International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 6 ||Issue|| 4 ||Pages 192-205 ||2024||

Strengthening Tanzania's Digital Infrastructure: Assessing Cyber Threats to the Government e-Payment Gateway for National Security

[1,]Nasania Stanslaus Shalua, [2,]Adam Aloyce Semlambo
ORCiD: https://orcid.org/0009-0001-9054-1497
[1,]*Department of Computer Science: Institute of Accountancy Arusha, Tanzania*
ORCiD: https://orcid.org/0000-0002-6839-0215
[2,]*Department of Computer Science: Institute of Accountancy Arusha, Tanzania*

ABSTRACT: This study investigates the cybersecurity landscape in Tanzania through a descriptive research design, focusing on the threats and vulnerabilities within government and financial sectors amid rapid digital transformation. Employing a mixed-methods approach, the research targeted a population of 1420 government officials, with a sample size of 200 selected via purposive and convenience sampling techniques. Data were collected through structured questionnaires and in-depth interviews and analysed using both quantitative (SPSS for inferential statistics) and qualitative (content analysis) methods. Key findings reveal a significant lack of cyber literacy among staff, leading to increased susceptibility to cyber-attacks and substantial financial losses. The study recommends a multifaceted approach to enhance cyber resilience, including integrating cyber literacy into educational curricula, strengthening national cybercrime management, and fortifying government cyber networks with advanced security technologies. Additionally, it advocates for collaborative efforts among stakeholders to develop and enforce comprehensive cybersecurity policies, ensuring a secure digital environment conducive to national security and economic stability.

KEYWORDS: Cybersecurity, Cyber threats, National security, Government cyber networks

I. INTRODUCTION

The advent of Internet technology, characterised by rapid and dynamic changes, has significantly transformed global societies and economies. However, this digital evolution has also escalated the prevalence of cybercrimes, challenging the integrity and security of information systems worldwide (Nayak, 2013). Cybercrime, a multifaceted phenomenon, encompasses offences against the confidentiality, integrity, and availability of computer data and systems alongside computer-related crimes (Semlambo et al., 2023). The surge in internet users has exacerbated cybercrime, instigating a pervasive sense of uncertainty and distrust, particularly within the financial sector, which has seen a consequential erosion in consumer confidence towards online transactions (Siahaan, 2018; Baltezarevi & Baltezarevi, 2021) The Bank of England's 2022 Systemic Risk Survey highlighted the financial sector's vulnerability to cyber threats, where 74% of respondents identified cyber-attacks as the primary risk. This susceptibility was demonstrated in the 2016 cyber heist targeting the Bangladeshi central bank. Exploiting vulnerabilities in the SWIFT network, the heist stole $101 million (Statista, 2023). The rising trend of network and application anomalies, alongside account irregularities, underscores the escalating cyber threats within the global financial industry (Statista, 2023).

Africa, in particular, faces a disproportionate cybercrime challenge, with incidents and losses outpacing global averages. The Serianu Cyber Security Report estimated the continent's cybercrime costs at approximately $3.5 billion, with countries like Nigeria, Kenya, Tanzania, Uganda, and Ghana bearing substantial financial burdens (Olayemi, 2014). The situation is further compounded in nations like South Africa and Kenya, where rapid ICT growth has attracted sophisticated cybercriminal activities, severely impacting national security and economic stability (Fripp, 2014; Griffiths, 2016; MacAfee, 2014; Brenner, 2010). Amidst this backdrop, like its African counterparts, Tanzania is grappling with the escalating menace of cybercrime, especially in its growing financial sector. Despite substantial internet penetration, with nearly 50% of Tanzanians online (Nawalagatti, 2022), cybercriminals have increasingly targeted the financial industry, exploiting its digital vulnerabilities. Reports indicate significant financial losses, with almost Tsh. 1 billion stolen through cyber activities in 2014 alone. (Kshetri, 2017). The pervasive nature of high-tech crimes such as money laundering and financial terrorism has necessitated a robust response from the Tanzanian government, leading to various legal and policy frameworks to mitigate these cyber threats (Semboja et al., 2017).

Despite these efforts, cybercrime's persistent and evolving nature continues to pose significant challenges to Tanzania's financial sector and national security. The increasing sophistication of cyber threats, coupled with the strategic importance of the government's e-Payment gateway, necessitates a critical assessment of the existing digital infrastructure's resilience. This study explores the depth and breadth of cyber threats to Tanzania's government e-payment gateway, assessing its vulnerabilities and the implications for national security. Understanding these dynamics is crucial for enhancing the effectiveness of current strategies and developing robust measures to safeguard Tanzania's digital and financial ecosystems, thereby contributing to the broader discourse on cyber security in the African context.

II. LITERATURE REVIEW

Theoretical Literature Review : General Deterrence Theory (GDT) posits that individuals weigh the potential costs and benefits before engaging in any behaviour, including cybercrimes. (Grasmick & Bryjak, 1980). Originating from the ideas of philosophers such as Hobbes, Beccaria, and Bentham, GDT suggests that the threat of sanctions and deterrents, like loss of reputation or financial penalties, can prevent malicious actions against information systems. Krassowski (2018) and Keinonen (2023) advocate for countermeasures, including education, training, and robust security protocols to bolster deterrence, emphasising the theory's foundational components of deterrence, prevention, detection, and remedy in maintaining cybersecurity.

The Theory of Technology-Enabled Crime delves into the complexities of criminal activities facilitated by advancements in computer and telecommunications technologies. (Gordon, 1995). Bregant and Bregant (2014) categorise technology-enabled crimes into direct offences against computer systems, cybercrimes utilising computers, the facilitation of traditional crimes through technology, and technology-aided crimes like fraud and harassment. This theory underscores the nuanced challenges posed by tech-enabled crimes. It stresses the importance of collaboration among regulators, enforcement agencies, and the public to effectively mitigate and combat cyber threats. The selection of the General Deterrence Theory and the Theory of Technology-Enabled Crime as theoretical frameworks is justified by their relevance to understanding and addressing cyber threats and security dynamics. GDT provides insights into the preventive measures and retaliatory actions necessary to deter potential cyber offenders. At the same time, the Technology-Enabled Crime theory offers a comprehensive perspective on the spectrum of crimes facilitated by technological advancements. Together, these theories furnish a robust conceptual foundation for examining the efficacy of cybersecurity measures in mitigating risks and protecting against cyber threats in Tanzania's digital infrastructure.

Empirical literature review : The proliferation of smartphones in Africa, predicted by Sulieman and Salleh to reach 660 million by 2020, has heightened the significance of mobile money services and their associated security risks (Sulieman & Salleh, 2020). Studies highlight the complexities of cybercrime, stressing the blurred lines in its definition and the challenges in law enforcement, as seen in England and India (Goswami, 2017; Jeandesboz et al., 2015). Bellini et al. (2023) also note mobile device security vulnerabilities, emphasising the increased risk to financial services. The global nature of cybercrime complicates criminal investigations, necessitating enhanced cooperation and resources (Setiabudi & Sumadinata, 2023; Hussain & Ibrahim, 2019). In Africa, increased internet usage has led to sophisticated cyber-attacks, with countries like South Africa facing substantial cyber risks due to inadequate cybersecurity measures (Olofinbiyi, 2022; Mohamed & Kamau, 2023). Cyberattacks on national security have a profound impact, and cybercrimes can cause significant financial and societal damage (Nayak, 2013). (Mbuthia, 2023; Aguboshim, Ezeife, & Obiokafor, 2022) Underscores African governments' technical and financial inadequacies in monitoring national security-sensitive electronic exchanges. Studies specific to Tanzania (Semboja et al., 2017; Semlambo et al., 2022) reveal adequate cybersecurity frameworks and preparedness, highlighting the need for comprehensive national policies and better institutional coordination.

Regarding measures against cyber vulnerabilities, research advocates for multifaceted security approaches, incorporating best practices and standards like ITIL and ISO (Lubua et al., 2022). The need for holistic security frameworks is emphasised, integrating technical, administrative, and compliance controls to address internal and external threats (Alotaibi et al., 2016; Alsowail & Al-Shehari, 2021)). Compliance with information security policies and regulations emerges as a critical factor in mitigating cyber risks, highlighting the importance of a comprehensive, multi-layered security strategy in enhancing IS security (Alsowail & Al-Shehari, 2021; Alotaibi et al., 2016). This empirical review synthesises findings from various studies to underscore the escalating challenge of cyber threats to national security, particularly in the African context, and the imperative for robust, integrated cybersecurity measures.

Despite the extensive research on the security vulnerabilities associated with mobile money services in Africa, including Tanzania (Pallangyo, 2022; Ntigwigwa, 2019), there is a notable gap in understanding the specific cybersecurity challenges and threats faced by government e-payment gateways in the region. Previous studies have predominantly focused on the broader landscape of cyber threats within the financial sector and the general internet user population, overlooking government digital financial services' unique vulnerabilities and security needs. This gap is significant given the increasing reliance on these gateways for public financial transactions and the potential national security implications of their compromise. Therefore, a focused investigation into the cybersecurity threats and challenges specific to government e-Payment gateways in Tanzania is warranted to develop targeted strategies for enhancing their security and resilience.

III. METHODOLOGY

This study employed a descriptive research design to systematically investigate the cyber threats to Tanzania's Government electronic Payment Gateway (GePG) and assess their impact on national security. As defined by Kothari (2019) and supported by Creswell (2014), descriptive research facilitated the comprehensive description and analysis of the situation, providing a narrative and interpretative emphasis without judgmental bias.A mixed-methods approach was adopted, integrating both quantitative and qualitative research methods. This combination allowed for a broader analysis of the research problem, balancing the strengths and weaknesses of each approach to yield a more comprehensive understanding of the cyber threats facing Tanzania's GePG (Creswell, 2012).

The study focused on the GePG, a critical component of the Tanzania Ministry of Finance and Planning in Dodoma, chosen for its central role in managing government financial transactions. The target population comprised 1420 officials from various departments within the ministry who were knowledgeable about cyber threats and their implications for national security (Oruj, 2023). Purposive and convenience sampling methods were utilised to select 200 respondents, with 190 for quantitative analysis and 10 for qualitative insights. This selection ensured a comprehensive representation of perspectives across the ministry's departments, facilitating a detailed examination of the cybersecurity landscape (Kothari, 2014).

Data were gathered through structured questionnaires and in-depth interviews with key informants, supplemented by a review of relevant documents. This triangulation of data sources enriched the study's findings, providing a multifaceted view of the cybersecurity challenges faced by the GePG (Kothari, 2019; Kebalepile et al., 2024). Quantitative data were analysed using SPSS and Microsoft Excel, employing descriptive and inferential statistics. Qualitative data underwent content analysis, integrating insights from interviews to complement the quantitative findings and provide a nuanced understanding of the cyber threats (Creswell, 2014). Validity was ensured through careful data interpretation, reducing researcher bias and delineating the phenomena under study. Reliability was achieved by using consistent data collection methods and instruments and by conducting the questionnaire in Kiswahili to facilitate understanding among respondents (Balińska, 2020) Ethical guidelines were strictly followed, research permits were obtained, and respondent confidentiality was maintained throughout the study. Participants' anonymity was preserved in the data analysis and reporting phases to uphold ethical standards and the integrity of the research process.

IV. FINDINGS AND DISCUSSIONS

This section comprehensively analyses the study's results, exploring the extent, impact, and nuances of cyber threats to Tanzania's Government Electronic Payment Gateway (GePG) and national security. It delves into the cyber threat landscape and security implications for Tanzania's GePG, the impact of cyber-attack threats on national security, and measures to protect against cyber-attack threats and improve national security.

Cyber Threat Landscape and Security Implications for Tanzania's GePG

Cyber Security Awareness and Its Impact on National Security : Understanding the level of cyber security awareness among staff is crucial for assessing the vulnerability of Tanzania's Government electronic Payment Gateway (GePG) to cyber threats. This section delves into the awareness levels of the respondents regarding cyber security threats and their implications for national security.

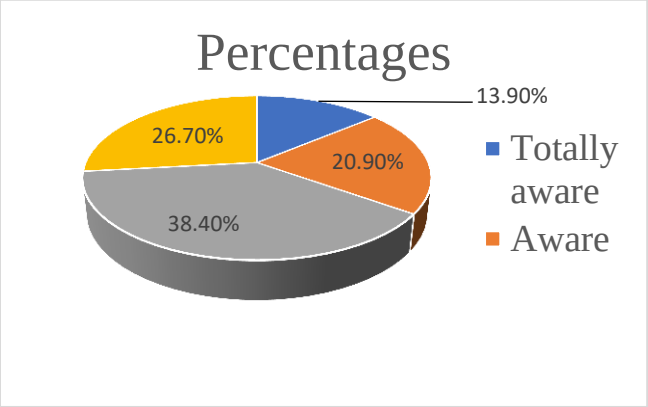

Figure 1: Staff awareness of cyber threats
Source: Researchers, 2024

The survey results highlight a concern for a need for cybersecurity awareness among staff. Nearly a third (26.7%) are entirely unaware of cyber threats to national security. This significant vulnerability needs to be addressed through comprehensive cybersecurity training programs. The data indicates a significant gap in cyber security awareness, with only a tiny fraction of respondents demonstrating a comprehensive understanding of its implications for national security. Most staff possess only partial awareness, highlighting the need for enhanced training and capacity-building programs. Interviews with key informants revealed insights into the awareness levels. One respondent stated, "The understanding of cyber threats among our staff is surface-level, compromising our ability to preempt and counter these threats effectively." Another noted, "There is a lack of continuous and in-depth training on the evolving nature of cyber threats, which leaves our systems and national security at risk."The findings resonate with the General Deterrence Theory (GDT) and the Theory of Technology-Enabled Crime, emphasising the importance of education and awareness in preventing cybercrime. The gap in cyber security awareness among the staff mirrors the challenges highlighted in the empirical literature, where the lack of adequate knowledge and training on cyber threats constitutes a significant vulnerability (Goswami, 2017; Jeandesboz et al., 2015) To bridge the awareness gap, comprehensive and continuous training programs are essential. These programs should focus on the basics of cyber security and the latest trends and tactics cybercriminals use. Creating a culture of cyber security awareness and preparedness within the organisation can enhance the resilience of Tanzania's digital infrastructure against cyber threats. Collaboration with cybersecurity experts and institutions can provide the necessary knowledge and skills to the staff, aligning with the best practices and standards mentioned in the literature review (Lubua et al., 2022; Alotaibi et al., 2016).

Incident Reporting and System Resilience in GePG : Understanding the occurrence of cyber-attacks within the Government's electronic Payment Gateway (GePG) systems is essential for evaluating the security and resilience of Tanzania's digital financial infrastructure. Data was collected and analysed to assess staff experiences with cyber-attacks on the GePG systems and their implications for national security.

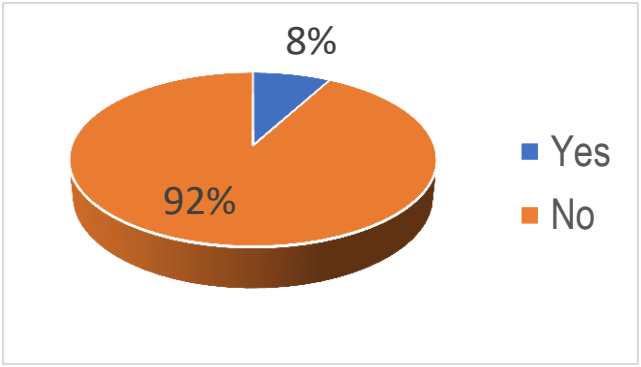

Figure 2: Cyber-attack within GEPG systems
Source: Researchers, 2024

According to Figure 2, provided by the researcher, 92% of respondents had never witnessed or experienced cyber-attacks affecting the GePG systems, while 8% stated they had witnessed such attacks. This quantitative analysis indicates a relatively low incidence of reported cyber-attacks, which could reflect the robustness of the current cybersecurity measures or a lack of awareness and underreporting of such incidents.Further qualitative insights from interviews with GePG system operators shed light on this issue. One operator mentioned, "Our system is generally secure, and direct cyber-attacks are rare. However, we occasionally face technical delays, which some might confuse with cyber incidents, mainly due to system overload or maintenance issues." This statement indicates that while direct cyber-attacks may be rare, operational challenges must be distinguished from cybersecurity issues.

The relatively low rate of reported cyber-attacks corroborates with the General Deterrence Theory, suggesting that the existing security measures may act as a deterrent against potential cyber criminals. The Theory of Technology-Enabled Crime also underscores the importance of continuously monitoring and upgrading systems to identify and mitigate cyber threats preemptively. However, the findings also highlight the need for improved cybersecurity awareness and training among staff, as echoed in the literature (Goswami, 2017; Jeandesboz et al., 2015), 2, to ensure that potential cyber incidents are recognised and reported promptly. Therefore, enhancing the cybersecurity posture of the GePG systems requires a multifaceted approach. Comprehensive cybersecurity training should be provided to all staff to improve their ability to recognise and report potential threats. Regular updates and audits of the systems are necessary to identify and address vulnerabilities. Additionally, establishing a robust incident reporting and response mechanism is critical for managing cyber threats effectively. By adopting these measures, the GePG can improve its resilience against cyber-attacks, contributing to the national security framework and safeguarding Tanzania's critical financial infrastructure.

The Efficiency of GePG's Information Retrieval : Assessing the performance of the Government electronic Payment Gateway (GePG) in terms of information retrieval speed is crucial for understanding its operational efficiency and user satisfaction. The GePG system's responsiveness directly impacts the effectiveness of financial transactions and the overall user experience.

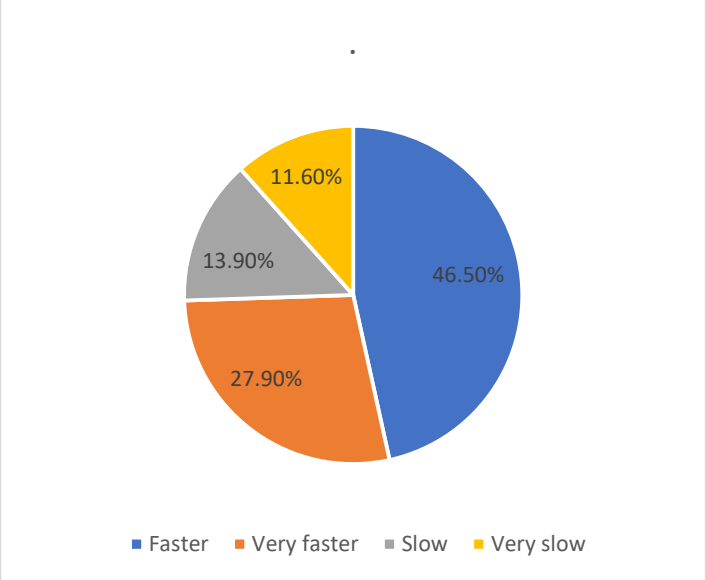

Figure 3: speed of GEPG system in retrieving information.
Source: Researchers, 2024

According to the study, respondents provided varied feedback on the speed of the GePG system in retrieving information. Figure 3, sourced from the researchers, indicates that 46.5% of the respondents found the retrieval speed of the GePG system to be fast, while 27.9% rated it as very fast. In contrast, 13.9% perceived the system as slow, and 11.6% considered it very slow. These mixed responses suggest that while most users experience satisfactory speeds, a significant minority face delays, which could affect the efficiency of their operations. The variation in perceived speed could be attributed to several factors, including inadequate ICT infrastructure, such as poor network bandwidth, power supply fluctuations, the type of electronic devices used to access the GePG,

and the system's server capacity. The correlation between system performance and infrastructure quality aligns with the theoretical insights from the Theory of Technology-Enabled Crime, which emphasises the role of technological advancements in enhancing or hindering operational efficiency, as Gordon (1995) suggested. Additionally, the empirical literature on cyberinfrastructure resilience suggests that technological capabilities, including network bandwidth and server capacity, are critical to system performance and reliability (Goswami, 2017; Jeandesboz et al., 2015). Therefore, addressing the issue of speed in information retrieval is not only a matter of enhancing user experience but also relates to the broader theoretical framework of maintaining robust and efficient digital infrastructure. The slow response time reported by some users points to potential areas for improvement, particularly in upgrading the ICT infrastructure to ensure faster and more reliable access to the system. Enhancing the network bandwidth, ensuring a stable power supply, and increasing server capacity are essential steps that can be taken to improve the performance of the GePG system.

These findings underscore the importance of continuously monitoring and upgrading the system's infrastructure to meet its users' growing demands and expectations. As the GePG plays a pivotal role in Tanzania's financial transactions, its efficiency and reliability are paramount in fostering trust and confidence among its users. Therefore, addressing the identified issues related to information retrieval speed is imperative for maintaining the integrity and effectiveness of the GePG system, thereby supporting the country's broader financial and economic stability.

The Impact of Cyber-Attack Threats on National Security.

The Influence of Cyber-Attacks on *The* GEPG System and National Security : Understanding the influence of cyber attacks on the Government Electronic Payment Gateway (GePG) system and broader national security is paramount for developing effective cybersecurity strategies in Tanzania. The study's respondents provided insights into the main factors contributing to the GePG system's vulnerability and, by extension, national security.

Table 1: The influence of cyber-attacks on the GEPG system and national security at large

Variables	Frequency	Percent
High penetration rate of smartphones	24	16
Insufficient of the policy	18	12
Inadequacy of server-side devices	22	14.7
Weaknesses in the technology infrastructure	54	36
Technical security loopholes	32	21.3
Total	**150**	**100.0**

Source: Researchers, 2024

According to Table 1, the majority of respondents (36%) identified technological infrastructure weaknesses as the most significant factor influencing cyber-attacks impact on the GePG system and national security. Technical security loopholes were also a major concern, with 21.3% of respondents highlighting them. Other factors included the high penetration rate of smartphones (16%), inadequacy of server-side devices (14.7%), and insufficient policy measures (12%). These findings suggest that technological and infrastructural vulnerabilities are the primary enablers of cyber-attacks affecting the GePG system. The high penetration rate of smartphones indicates a growing attack surface due to the widespread use of mobile devices, which can exacerbate security risks if not adequately managed. The inadequacy of server-side devices and technical security loopholes further underscore the critical need for robust, secure infrastructure to withstand potential cyber threats.The reported influence of insufficient policy measures on cyber-attacks highlights the importance of comprehensive and enforceable cybersecurity policies to guide the protection of digital assets. This aligns with the General Deterrence Theory, which posits that strong policies and deterrents can reduce the incidence of cybercrime (Grasmick & Bryjak, 1980). Furthermore, the empirical literature supports that combining technological enhancements and policy improvements is essential for mitigating cyber risks (Goswami, 2017; Jeandesboz et al., 2015). To mitigate the influence of these factors on national security, there needs to be a concerted effort to strengthen the technological infrastructure and enact robust cybersecurity policies. Improving server capacity,

addressing technical security loopholes, and enhancing the overall technology infrastructure can significantly reduce the vulnerability of the GePG system to cyber-attacks. Concurrently, developing and implementing comprehensive cybersecurity policies will provide a structured framework for protecting national digital assets against cyber threats.

Thus, cyber-attacks influence the GePG system, and national security is a multifaceted issue that requires a holistic approach. Enhancing the technological infrastructure, closing security gaps, and strengthening policy frameworks are critical steps toward safeguarding Tanzania's digital and financial ecosystems against the evolving landscape of cyber threats.

Cyber-attack Scenarios and Their Implications for National Security : Understanding potential cyber-attack scenarios and their impacts on national security is crucial for developing effective countermeasures. The study explored various cyber-attack scenarios that could threaten Tanzania's national security, focusing on their frequency and perceived impact.

Table 2: cyber-attack scenarios and its impact on national security

	Frequency	Percent
Cyber terrorist acts	24	16
Damaged of the expected economic growth	18	12
Infrastructure damage	22	14.7
Loss of essential data	54	36
Total	**150**	**100.0**

Source: Researchers, 2024

The table reveals that the loss of essential data is perceived as the most significant threat, with 36% of respondents identifying it as a key cyber-attack scenario impacting national security. This is followed by cyber-terrorist acts (16%), infrastructure damage (14.7%), and damage to expected economic growth (12%). Respondents provided insights into the nature of these threats. One participant stated, "The loss of essential data could paralyse government operations and severely undermine public trust." Another noted, "Cyber terrorist acts pose a unique threat as they aim to disrupt societal functions and instil fear among the populace."These scenarios align with the General Deterrence Theory, which suggests that the threat of significant penalties can deter malicious cyber activities. The Theory of Technology-Enabled Crime also supports the need for robust cybersecurity measures to protect against the diverse threats posed by technological advancements. The empirical literature underscores the multifaceted nature of cyber threats and their potential to disrupt national security, economic stability, and critical infrastructure, mirroring the concerns of the study's respondents (Grasmick & Bryjak, 1980; Gordon, 1995).

A comprehensive national cybersecurity strategy is imperative to mitigate these threats. This strategy should include enhancing data protection mechanisms, strengthening infrastructure security, and developing robust countermeasures against cyber terrorism. Collaborative efforts among government, industry, and international partners are essential to bolster the nation's defence against these evolving cyber threats, ensuring the protection and resilience of Tanzania's national security.

Increasing Trends of Cyber Threats and Their Implications : Assessing the perception of the increase in cyber threats provides insights into Tanzania's evolving landscape of cybersecurity challenges. The study aimed to determine if stakeholders believe cyber threats are increasing more now than ever.

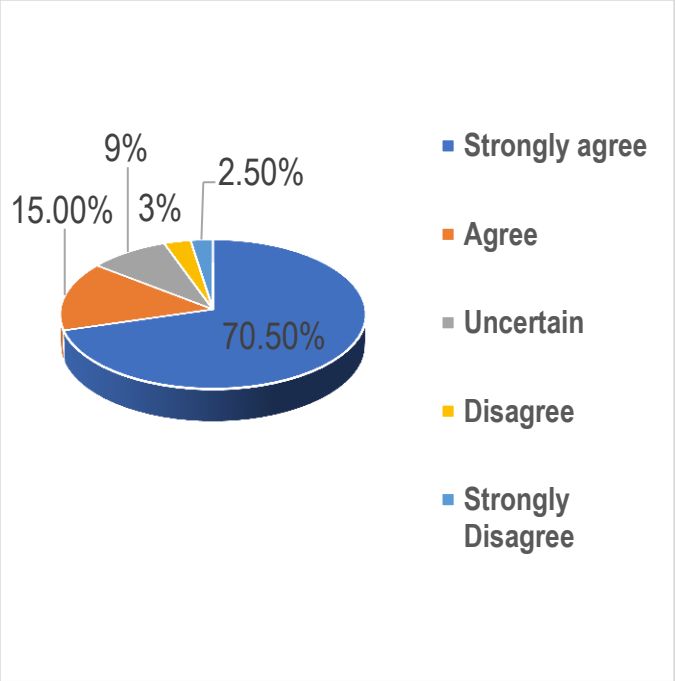

Figure 4: Cyber threat trends
Source: Researchers, 2024

The figure indicates that 54% of the participants strongly agree that cyber threats are increasing, with 22% agreeing and 15% undecided. The data clearly shows a predominant belief among respondents that cyber threats are escalating. Most of the study's participants perceive increased cyber threats, reflecting a growing concern within the cybersecurity community. The trend of increasing cyber threats is supported by Siegel et al. (2017), who noted that the most common types of computer fraud involve operations where intangible assets, such as data and money transactions, are lucrative targets. This perspective is particularly relevant in Tanzania, where internet penetration and technological advancements have expanded the attack surface for cybercriminals.
The observed increase in cyber threats correlates with the theoretical understanding that technological progress, while beneficial, also presents new opportunities for cybercrime. The findings resonate with empirical studies indicating a global surge in cyber threats, particularly in regions with rapidly expanding digital infrastructures like Africa.

Given the increasing trend of cyber threats, particularly in the form of cyber fraud in mobile banking, there is a critical need for comprehensive cybersecurity education and awareness programs in Tanzania. Most users with limited knowledge of cybersecurity are vulnerable to internet fraud. Therefore, enhancing cybersecurity awareness among the public and strengthening the security measures of digital platforms, especially in banking and financial services, are imperative. Establishing robust cybersecurity frameworks and fostering a culture of security among internet users can significantly reduce the incidence of cyber threats and safeguard national security.

Emerging Patterns of Cyber Threats as a National Security Concern in Tanzania : The study sought to ascertain stakeholders' perceptions of the emergence of patterns in cyber technology threats and their impact on national security in Tanzania. Identifying these patterns is crucial for understanding the evolving nature of cyber risks associated with technological advancements.

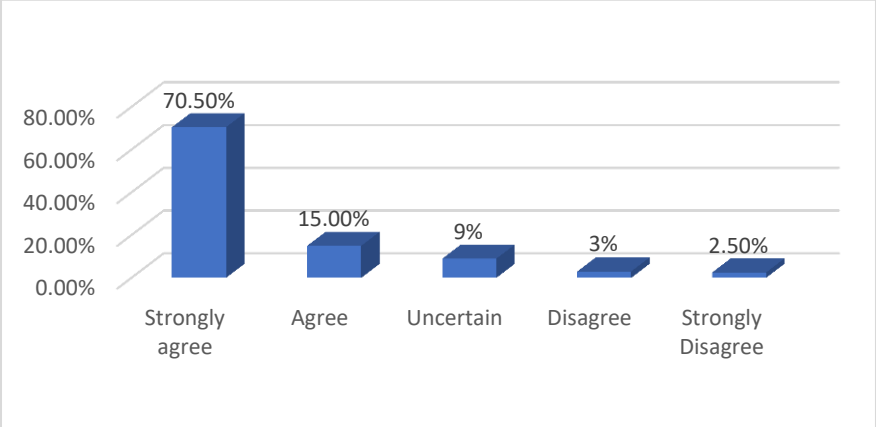

Figure 5: Increase in Pattern of Cyber Threats
Source, Researcher, 2024

The survey results showed a varied perception among the participants: 0.5% strongly agree, 15% agree, and 9% remain undecided about the emergence of discernible patterns in cyber threats as a national security concern. The relatively low percentage of agreement on the emergence of patterns in cyber threats could indicate a need for more awareness or understanding among the respondents about the evolving nature of these threats. However, the acknowledgement by a segment of the participants suggests some level of recognition of the issue. Various studies have acknowledged the evolving complexity of information technologies and the associated cyber threats, including the TCRA Cyber Security Report (2019), which notes that Tanzania is a significant consumer of information technologies. This consumption is paralleled by increased cyber-attacks, especially those targeting national infrastructure.

The recognition of emerging patterns of cyber threats aligns with the Theory of Technology-Enabled Crime, which posits that technological advancements can lead to new forms of criminal activities (Gordon, 1995). The findings also corroborate with empirical studies indicating that the rapid adoption of digital technologies increases cyber-attack vulnerabilities (Keller, 2017). To address the emerging patterns of cyber threats, Tanzania needs to adopt a proactive approach to its national cybersecurity strategy. This includes continuous monitoring of cyber threat landscapes, enhancing the technical capacity to deal with sophisticated cyber-attacks, and promoting cybersecurity awareness among the population. Strengthening collaboration between governmental bodies, the private sector, and international partners is also vital to effectively mitigate the risks posed by the evolving nature of cyber threats to national security.

The Measures to Protect Against Cyber-Attack Threats on Improving National Security.
Understanding Cybersecurity Policies, Strategies, and Legal Frameworks in Tanzania : The study evaluated the respondents' awareness and knowledge of Tanzania's cybersecurity policies, strategies, and legal frameworks. Understanding these aspects is crucial for the effective implementation and adherence to cybersecurity measures against cyber-attacks.

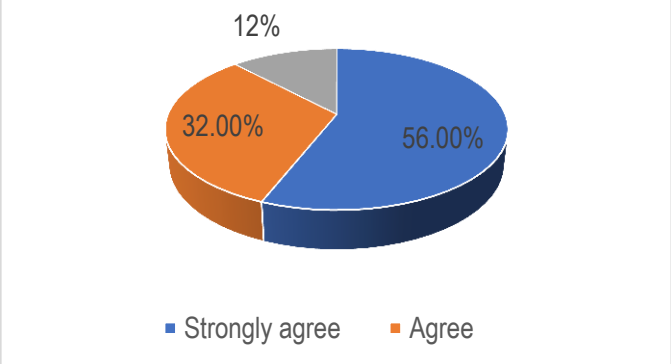

Figure 6: Awareness of Cybersecurity Policies, Strategies, and Legal Framework
Source, Researcher, 2024

The survey results indicated that 56% of respondents strongly agree that the Cyber Security Policy has effectively mitigated cyber-attacks, while 32% agreed, and 12% were unaware of these policies. A significant majority of the respondents acknowledge the existence and efficacy of cybersecurity policies in mitigating cyber threats. However, there appears to be a gap in detailed knowledge of these policies, as indicated by the limited number of respondents who could precisely identify specific legislation like the Cyber Act of 2015. During the interviews, approximately 25% of participants could identify the Cyber Act of 2015, while 64% were unable to name any specific policy, and 11% needed clarification. One respondent remarked, "We know there are policies in place, but the specifics and how they apply to our daily operations remain unclear."

The findings highlight the critical need to enhance awareness and understanding of cybersecurity policies and strategies. This need aligns with the General Deterrence Theory, which posits that awareness of legal frameworks and policies can deter cybercriminal activities. The empirical literature also supports the importance of comprehensive cybersecurity policies and education in mitigating cyber threats (Keller, 2017). Comprehensive education and training programs focusing on cybersecurity policies, strategies, and legal frameworks are imperative to bridge the knowledge gap. Ensuring that individuals and organisations are well-informed about the existing cybersecurity measures and their legal obligations can enhance compliance and the overall effectiveness of these policies in combating cyber threats. Furthermore, regional collaboration and learning from the cybersecurity initiatives of other African states can provide valuable insights and strengthen Tanzania's approach to cybersecurity.

Assessment of Cybersecurity Measures in Tanzania : The study sought to ascertain Tanzania's key cybersecurity measures and strategies to combat cyber threats. This assessment helps in understanding the extent of the country's preparedness and response to the evolving landscape of cyber risks.

Table 4: Cyber security measures in Tanzania

	Frequency	Percent
Central Bank of Tanzania cyber guideline	24	16
Cyber Police Framework	14	9.3
Cyber Security Government	22	14.6
Tanzania cybercrimes act, 2015	50	33.3
The Electronic and Postal Communications Act, 2022	20	13.3
Tanzania Information and Communications Act	12	8
Government Cyber Security Strategy 2022–2027	8	5.3
Total	**150**	**100.0**

Source: Researchers, 2024

The Tanzania Cybercrimes Act of 2015 was the most frequently mentioned measure, cited by 33.3% of respondents, indicating its prominence in the national cybersecurity landscape. Other significant measures include the Central Bank of Tanzania's cyber guidelines and the Cyber Security Government initiatives. The findings reflect discussions from the Cyber Defence East Africa 2017 Conference, highlighting Tanzania's comprehensive approach to cyber security, encompassing legal frameworks, institutional structures, and strategic collaborations. Developing the Tanzania National Cyber Security Master Plan 2022/2023 and response centres exemplifies the country's proactive stance in securing its ICT infra-structure. The identified cyber security measures align with the proactive and preventive approach advocated by the General Deterrence Theory in curbing cyber threats. The empirical literature, reflecting on the necessity of robust legal and institutional frameworks for effective cyber security, supports these findings (Keller, 2017). To enhance cyber security in Tanzania, continuous evaluation and strengthening of the existing measures are essential. This includes updating legal frameworks, enhancing institutional capacities, and fostering national and international collaboration.

Developing cyber security expertise and public awareness are crucial in creating a resilient and secure cyber environment in Tanzania.

Progress and Challenges in Tanzania's Cyber security Efforts : The study explored Tanzania's perceived achievements and challenges in combating cyber threats. Understanding these aspects is vital for assessing the effectiveness of the country's cyber security strategies and identifying areas for improvement.

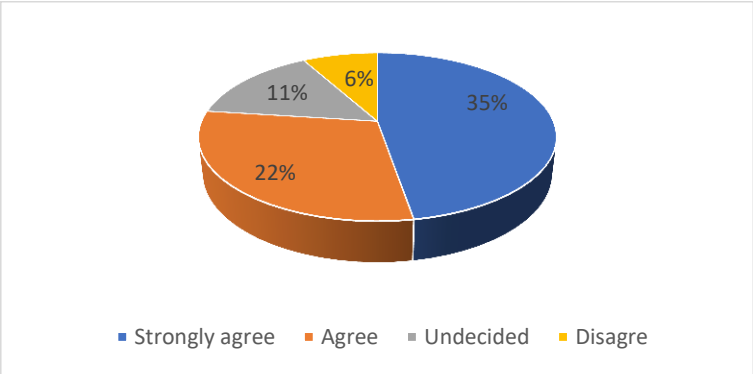

Figure 7 Achievements in the fight against cyber threats
Source, Researchers, 2024

The survey indicated that 35% of respondents strongly agree there have been achievements in combating cyber threats, 22% agree, 11% are undecided, and 6% disagree. Most respondents acknowledge progress in Tanzania's cyber security initiatives, particularly in developing a national cyber security framework and legislation for electronic identification. Those who agreed or strongly agreed cited establishing consumer awareness programs and national cyber security initiatives as key accomplishments. However, the undecided respondents pointed to the vulnerabilities in Tanzania's cyberspace due to rapid digitalisation without corresponding advancements in defence capabilities.

The achievements in cyber security align with proactive strategies advocated in the cyber security literature. They are consistent with the General Deterrence Theory, which emphasises the importance of comprehensive measures to prevent cyber threats. The challenges highlighted by respondents reflect concerns raised in the cyber security field about the pace of technological advancements outstripping the development of security measures (Cyber Security, 2015). To build on the achievements and address the challenges in cyber security, Tanzania needs to continue developing its legal and regulatory framework, enhance public awareness programs, and bolster the technical capabilities of cyber security institutions. Strengthening collaboration with regional and international partners will also be crucial in addressing cyber threats' sophistication and transnational nature. Investing in research and development to keep pace with technological advancements will further enhance Tanzania's resilience against cyber threats.

Inferential Analysis : This section examines the relationships between independent variables and the dependent variable, focusing on how Cyber Threats (CT), Cyber-attack Scenarios (CS), and Cyber Security Policies (CP) influence National Security (NS).

Correlation Analysis : The correlation analysis aims to identify the strongest predictors among the independent variables concerning the dependent variable. The results, displayed in Table 4.10, indicate varying degrees of correlation.

Table 5: Correlation Analysis

	NS	CT	CS	CP
NS	1.000000			
CT	0.823363	1.000000		
CS	0.522747	0.631797	1.000000	
CP	0.356746	0.588233	0.105620	1.000000

Source: Field data, 2024

The data reveals that Cyber Threats (CT) exhibit the highest correlation with National Security (NS), suggesting that CTs significantly impact NS more than other variables. The correlation coefficients are sufficiently distinct, indicating no multicollinearity concerns, which typically require management through regression analysis.

Regression Analysis : The relationship between the independent and dependent variables was further examined using the Ordinary Least Squares (OLS) regression method. The detailed outcomes are presented in Table 4.11:

Table 6: Regression Analysis

Dependent Variable: NS
Method: Least Squares
Sample: 150

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.015981	0.002121	-7.534967	0.0000
CT	0.199748	0.003571	55.93454	0.0114
CS	0.129404	0.016955	7.632024	0.0829
CP	0.030058	0.002319	12.96068	0.0490

R-squared	0.719336	Mean dependent var	0.012950
Adjusted R-squared	0.708150	S.D. dependent var	0.014210
S.E. of regression	0.000285	Akaike info criterion	-13.63631
Sum squared resid	8.10E-08	Schwarz criterion	-13.77485
Log likelihood	45.84893	Hannan-Quinn criter.	-14.31798
F-statistic	3906.937	Durbin-Watson stat	2.315326
Prob(F-statistic)	0.011998		

Source: Field data, 2024

The study results on regression analysis depict that among the variables tested national security as the dependent variable, two predictors, namely Cyber Threats (CT) and Cyber-attack Scenarios (CS), constitute a significant effect on national security since $p<0.05$; In contrast, Cyber security Policies (CP) has been generated insignificant on national security with $p>0.05$ This implies that national security in Tanzania is affected with Cyber Threat (CT), Cyber-attack Scenarios (CS) and Cyber security Policies. Also, this study indicates that in Tanzania, cyber security policies are poorly implemented in government information systems. This indicates that the most common reason for individuals and organisations being vulnerable to cyber-attacks is the ignorance of security measures that need to be taken by the customers and employees of these organisations. Also, weak platforms that organisations have set up online make institutors vulnerable to breaches of information or even monetary losses. This is common in mobile money platforms. Law enforcement has failed to curtail this problem because of inadequate training, not only policemen but also judicial officers, who have difficulty understanding the technicalities of such issues.

V. CONCLUSION AND RECOMMENDATIONS

Conclusion : This study concludes that the rapid advancement of technology has significantly increased vulnerabilities to cyber-attacks, affecting individuals, organisations, and governments globally. With the expansive use of the internet and digital applications, the cyber domain has become a prominent target for threats that exploit, disrupt, or damage the infrastructure critical for information processing, communication, and storage. A notable finding of the study is the widespread lack of cyber threat awareness among staff in government sectors, contributing to substantial financial and informational losses. Current cyber security measures are inadequate, often due to the absence of established security practices necessary for protecting critical cyber infrastructure. Moreover, the ease of accessing information in the digital age, where personal data is readily available through social media and other online platforms, exacerbates these vulnerabilities. Therefore, Tanzania urgently needs to revise its cybersecurity strategies to develop robust national policies that enhance threat management capabilities to anticipate, detect, respond to, and contain cyber security threats effectively.

Recommendations: This study recommends enhancing cyber literacy across all levels of society, emphasising the importance of integrating cyber security education early to build a resilient digital culture. It advocates for a collaborative approach among stakeholders to bolster national cybercrime management and strengthen defences by equipping government networks with necessary firewalls and antivirus software. Additionally, it suggests promoting awareness about potential cyber dangers in organisational settings and encouraging the use of secure IT products to mitigate risks and prevent breaches effectively.

REFERENCES

1. Aguboshim, F. C., Ezeife, J. E., & Obiokafor, I. N. (2022). Managing organisation information security systems, conflicts, and integrity for sustainable Africa transformation. World Journal of Advanced Research and Reviews. Retrieved from https://api.semanticscholar.org/CorpusID:248728381
2. Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. International Journal for Information Security Research (IJISR), 6(2), 160-166. Retrieved from https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security- Awareness.pdf
3. Alsowail, R., & Al-Shehari, T. (2021). A Multi-Tiered Framework for Insider Threat Prevention. Electronics, 10. Retrieved from https://api.semanticscholar.org/CorpusID:234919982
4. Balińska, A. (2020, March 22). Data collection methods in rural tourism in the eyes of respondents. Studia Periegetica, 29(1), 115–126. https://doi.org/10.5604/01.3001.0014.1234
5. Bellini, R., Lee, K., Brown, M. A., Shaffer, J., Bhalerao, R., & Ristenpart, T. (2023). The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. USENIX Security Symposium. Retrieved from https://api.semanticscholar.org/CorpusID:260777707
6. Brenner, W. (2010). Cybercrime: Criminal Threats from Cyber Space. Santa Barbara, California: Greenwood Publishing Group, p. 38.
7. Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. Law, Computer Science. Retrieved from https://api.semanticscholar.org/CorpusID:152608546
8. Creswell, J. W. (2012). Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research. Upper Saddle River, NJ: Prentice Hall.
9. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed approaches (3rd Ed). London: Sage Publications
10. Fripp, C. (2014). This is why Africa is a cybercrime target. [Online] Available at: http://www.htxt.co.za/2014/11/12/this-is-why-africa-is-a-cybercrime-target/ [Accessed 30 November 2014].
11. Goswami, P. K. (2017). Cyber crime: the legislative enactments and the interpretation of the judiciary with special reference to India. The Clarion- International Multidisciplinary Journal, 6, 91-94.
12. Gordon, S. (1995). Technologically enabled crime: Shifting paradigms for the Year 2000. Comput. Secur, 14, 391-402. Retrieved from https://api.semanticscholar.org/CorpusID:46059284
13. Griffiths, J.L. (2016). Cyber Security as an Emerging Challenge to South African National Security.
14. Grasmick, H. G., & Bryjak, G. J. (1980). The Deterrent Effect of Perceived Severity of Punishment. Social Forces, 59, 471-491.
15. Hobbes T (1651) Leviathan: Or the Matter, Forme and Power of a Commonwealth Ecclasiasticall and Civil. Menston: Scolar Press.
16. Hussain, W. S., & Ibrahim, N. J. (2019). A Survey of Cybercrimes, Investigations and Penal Laws Imposed on the Criminals. Law. Retrieved from https://api.semanticscholar.org/CorpusID:212607514
17. Jeandesboz, B. H., Ragazzi, F., Simon, S., & Mitsilegas, V. (2015). The law enforcement challenges of cybercrime: are we really playing catch-up? Law, Computer Science. Retrieved from https://api.semanticscholar.org/CorpusID:167905993
18. Keinonen, M. (2023). The Concept of Comprehensive Security as a Tool for Cyber Deterrence. European Conference on Cyber Warfare and Security. Retrieved from https://api.semanticscholar.org/CorpusID:259292173
19. Keller, J. P. (2017, July). Patient safety implications with the rapid adoption of IT-based health technologies. Digital Medicine, 3(3), 115–119. https://doi.org/10.4103/digm.digm_20_17
20. Kebalepile, M. M., Dzikiti, L. N., & Voyi, K. (2024, February 28). Using Diverse Data Sources to Impute Missing Air Quality Data Collected in a Resource-Limited Setting. Atmosphere, 15(3), 303. https://doi.org/10.3390/atmos15030303
21. Kothari, C. K. (2014). Research methodology; methods and techniques, second revised edition. New Delhi: New age International (P) Limited

22. Kothari, C.R. (2019). Research Methodology: Methods and Techniques. 4th Edition, New Age International Publishers, New Delhi.
23. Krassowski, K. (2018). A concept of information and education of a human as tool of prevention of cyberspace threats. Journal of Modern Science. Retrieved from https://api.semanticscholar.org/CorpusID:158405180
24. Kshetri, N. (2017). Global Cybersecurity: Issues and Concerns [Editorial]. Computer Science, Law. Retrieved from https://api.semanticscholar.org/CorpusID:117302682
25. Lubua, E. W., Semlambo, A. A., & Mkude, C. G. (2022). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar es Salaam Library Journal, 17(2), 94- 114.
26. MacAfee. (2014). MacAfee Labs Threats Reports. June 2014.
27. Mbuthia, P. M. (2023). Implications of increased foreign surveillance technologies on national security in Africa. Scientific Scholer. Retrieved from https://api.semanticscholar.org/CorpusID:261130644
28. Mohamed, A. Y., & Kamau, S. K. (2023). A Continent-Wide Assessment of Cyber Vulnerability Across Africa.Ar Xiv, abs/2301.03008. Retrieved from
29. https://api.semanticscholar.org/CorpusID:255546218
30. Nawalagatti, A. (2022) Analysis of Security and Privacy issues in social networks. International journal 0f creative research thoughts (IJCRT).
31. Nayak, S.D.T. (2013). Impact of Cyber Crime: Issues and Challenges. International Journal Of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©Ijeset.
32. Ntigwigwa, A.N. (2019).Factors that Contribute to Cybercrime in Mobile Money Services in Tanzania: A Case of Kibaha Town"
33. Olayemi Yagoda, B. (2015). "A Short History/ of "Hack"". The New Yorker. Retrieved November 3, 2015.
34. Olofinbiyi, S. A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. ScienceRise: Juridical Science. Retrieved from https://api.semanticscholar.org/CorpusID:250209518
35. Oruj, Z. (2023, February 24). CYBER SECURITY: CONTEMPORARY CYBER THREATS AND NATIONAL STRATEGIES. Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects, 2, 100–116. https://doi.org/10.18372/2786-5495.1.17309
36. Pallangyo, H. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. Tanzania Journal of Engineering and Technology. Retrieved from https://api.semanticscholar.org/CorpusID:251425859
37. Semboja, H.H., Silla, B. & Musuguri, J.N. (2017). Cyber-security Institutional Framework in Tanzania: A Policy Analysis. Global Scientific Journals. GSJ: Volume 5, issue 6: ISSN2320-9186.
38. Semlambo, A. A., Lubua, E. W., & Mkude, C. G. (2023). The Quality of Information Systems Security Policies in Addressing Security Challenges in Public Learning Institutions of Tanzania. International Journal of Technology and Management, 8(1), 1-22.
39. Semlambo, A., Lubua, E. W., & Mkude, C. (2022). Information Systems security policy framework for enhanced ICT governance in public institutions of Tanzania. The Journal of Informatics, 2(1), 54- 68.
40. Setiabudi, W., & Sumadinata. (2023). Cybercrime And Global Security Threats: A Challenge In International Law. Law, Political Science, Computer Science. Retrieved from https://api.semanticscholar.org/CorpusID:259197920
41. Siahaan, A. P. (2018). Impact of Cybercrime on Technological and Financial Developments. Computer Science, Law, Economics, Business. Retrieved from https://api.semanticscholar.org/CorpusID:239780165
42. Statista.com. (2023). Cybercrime and the financial industry in the United States - Statistics & Facts. Available at https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/#topicOverview. Published by Ani Petrosyan, March 28, 2023
43. Sulieman, D. M., & Salleh, F. (2020). Anti-Money Laundering Risk Posed By Mobile Money Services In Sub-Saharan Africa. Business, Economics, Law. Retrieved from https://api.semanticscholar.org/CorpusID:226434897
44. Yonazi, J., (2012). Cyber Security in Tanzania; Report on from the Cyber-Security Mini-Conference, Center for ICT Research and Innovations