ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Cybersecurity Governance in Tanzania: Assessing Legal and Institutional Responses to Rising Cybercrime

Herbert Wanga

University of Iringa, Tanzania

ABSTRACT

The rapid expansion of digital technologies in Tanzania has brought significant socio-economic benefits, but it has also introduced new challenges, particularly the rise of cybercrime. This article examines the evolving landscape of cybercrime in Tanzania through a cybersecurity governance lens, analyzing prevalent threats such as financial fraud, identity theft, and cyberterrorism, as well as the legal and institutional frameworks designed to combat these crimes. Despite the enactment of the Cybercrimes Act (2015), Tanzania faces persistent challenges, including inadequate enforcement, limited public awareness, and jurisdictional complexities. Drawing on a systematic review of recent studies (2018-2024) and Tanzanian case reports, this article highlights the urgent need for comprehensive legal reforms, enhanced cybersecurity infrastructure, and international cooperation. Recommendations include updating legislation to align with the Budapest Convention, launching targeted public awareness campaigns, and fostering multi-stakeholder collaboration to safeguard Tanzania's digital future.

***Corresponding author**

Herbert Wanga, University of Iringa, Tanzania

Received: December 16, 2025; **Accepted:** December 22, 2025, **Published:** June 27, 2026

Keywords: Cybercrime, Tanzania, Cybersecurity, Digital Governance, Legal Frameworks, Financial Fraud

Introduction

The digital revolution has transformed Tanzania's socio-economic landscape, enabling advancements in communication, finance, and governance [1]. Internet penetration in Tanzania rose from 23% in 2017 to over 46% in 2023 while mobile money transactions exceeded TZS 12 trillion monthly [2,3]. However, this progress has also exposed the country to cybercrime, a global menace that threatens individuals, businesses, and national security [4]. Cybercrime encompasses illegal activities such as financial fraud, hacking, identity theft, and cyberterrorism, all of which are increasingly prevalent in Tanzania. With rising digital adoption, cybercriminals exploit vulnerabilities in Tanzania's cybersecurity infrastructure, necessitating robust and governance-oriented countermeasures [5].

Research Gap and Contribution: While existing studies have documented cybercrime trends in Tanzania, few have critically analyzed the governance and institutional gaps within the cybersecurity ecosystem. This article addresses this gap by evaluating Tanzania's legal and operational frameworks through a cybersecurity governance lens, integrating recent case studies and regional comparisons. The study aims to provide actionable, context-specific recommendations for policymakers, regulators, and private stakeholders.

This article is structured as follows: Section 2 outlines the methodology; Section 3 examines the state and forms of cybercrime; Section 4 analyzes the legal and institutional frameworks; Section 5 discusses key challenges; Section 6 offers targeted recommendations; and Section 7 concludes.

Methodology

This study adopts a qualitative desk review methodology, allowing for a careful and contextual synthesis of existing knowledge on cybercrime in Tanzania and the wider East African region. Rather than generating new empirical data, the approach prioritizes depth, interpretation, and triangulation of credible secondary sources in order to capture how cybercrime is understood, governed, and addressed in practice.

Specifically, the analysis draws on several complementary categories of materials. First, it reviews peer-reviewed academic literature published between 2018 and 2024, with a focus on cybercrime trends, digital financial fraud, regulatory challenges, and institutional responses in Tanzania and East Africa. This body of scholarship provides the theoretical grounding and situates Tanzania's experience within broader regional and global debates.

Second, the study examines official government and regulatory reports, including publications and public statements from the Tanzania Communications Regulatory Authority, the Bank of Tanzania, and the Tanzania Police Cyber Unit. These sources offer authoritative insights into national policy priorities, reported cyber incidents, enforcement capacity, and institutional mandates.

Third, the review incorporates case studies and incident reports drawn from reputable local media outlets and cybersecurity firms operating in Tanzania. These materials help humanize the analysis by illustrating how cybercrime manifests in real-world settings, particularly in relation to mobile money fraud, online scams, and attacks on financial institutions.

Fourth, the study considers regional policy and strategic documents, notably frameworks developed under the auspices of the East African

Community. These documents are used to assess the extent of regional harmonization, cross-border cooperation, and shared legal and institutional responses to cyber threats.

Finally, the analysis is informed by international normative instruments and best-practice guidelines, including the Budapest Convention and the AU Malabo Convention. These frameworks serve as benchmarks against which Tanzania's legal and governance arrangements are evaluated.

Overall, the review is analytically anchored in a cybersecurity governance framework, with particular attention to the interaction between institutions, legal frameworks, enforcement mechanisms, and multi-stakeholder coordination. This lens enables the study to move beyond isolated incidents and instead examine cybercrime as a systemic governance challenge shaped by policy coherence, institutional capacity, and collaboration across public and private actors.

The State of Cybercrime in Tanzania

Prevalence and Forms of Cybercrime

Cybercrime in Tanzania manifests in various forms, including:

i. **Financial Fraud:** Mobile money platforms, such as M-Pesa and Tigo Pesa, are prime targets for phishing scams, SIM-swapping fraud, and unauthorized transactions [2]. A 2023 study in Kongwa District found that 76.7% of respondents attributed fraud to technical security loopholes [6]. Recent cases include smishing attacks targeting bank customers.

ii. **Identity Theft:** Weak data protection laws enable cybercriminals to steal personal information via social engineering or malware attacks; updated with social media scams accounted for 42% of reported identity theft cases in 2022 [2].

iii. **Cyberterrorism:** Extremist groups leverage encrypted platforms for recruitment and propaganda, posing risks to national security [7]. Tanzania's proximity to conflict zones amplifies this threat.

iv. **Cyberbullying and Harassment:** Social media platforms are increasingly used for cyberbullying, particularly targeting women and youth. A 2022 survey found that 1 in 3 female internet users experienced online harassment [8].

v. **Emerging Threats:** Cryptocurrency fraud, ransomware attacks on SMEs, and AI-driven disinformation are growing concerns [9].

Economic and Social Impacts

Cybercrime has far-reaching consequences. Financial losses are estimated at TZS 1.2 trillion annually, with SMEs disproportionately affected. Beyond economic harm, cybercrime erodes trust in digital systems and exacerbates social inequalities, particularly for women and rural populations; updated with [3,10].

Legal and Institutional Frameworks

National Legislation

Tanzania's primary legislative tool is the Cybercrimes Act (2015), which criminalizes offenses such as unauthorized access, data interference, and cyber harassment [11]. However, the Act has been criticized for vague definitions and potential human rights infringements (e.g., on freedom of expression). Other relevant laws include:

- **The Electronic and Postal Communications Act (2010):** Regulates digital communications but lacks provisions for ransomware and crypto-crimes.
- **The Personal Data Protection Act (2022):** A recent addition that strengthens data governance but is yet to be fully operationalized.
- **The Anti-Money Laundering Act (2009):** Targets financial crimes but does not explicitly address cyber-enabled fraud.

Institutional Landscape

Institutions such as the Tanzania Police Cyber Unit and the TCRA are tasked with addressing cyber threats but face resource constraints and skill shortages. The Bank of Tanzania's Cybersecurity Guideline (2023) is a positive step but not legally binding.

Regional and International Alignment

Tanzania has not ratified the Budapest Convention or the AU Malabo Convention on Cyber Security, limiting cross-border collaboration. By comparison, Kenya's Computer Misuse and Cybercrimes Act (2018) includes clearer provisions on digital evidence and public awareness [12].

Challenges in Combating Cybercrime

Tanzania continues to face a complex and evolving cyber-security landscape, and several structural and socio-technical challenges limit the country's ability to respond effectively.

First, *inadequate cybersecurity infrastructure* remains a foundational barrier. Many public and private institutions still rely on outdated systems, lack real-time threat-monitoring tools, and have minimal incident-response capabilities. As (2020) observe, this leaves organizations reactive rather than proactive, creating an environment where breaches can go undetected for long periods.

Second, *low public awareness and digital literacy* significantly heighten vulnerability. Although mobile money has become deeply embedded in everyday life, more than 60 percent of users are unaware of basic security practices, such as safeguarding PINs, recognizing phishing attempts, or verifying transaction authenticity [6]. This human-factor gap provides fertile ground for social-engineering attacks and scams.

Third, *jurisdictional and coordination gaps* complicate enforcement. Cybercrime is inherently transnational, yet Tanzania lacks comprehensive extradition treaties and cross-border collaboration mechanisms specifically tailored for cyber offenses. Ebolbi notes that offenders often exploit these legal and procedural loopholes, making it difficult for law-enforcement agencies to pursue suspects operating from outside the country.

Fourth, *outdated legislation* limits the country's ability to address emerging forms of cybercrime. Current laws were not designed with cryptocurrency-driven fraud schemes, deepfake-enabled impersonation, or large-scale Internet-of-Things (IoT) attacks in mind. As Bwanga argues, this gap results in ambiguous legal interpretations and slows down prosecution of technologically sophisticated crimes.

Fifth, *limited capacity within law-enforcement agencies* further constrains the national response. The specialized Cyber Unit is understaffed, lacks modern forensic tools, and faces continuous skill-gaps due to the fast-changing nature of digital threats This undermines both investigative effectiveness and deterrence.

Finally, *private-sector under-involvement* remains a persistent challenge. Telecommunications companies, fintech firms, and financial institutions hold vast amounts of security-relevant data, yet they often operate in silos. Without structured information-sharing frameworks or collective-defense strategies, critical threat intelligence remains fragmented, weakening the overall resilience of the national cyber ecosystem.

Recommendations: A Multi-Stakeholder Approach

Given the scale and sophistication of today's cyber threats, Tanzania requires an integrated governance strategy that brings government,

private industry, civil society, and international actors into a cohesive defensive ecosystem. The following recommendations outline a coordinated pathway toward a safer and more resilient digital environment.

Strengthen and Update Legal Frameworks

Tanzania's legal instruments must evolve at the same pace as digital technologies. Updating the Cybercrimes Act to align with the Budapest Convention would provide clearer definitions of cyber offenses, strengthen investigative powers, and facilitate international cooperation. In addition, accelerating the rollout and enforcement of the Personal Data Protection Act would help safeguard citizens' information and build public trust in digital services. A modern legal framework sets the foundation for effective prevention, detection, and prosecution.

Enhance Institutional Capacity

A dedicated National Cybersecurity Agency would help streamline national responses, reduce duplication of efforts, and ensure consistent oversight across sectors. Beyond institutional restructuring, capacity-building is critical. Judges, prosecutors, and police officers need targeted training in digital forensics, cyber-law, and evidence preservation. Equipping frontline personnel with both the knowledge and the tools to investigate cyber incidents will significantly improve response effectiveness and reduce case backlogs.

Promote Public Awareness and Digital Literacy

Because many cyber incidents exploit human error, strengthening public awareness is just as important as strengthening technical systems. Tailored outreach programs, especially for women, young people, and rural populations, can demystify cybersecurity and empower citizens to protect themselves. Integrating cybersecurity fundamentals into school curricula will ensure that future generations develop safe digital habits from an early age, creating a long-term culture of cyber hygiene.

Foster Public-Private Collaboration

The private sector holds critical intelligence on threat patterns, yet this information often remains siloed. Establishing a Cybersecurity Information Sharing Platform for telecommunications providers, financial institutions, and internet service providers would enable timely exchange of threat indicators and best practices. In parallel, the government can spur private-sector investment in cybersecurity, through tax incentives, innovation grants, or procurement preferences, to expand security solutions and stimulate the local cybersecurity industry.

Boost International and Regional Cooperation

Cybercrime rarely respects borders, making international collaboration indispensable. Ratifying the African Union's Malabo Convention would signal Tanzania's commitment to regional cybersecurity governance and facilitate continent-wide information sharing. Participation in regional cyber-drills and INTERPOL-led initiatives would also help Tanzanian agencies test their readiness, learn from global best practices, and strengthen cross-border operational networks.

Leverage Technology

Emerging technologies offer powerful tools for prevention and detection. Piloting AI-driven fraud detection systems within mobile money platforms would enable early identification of suspicious transactions and reduce losses. Similarly, encouraging the adoption of blockchain technologies, particularly in financial services, supply chains, and land registries, can enhance transparency and reduce data tampering. Technology, when deployed responsibly and ethically, can amplify national resilience [13].

Conclusion

Cybercrime poses a significant and growing threat to Tanzania's digital growth and socio-economic stability. While the country has made strides in enacting cybercrime laws, critical gaps in enforcement, public awareness, and multi-stakeholder coordination persist. By adopting a governance-focused, inclusive, and proactive approach, grounded in updated laws, institutional strengthening, and international collaboration, Tanzania can mitigate cyber risks and secure its digital future.

References

1. Kshetri N (2019) Cybercrime and cybersecurity in the global South. Palgrave Macmillan https://www.researchgate.net/publication/317847658_Cybercrime_and_Cybersecurity_in_the_Global_South.
2. (2023) Tanzania Communications Regulatory Authority (TCRA). Annual Cybersecurity Report https://www.nao.go.tz/uploads/Annual_General_Report_for_Audit_of_Information_Systems_FY_2023-24.pdf.
3. (2023) Bank of Tanzania (BoT). Annual Report on Payment Systems https://www.bot.go.tz/Publications/Regular/Annual%20Report/en/2024082116493467.pdf.
4. Jahan Khani H, Al Nemrat A, Hosseinian Far A (2014) Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook Elsevier 149-164.
5. Mushi G (2021) Digital transformation and cyber risks in Tanzania. Dar es Salaam: University of Dar es Salaam Press https://www.researchgate.net/publication/392534932_Digital_transformation_and_cybersecurity_risks.
6. Moses N, Sem Lambo AA, Sabaya DP (2023) The impacts of cybercrime on the growth of mobile money services in Tanzania: A case of Kongwa District. International Journal of Business Management 6: 42-63.
7. Ogwueleka F, Aniche C (2021) Cyberterrorism in Sub-Saharan Africa: Trends and Countermeasures. African Security Review 30: 245-262.
8. (2022) Gender and Cyber Survey Tanzania. Women and Online Safety. Dar es Salaam: FEMNET 26.
9. Bwanga O (2023) Emerging Cyber Threats in East Africa: Cryptocurrency and Beyond. Journal of African Cybersecurity 5: 112-130.
10. Uwezo Tanzania (2023) Digital Literacy and Vulnerability to Cybercrime. Dar es Salaam 35-38.
11. Magalla A (2017) Human rights protection in Tanzania as described by the Cyber Crime. Independent Researcher https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4134618.
12. (2020) KICA Computer Misuse and Cybercrimes Act: Kenya's Experience. Nairobi: KICTA Net https://www.kictanet.or.ke/document/five-years-on-a-review-of-the-impact-of-kenyas-computer-misuse-and-cybercrimes-act-2018/.
13. (2023) World Economic Forum. Global Cybersecurity Outlook https://www.weforum.org/publications/global-cybersecurity-outlook-2023/.