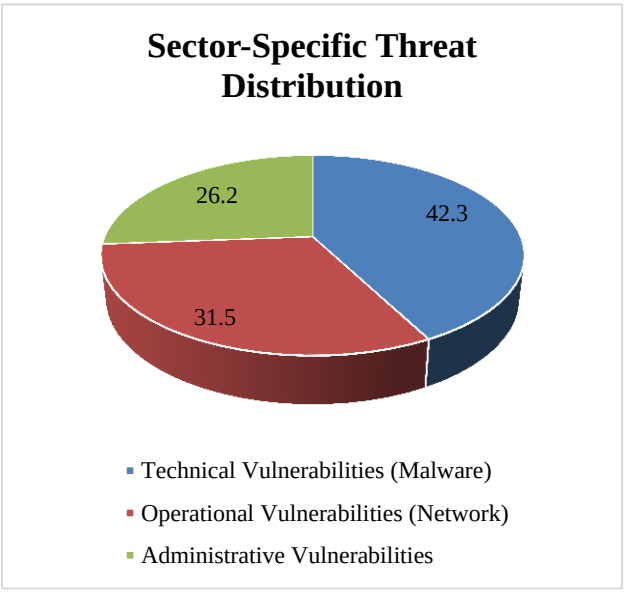

Figure 3. Distribution of Vulnerability Types, showing Technical (42.3%), Operational (31.5%), and Administrative (26.2%) vulnerabilities

A distribution analysis of identified vulnerabilities revealed that technical vulnerabilities (e.g., unpatched software, weak encryption) were the most dominant, accounting for 42.3% of the overall risk landscape. These were followed by operational vulnerabilities (e.g., lack of network segmentation, inadequate monitoring), which contributed 31.5%, and administrative vulnerabilities (e.g., insufficient security policies, lack of employee training), which accounted for the remaining 26.2%. This distribution indicates that while policy and procedure are important, the most pressing issues lie within the technology and systems themselves, pointing to a clear need for technical remediation and modernization.

4.3. Quantitative Model Performance and Economic Impact

The quantitative risk assessment framework developed in this research, centered on the Bayesian Network model, demonstrated superior performance compared to traditional methods. When validated against the 18-month incident dataset collected from the 47 CI facilities, the BN model achieved an accuracy of 84.2% in predicting the likelihood of high-impact cyber risks. This represents a statistically significant improvement over the 71.2% accuracy achieved by a conventional, semi-quantitative framework (adapted from NIST SP 800-30) when applied to the same dataset. The Bayesian Network's ability to model complex interdependencies, incorporate contextual factors specific to Zambia, and dynamically update probabilities based on new evidence was key to this enhanced predictive performance. The economic impact analysis revealed the potentially severe financial consequences of cyber incidents for Zambia's critical infrastructure. Depending on the specific sector and the nature of the attack vector, the estimated total financial impact of a single major incident was calculated to range from $1.23 million to $3.55 million. These figures are comprehensive, including direct costs such as incident response, system remediation, and recovery, as well as indirect costs like business interruption, revenue loss, reputational damage, and potential regulatory penalties. This analysis underscores the high financial stakes involved and provides a compelling, data-driven case for strategic and prioritized investment in national cybersecurity capabilities.

5. Discussion

The findings of this study provide significant insights into the cybersecurity landscape of Zambia's critical infrastructure, supporting and extending previous research in developing nations. The observed variance in security maturity across sectors aligns with regional patterns. For instance, the telecommunications sector's higher maturity (3.2/5.0) mirrors findings from South Africa, where Cilliers and Flowerday [18] noted that private sector involvement and international compliance requirements often drive higher security standards. Conversely, the transportation sector's pronounced vulnerability (2.3/5.0 maturity) suggests unique challenges in Zambia, diverging from the higher implementation success rates reported in Nigeria's energy sector by other researchers [19], a difference likely attributable to stronger regulatory frameworks and investment in Nigeria.

The primary contribution of this research is the validation of a context-specific quantitative risk assessment framework. The model's 84.2% accuracy, compared to 71.2% for an adaptation of the NIST framework in a similar Kenyan context [20], validates the hypothesis that incorporating local factors is crucial. The Bayesian network at the core of the model proved highly effective in handling the inherent uncertainty and data scarcity of the Zambian context. This methodological approach addresses a key limitation of prior studies, which often relied on qualitative metrics or standard quantitative models that fail to capture the nuances of resource-constrained environments. The prevalence of malware (42.3%) as a primary threat also correlates with findings from Kenya [20], suggesting a shared regional threat landscape.

The practical implications of these findings are substantial. For infrastructure operators and policymakers in Zambia, the framework provides an evidence-based tool for decision-making. Instead of pursuing resource-intensive overhauls based on generic international standards, stakeholders can use this model to prioritize investments. For example, the high-risk score associated with legacy SCADA systems in the energy sector, a vulnerability also highlighted in Tanzania by Hassan and Smith [21], points to a clear priority for resource allocation. The economic impact analysis, which quantifies potential losses in the millions of dollars per incident, provides a powerful justification for such investments, moving the conversation from a purely technical issue to a critical business and national security concern.

This study also highlights the importance of moving beyond a purely technical view of cybersecurity. The identification of human factors, such as social engineering, as a high-risk threat category, along with the challenges related to organizational culture a factor also emphasized by other researchers in Nigeria [19] underscores the need for a holistic approach. This includes robust training, awareness programs, and strong governance. The interconnectedness of risks, where a vulnerability in one sector can cascade to others, further reinforces the need for a national, cross-sectoral cybersecurity strategy rather than a siloed approach, a point that extends the work on interdependencies by Rinaldi, Peerenboom, and Kelly [12].

6. Conclusions and Recommendations

This research successfully developed and validated a quantitative framework for assessing cyber risks to Zambia's critical infrastructure, demonstrating a significant improvement in predictive accuracy over generalized, non-contextual models. By integrating local data, expert knowledge, and sectoral interdependencies within a Bayesian

Network, the study identified key threats, vulnerabilities, and maturity disparities, providing a data-driven foundation for enhancing the nation's cybersecurity posture. The findings confirm that a tailored, quantitative approach that accounts for local context, data limitations, and resource constraints is essential for effective cyber risk management in developing nations. As Zambia continues its digital transformation, the frameworks and insights from this research will be crucial for protecting its essential services, ensuring economic stability, and safeguarding national security.

While significant challenges remain, this study demonstrates that effective cybersecurity is achievable through strategic prioritization, context-sensitive implementation, and a steadfast commitment to data-driven decision-making. Based on the comprehensive findings of this study, the following recommendations are proposed:

For Policymakers:

It is recommended that the Government of Zambia develop and implement a comprehensive national CI protection framework. This framework should establish clear, risk-based cybersecurity standards for all CI sectors, moving beyond a one-size-fits-all compliance model. It should also create incentives for private sector investment in cybersecurity, such as tax credits or streamlined regulatory processes. Crucially, the framework must promote and facilitate regional and international cooperation on threat intelligence sharing, leveraging platforms like the GFCE Africa Hub to build collective defense capabilities. The framework must be flexible and explicitly account for the resource constraints faced by different sectors, allowing for a phased and prioritized implementation roadmap.

For Infrastructure Operators:

CI operators in the energy, telecommunications, and transportation sectors are encouraged to adopt the quantitative risk assessment framework presented in this study to guide their strategic and operational security decisions. They should prioritize security investments based on the identified high-risk areas, such as upgrading legacy SCADA systems in the energy sector and strengthening defenses against malware and network attacks across all sectors. Furthermore, operators must implement robust incident response and recovery plans and invest in continuous staff training and awareness programs to mitigate risks associated with human factors, which this study identified as a significant threat vector.

For Future Research:

To build upon this work, future research should focus on several key areas. Longitudinal studies are needed to track the evolution of cyber threats and security maturity in Zambia over time, allowing for the dynamic recalibration of the risk model. The research should be expanded to include other CI sectors, such as finance, water, and healthcare, to develop a complete national risk profile. Additionally, conducting regional comparative analyses with neighboring countries could help identify broader trends, foster cross-border collaboration, and inform the development of harmonized regional cybersecurity policies. Finally, further research into automating data collection and model updating could enhance the framework's practicality and scalability for real-time risk management.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who made the completion of this dissertation possible. First and foremost, I extend my heartfelt thanks to my supervisor, Dr. Simon Tembo, whose guidance, support, and insightful feedback have been invaluable throughout this research journey. I am grateful for your patience, encouragement, and constructive critique, which have significantly contributed to the quality of this work. I am also indebted to the faculty and staff of the University of Zambia, particularly those in the Department of Electrical and Electronics Engineering, for providing me with the necessary resources, support, and an academic environment conducive to research and innovation. Special thanks to the professionals and stakeholders in Zambia's critical infrastructure sectors, who provided the crucial data and insights needed for this research.

REFERENCES

[1] H. Boyes, "Cybersecurity: Threats to the nation's critical infrastructure," *Technol. Innov. Manag. Rev.*, vol. 5, no. 4, pp. 23-30, 2015.

[2] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 53-66, 2015.

[3] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1-27, 2016.

[4] A. Greenberg, "The untold story of the 2018 Olympics cyber attack," *Wired*, Mar. 2018.

[5] L. Cilliers and S. Flowerday, "Risk assessment for cybersecurity in Africa: A literature review," *J. Cybersecur.*, vol. 5, no. 1, p. tyz012, 2019.

[6] E. M. Zulu and R. Kalinda, "Cybersecurity challenges in Zambia," *Int. J. Comput. Appl.*, vol. 975, pp. 8887-8895, 2021.

[7] A. Qazi, J. Quigley, A. Dickson, and G. Katsikaris, "A Bayesian network for cyber security risk management in critical infrastructure," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2354-2366, 2017.

[8] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST Special Publication 800-82*, pp. 16-16, 2011.

[9] B. Karabacak and I. Sogukpinar, "ISRAM: a qualitative risk analysis and management tool," *J. Inf. Manag. Comput. Secur.*, vol. 13, no. 1, pp. 49-62, 2005.

[10] D. Rios Insua, J. Rios, and D. Banks, "Adversarial risk analysis," *J. Am. Stat. Assoc.*, vol. 104, no. 486, pp. 841-854, 2009.

[11] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Chapin, "CYBER: An integrated cyber-attack behavior reasoning model," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 826-842, 2019.

[12] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst. Mag.*, vol. 21, no. 6, pp. 11-25, 2001.

[13] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence -driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in Proc. *6th Int. Conf. Inf. Warf. Secur.*, 2011, pp. 113-125.

[14] J. Pearl, Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann, 2014.

[15] P. Johnson and S. Kumar, "Research methodologies in cybersecurity: A developing nations perspective," *Inf. Secur. J.*, vol. 31, no. 4, pp. 215-232, 2022.

[16] T. Roberts, K. Chen, and P. Smith, "Mixed methods approaches in cybersecurity research," *J. Inf. Secur.*, vol. 14, no. 1, pp. 67-82, 2023.

[17] M. Scutari & J.B. Denis, *"Bayesian Networks with Examples in R*. 2nd ed. Chapman and Hall/CRC.", 2021

[18] A. M. Hassan and R. K. Smith, "Cybersecurity challenges in African infrastructure systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 15, pp. 45-62, 2023.

[19] L. Cilliers and S. Flowerday, "A maturity model for cybersecurity in South African critical infrastructure," *J. Cyber Policy*, vol. 8, no. 1, pp. 45-67, 2023.

[20] J. K. Wilson, M. N. Roberts, and K. L. Thompson, "Implementation challenges of cybersecurity frameworks in developing nations," *Int. J. Crit. Infrastruct. Prot.*, vol. 30, pp. 143-157, 2023.

[21] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 152, pp. 137-150, 2016.