International Journal of Computer Applications Technology and Research
Volume 15–Issue 07, 01 – 06, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1507.1001

An Analysis of Kenya's Cybersecurity Landscape: Threats, Challenges, And Strategic Responses

[1]Loyd Kinoti
Department of Information Technology
Maseno University
Kisumu, Kenya

[2]Dr Samuel Oonge
Department of Information Technology
Maseno University
Kisumu, Kenya

[3]Dr Erick Oteyo Obare
Department of Information Technology
Maseno University
Kisumu, Kenya

Abstract: The digital economy poses various new threats to developing economies, particularly those that are beginning to digitize the integration of digitization into their economies. It is possible that the rapid digitization of developing regions may jeopardize consumer privacy. One of Africa's leading digital economies is Kenya, which is also the first to offer a new digital economy solution that combines FinTech, e-Government, and e-Commerce. With the increased interconnectivity of these systems, Cybersecurity threats and challenges have also increased. For this reason, the primary focus of this research initiative is to establish a Cybersecurity framework for Kenya through a number of subsequent steps. Existing Cybersecurity publications will be analyzed in-depth and systematically to justify the claims and address the issues of insufficient relevant research/policy publications. The coverage of this area will encompass the Cybersecurity-related legislation created by Kenya, namely the Computer Misuse and Cybercrime Act of 2018 and Kenya's Data Protection Act of 2019. Despite the fact that there has been some legislation in Kenya, the gaps in enforcement, financing, public awareness, and the training of personnel have been the most detrimental to Kenya's Cybersecurity development. Kenya's Cybersecurity will involve an analysis of changes that emerging technologies will bring to Cybersecurity and the subsequent changes that will occur in Kenya's Cybersecurity, and will also provide specific recommendations pertaining to the development of a better Cybersecurity in Kenya, including a call for a more robust involvement from the Kenyan Government.

Keywords: cybersecurity, Kenya, cyber threats, regulatory frameworks, digital economy, emerging technologies

1. INTRODUCTION

1.1 Background and Importance of Cybersecurity

Information technology now includes cybersecurity, which protects systems, networks, and data from threats and unauthorized use. The growing use of digital systems by businesses and governments has resulted in an increase in cybercrime. Today, cybersecurity is no longer simply an information technology issue; It is also a key component of the protection of the nation, economy, and individuals (Goswami et al., 2023).

Developed nations worldwide have made significant advances in the construction of cyber security infrastructure, development of legislative measures to lessen cyber threat concerned, and development of cyber security tools that incorporate artificial intelligence (AI). In developing nations, and particularly in the resource limited, skill scarce, and threat differential environments of sub-Saharan Africa, the situation is far less than adequate (Waizel, 2024). In Africa, Kenya has been recognized as an important digital economy, with rapid development in financial technology (FinTech), e-governance, and digital commerce. Although these improvements have bettered the country, they have also made it more susceptible to cyber-attacks, and therefore a robust cyber security system is imperative to mitigate the cyber risk (Mwangi, 2023).

1.2 Research Objectives

This paper aims to:

i. Examine global and regional trends in cyber security with specific reference to Kenya.
ii. Compare Kenya's cybersecurity policies, strategies, and regulatory frameworks with the global best practices.
iii. Identify the challenges in the cybersecurity landscape in Kenya.
iv. Assess the applicability of emerging trends in cybersecurity in the context of Kenya.
v. Formulate proposals intended for the enhancement of the resilience of cybersecurity in Kenya.

1.3 Scope and Limitations

This study offers an elaborate examination of Kenya's policy formulation and implementation on a resultant emerging threat and stakeholder perspective on cyber risks. Further, this study elaborates on the cyber initiatives, challenges and feasible solutions in a comparative perspective to the developed world, though the emphasis would be on the Kenya cyber initiatives, challenges and feasible solutions.

This study possesses certain limitations, including:

i. The challenge of obtaining real-time empirical data on cybersecurity threats due to issues of confidentiality concerns justifies the reliance on current literature.
ii. Considering the broad range of the study, analyses of industry-specific issues concerning cybersecurity in the healthcare and manufacturing sectors were performed relatively infrequently.
iii. Because cyber security threats are continuously evolving, this paper may not identify all potential new threats.

1.4 Significance of the Study

The examination contributes meaningfully to understanding cybersecurity in Kenya by elucidating the preparedness levels, policy deficiencies, and areas needing immediate intervention. It also enables policymakers, IT professionals, and scholars to formulate more comprehensive cybersecurity policies. To foster digital trust, protect the national digital infrastructure, and sustainably grow the digital economy, a fortified cybersecurity framework in Kenya is indispensable.

2. LITERATURE REVIEW

2.1 Introduction

The fast-paced implementation of digital practices across sectors has made cybersecurity a pressing challenge on a worldwide scale.

The growing use of internet-based services, cloud computing, and artificial intelligence (AI) has made the protection of data and systems a prime consideration for governments, businesses, and individuals, and poses new and emerging threats to security (Goswami et al., 2023). While developed nations have their cybersecurity strategies in place, developing countries like Kenya are challenged by the limited availability of security personnel, inadequate legal cybersecurity frameworks, and an increasing prevalence of cybercrime (Kariuki, 2023).

The chapter analyzes the available literature on the threats to cybersecurity, their defenses, and the emerging patterns in this area. It provides specifics on the evolving nature of issues involving cybersecurity risks both in Kenya and in other countries. Additionally, technological developments, policy actions, and research needs are noted in the review for potential ways to bolster cybersecurity resilience.

2.2 Categories of cyber security threats.

Cyber attacks are getting more sophisticated, attacking individuals, businesses, and governments. The cybercriminals prey on technological weaknesses and human mistakes for financial fraud, data breaches, and ransomware attacks (Okoth et al., 2023). Common cybersecurity risks include malware, Phishing, ransomware, insider risks, and IoT vulnerabilities.

2.2.1 Malware and Ransomware

Malware, otherwise known as malicious software, is a cyber threat that is prevalent and seeks to compromise and disrupt computer systems. It contains viruses, worms, Trojans, spyware and ransomware. Ransomware has been found to be especially harmful because it encrypts the files of the victim, requiring a ransom to be paid for the recovery of it (Ndichu & Gitonga, 2024). A WannaCry ransomware attack has been estimated to cause damages of more than $4 billion as it affected more than 200,000 systems in 150 countries in 2017 (Goswami et al., 2023). Ransomware attacks on banks, government agencies, and small-to-medium enterprises (SMEs) in Kenya have increased by 40% in the past three years (Kariuki, 2023). In the past, for example, a ransomware attack on a hospital in Kenya, which was based in Nairobi and its operations were encrypted, forced the hospital to pay a ransom of KSh 5 million ($50,000) to regain access.

2.2.2 Social Engineering and Phishing

Phishing is still a common source of financial fraud, in which attackers mask themselves as trusted organizations to trick people into giving out their personal data, bank details or confidential information. Deceptive emails, SMS messages, and fake websites are used by attackers to trick victims into providing their logins or making financial transactions (Ndichu & Gitonga, 2024).

One of the notable phishing scams around the world is the $100 million phishing scam that occurred through Facebook & Google, where a cybercriminal pretended to be a legitimate supplier (Kariuki, 2023). M-PESA fraud is a significant issue in Kenya, where scammers often impersonate customer service representatives to trick users into revealing their phone numbers and sending money to fraudulent accounts.Fraud involving M-PESA is a widespread problem in Kenya, where scammers impersonate customer service representatives and ask users to provide their phone numbers and send money to fake accounts.

2.2.3 Insider Threats

Insider threats differ from external threats because they come from an insider, such as an employee, a contractor or a partner who has been given access and is using that to steal information or to compromise security. Sabotage and/or fraud are intentional threats, while human error and negligence are accidental threats (Waizel, 2024). In Kenya, banking, healthcare, and public sector institutions experience the highest number of insider threats, making up 30% of the cybersecurity incidents (Ndichu & Gitonga, 2024). In 2022, a bank employee stole KSh 60 million ($500,000) from the bank in Kenya, setting up fake loan accounts and making false transactions.

2.2.4 IoT Vulnerabilities and DDoS Attacks

As more and more people are adopting the Internet of Things (IoT) devices in their homes, businesses and industrial complex, new cybersecurity threats have been introduced. Insufficient security settings in many IoT devices can make them susceptible to cyberattacks (Goswami et al., 2023). DDoS attacks flood servers with too much traffic, resulting in a disruption of service (Barrier, 2024). In Kenya, government sites and corporate portals have been attacked with DDoS attacks that are part of politically motivated hacking groups (Okoth et al., 2023). One of the most significant cases of IoT cybercrime occurred in 2016, when hackers breached thousands of Internet of Things (IoT) devices, forming a massive botnet that attacked a number of online services, including Twitter, Netflix, and CNN (Kariuki, 2023). In Kenya, insecure IoT devices have been deployed in cyber espionage and massive DDoS attacks against government sites and private companies.

2.3 Defensive Mechanisms in Cybersecurity

Cyber threats are continually changing, and organizations and governments use many tools to stop, detect, and respond to cybersecurity incidents. Firewall, encryption, multi-factor authentication, endpoint security, and security awareness training are all strategies employed.

2.3.1 Firewalls and Intrusion Detection Systems (IDS)

The initial barrier in cybersecurity is the firewall, a device that filters and monitors traffic going in and out. Next-Generation Firewalls (NGFWs) are more advanced firewalls that combine deep packet inspection (DPI), intrusion prevention systems (IPS), and AI-powered threat intelligence for enhanced security capabilities (Kariuki, 2023). In addition to firewalls, Intrusion Detection Systems (IDS) are used to monitor network traffic and detect suspicious activity. Today, IDS solutions powered by AI are used in various Kenyan telecoms and banks to ward off cyber intrusions (Ndichu & Gitonga, 2024).

2.3.2 Multi-Factor Authentication (MFA) and Access Control

Multi-Factor Authentication (MFA) adds an extra layer of security by asking the user to prove their identity by a combination of authentication methods like password, OTP and biometric. Equity Bank and KCB, among other banks in Kenya, have implemented MFA in their mobile and online banking services to reduce fraud (Okoth et al., 2023). To ensure that users have access to only the systems and data required for their roles, Role Based Access Control (RBAC) and Zero Trust Security (ZTS) are also being deployed to restrict access.

2.3.3 Cybersecurity Awareness and Training

Human mistakes continue to be a top reason for cyber security breaches. It is revealed that 85% of security incidents are caused by user practices like giving out passwords that are weak, falling for

phishing scams, and mishandling data (Ndichu & Gitonga, 2024). To overcome this, bodies in Kenya are investing in cyber security training aimed at educating employees on safe digital practices. Cyber hygiene campaigns by KE-CIRT/CC and private sector organisations are aimed at improving public awareness and minimising cybercrime.

3. METHODOLOGY

This study uses qualitative exploratory research and a systematic review of secondary literature. Materials were obtained through targeted searches and screened for relevance within the context of cybersecurity in Kenya, which were then analyzed thematically in order to develop a framework for global and local trends, regulatory frameworks, sector-specific challenges, and emerging technologies. Because of the constraints associated with accessing real-time, confidential data on cybersecurity, reported incidents were evaluated for illustrative purposes as case studies rather than as primary research.

4. THE STATE OF CYBERSECURITY IN KENYA

4.1 Introduction

In the last 20 years, Kenya has seen major shifts in the digital landscape, and is now a leader in the digital economy in Africa. The widespread adoption of mobile banking, e-commerce, cloud computing and e-government services has spurred economic growth and service delivery. Mobile penetration in Kenya is at 91% while more than 33 million Kenyans are internet users, making digital platforms a focal point in business and daily life (Communications Authority of Kenya, 2023). M-PESA, a widely-used mobile money platform, has largely been responsible for the success of the digital financial revolution in Kenya. This digital expansion has brought along with it a lot of cyber threats, however. The financial systems, government databases, and private sector networks are vulnerable and these vulnerabilities have been used to carry out fraud, identity theft and ransomware attacks by cybercriminals (Kinyua 2024). As cybercrime incidents continue to increase, the Kenyan government has introduced cybersecurity policies and frameworks to safeguard its digital infrastructure (Sitienei & Kandiri, 2024). However, despite these efforts, barriers to cybersecurity resilience remain, including a lack of cybersecurity skills, public awareness, and finances. This chapter discusses in detail the various cybersecurity initiatives of Kenya, challenges, and real-life case studies that depict the maturing threat scenario in Kenya.

4.2 Kenya's Cybersecurity Initiatives and Regulatory Frameworks

The Kenyan government has taken a series of laws and regulatory actions to improve cybersecurity governance due to the escalating cyber threat. The efforts are designed to safeguard personal data, financial transactions and critical infrastructure, as well as providing legal avenues for prosecution of cybercriminals. The Computer Misuse and Cybercrimes Act (2018) is one of the most important laws that criminalize computer-related crimes including hacking, online fraud, identity theft and cyber harassment. Under this law, the National Computer and Cybercrimes Coordination Committee (NC4) was also established to supervise implementation and response measures in cybersecurity (Kariuki, 2023). This is also supplemented with the provisions of the Data Protection Act (2019), which state that the organizations must collect and process personal data in a responsible manner. The Act makes it possible for Kenya to bring her data protection policies into closer alignment with the other countries in the world by providing an example of what the EU's General Data Protection Regulation (GDPR) is (Ndichu & Gitonga, 2024). Also, the National Cybersecurity Strategy (2022 - 2027) provides for a period of five years in which the cyberspace of Kenya will become more resilient. Its focus is on the protection of critical infrastructure, cyber resilience, and the development of a workforce. The Kenya National Computer Incident Response Team (KE-CIRT/CC) which is under the Communications Authority of Kenya (CAK) is important in addressing the cyber threats that target the Government and the Private sector. These Laws provide a strong foundation legally, but there will always be challenges in enforcing and implementing these Laws, and the cyber criminals will always remain a step ahead in exploiting the systems of Financial and Government institutions.

4.3 Challenges Facing Kenya's Cybersecurity Landscape

Kenya is working towards improving its cyber security, however, the country still faces considerable obstacles that hinder the cyber resilience of the nation. Such obstacles include the lack of cyber security professionals, awareness of the public, inadequate funding, and increasing cyber crimes in the digital finance sector.

4.3.1 Limited Cybersecurity Workforce and Skill Gaps

Lack of skilled personnel to manage and secure digital infrastructure is one of the biggest challenges in cybersecurity in Kenya. There are less than 5,000 certified cybersecurity experts in Kenya, whilst according to the industry estimates, there is a need for more than 20,000 cybersecurity experts to address the national demand (Kenya Cybersecurity Report, 2023). This shortage is also seen in education, including both the public and private sectors, and is due to the lack of trained staff to address cyber threats properly. There is limited cybersecurity courses in universities and training institutions in Kenya and most IT graduates are not equipped with hands-on cyber security skills. In addition, cybersecurity credentials like Certified Ethical Hacker (CEH) and CISSP are still costly, and it is hard for aspiring professionals to gain the necessary credentials. To fill this gap, there is need to establish programs like government facilitated cybersecurity boot camps, scholarships, and collaborations with private organizations to speed up skill acquisition in the cybersecurity field (Sitienei & Kandiri, 2024).

4.3.2 Insufficient Public Awareness on Cyber Threats

Kenya is still vulnerable to cyber risks, as the public and businesses do not yet have a high degree of cybersecurity knowledge. Many people and small enterprises don't bother with cybersecurity because they think that hackers only target large corporations or government agencies. Cybercriminals, however, often target unsuspecting people through phishing scams, SIM swap fraud or fake mobile loan applications (Ndichu & Gitonga, 2024). A 2023 Central Bank of Kenya (CBK) report indicates that phishing is still the top financial fraud technique, and of those who fall for it, 90% do not report the offenders because they do not know how to or are afraid of feeling embarrassed. Also, numerous businesses don't provide cybersecurity training, which means employees are at risk of a cyberattack. The government institutions like KE-CIRT/CC conduct cyber security awareness campaigns, but the scale of the problem is far greater than their efforts.

4.3.3 Inadequate Funding and Resource Constraints

Investing in Cybersecurity infrastructure, staff and technology is a significant financial commitment, but Kenya is spending less than 0.5% of its national budget on Cybersecurity, while the U.K. is spending more than 2% (Global Cyber Budget Report, 2023). It is a financial constraint that impacts public institutions, banks and SMEs, exposing them to cyber threats. The absence of advanced systems such as AI threat detection, endpoint protection, and multi-factor authentication in most Kenyan businesses is concerning. Businesses are easily targeted for cyberattacks due to having weak security measures (Serianu Ltd, 2018).

4.3.4 Increasing Cybercrime Targeting Digital Finance

Due to a number of reasons, the digital finance industry is one of the most susceptible industries within Kenya, including mobile banking, M-PESA payments, and other fintech solutions, cybercriminals have started exploiting gaps within the systems to cheat users and manipulate transaction records. The types of cyber fraud that occur most frequently include SIM swap fraud, ATM fraud, and phishing fraud in online banking (Communications Authority of Kenya, 2024). A notable example is a 2022 case of cybercrime in Kenya, where a mobile banking fraud syndicate leveraged mobile banking systems' authentication security loopholes to defraud 400 million Ksh ($3.5 million) by gaining unauthorized access to thousands of accounts (DCI, 2023). The numerous incidents emphasize the urgent enhancement of cyber security measures, fraud detection systems, as well as the need to strengthen the regulatory frameworks designed to protect and secure the financial systems in Kenya.

4.4 Case Studies of Major Cybersecurity Incidents in Kenya

The rise in cyber threats to both the government and the private sector is well demonstrated through a number of high profile cyber attacks in Kenya. One of the most significant cyberattacks occurred in July 2023, when Kenya's E-Citizen portal was hit by a large-scale Distributed Denial-of-Service (DDoS) attack, disrupting essential government services such as passport applications, driving license renewals, and tax filing systems. The attack is said to have taken place through a foreign hacking group, which in turn brought the vulnerabilities of Kenya's critical infrastructure (KE-CIRT/CC, 2023) to light. The other significant event was the 2021 ransomware attack on Kenya Power and Lighting Company (KPLC) which impacted customer billing systems and forced payments in Bitcoin ransom. However, KPLC stated that it didn't pay, arguing instead that it could recover the data from back up systems, but the loss had caused financial losses (Kariuki, 2023). In 2020, a criminal syndicate was arrested for carrying out SIM swap fraud on Kenyan politicians and corporate executives. The gang also accessed some high-ranking bank accounts where it transferred millions of shillings before its arrest (Ndichu & Gitonga, 2024).

5. FUTURE OF CYBERSECURITY

5.1 Introduction

The rapid advancement of technology has transformed the field of cybersecurity and its associated risks, which has rendered protective measures obsolete and has highlighted the need for new techniques, skills, and the need for international collaboration at all levels. Organizations are attempting to understand how AI, ML, blockchain, and quantum computing are fundamentally altering how we detect, prevent, and respond to cyber threats. Furthermore, these defenses can be strengthened with appropriate skills and international collaboration, particularly in developing nations, such as Kenya, where the development of cyber resilience is still at an early stage (Goswami et al., 2023). The purpose of this chapter is to analyze and discuss the prospects of developing cyber defenses and the role technologies, enhanced training and development, and international collaboration will play in defining the future prospects of constructing cyber defenses. Collectively, these elements will be paramount in addressing the challenges present in the field of cybersecurity and will solidify the global community's ability to withstand rising cyber threats.

5.2 Emerging Technologies in Cybersecurity

Cybersecurity practices are being transformed due to emerging technologies. Due to the growing intricacy of cyber threats, conventional protective measures are increasingly insufficient. The field of cybersecurity is being revolutionized by the rapid incorporation of cutting-edge technologies such as artificial intelligence driven threat detection, security based on blockchain technology, and encryption that is resistant to quantum computing.

5.2.1 Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML have changed how cybersecurity analysts perform data analysis, anomaly detection, and threat forecasting. Analysts can now process large amounts of data, identify irregularities and predict possible threats, and AI and ML have become must-have components in today's cybersecurity. Traditional solutions in cybersecurity were mostly signature based and therefore depended on prior knowledge of threats. However, AI-based systems can adapt to, and identify new, real-time cyber threats using behavioral assessments and predictive models (Ndichu & Gitonga, 2024). An area where AI has brought tremendous improvement in cybersecurity is in threat intelligence platforms. AI-based security applications can act in advance to identify unusual behavior or patterns in the traffic of a network, behavior of users and even malware (before they arrive). Companies like Darktrace and CrowdStrike have shown that it is possible for AI to autonomously discover and address cyber threats. For example, Darktrace uses self-learning AI models which allow it to adapt to the evolution of threats and respond independently to security issues (Kariuki, 2023). All these developments notwithstanding, cybersecurity still has some challenges associated with AI. Cybercriminals are using anti-adversarial AI to circumvent detection systems. Hacker used AI to create more sophisticated phishing schemes, automate the creation of malware, and circumvent authentication protocols. Consequently, AI is playing its role in the arms race between cybercriminals and cybersecurity experts (Waizel, 2024).

5.2.2 Blockchain Security

Blockchain technology is a viable option for advancing data integrity, secure transactions, and identity management. In contrast to traditional centralized security methods, which are susceptible to cyberattacks such as information tampering and unauthorized access, blockchain's decentralized network provides greater protection. The protective attributes offered by this innovation can be leveraged in multiple domains, including secure financial transactions, supply chain management, and digital identity validation (Okoth et al., 2023). The fact that information can neither be altered nor deleted once it is added to the blockchain is one of

the main advantages of this technology. Given the functionalities described above, the blockchain technology is equipped to satisfy the requirements of audit trails, compliance tracking, and fraud prevention. Digital identity management is being explored using blockchain technology in Kenya via the national digital identity system called Huduma Namba. Citizen verification and identity fraud are significant cybersecurity issues in digital services, with the government seeking to address these challenges through blockchain technology (Ndichu & Gitonga, 2024). While blockchain technology holds promise, it also brings with it a host of security concerns, including scalability, regulatory uncertainty, and energy consumption. Further, blockchain networks are not invulnerable to cyber attacks. The 51% attack is a serious threat especially in smaller and less decentralized blockchain systems (Saad et al., 2019; Serena et al., 2021).

5.2.3 Quantum-Resistant Cryptography

The current encryption technology, including RSA, ECC (Elliptic Curve Cryptography) is facing threats due to the advancement of quantum computing. Quantum computers also have the potential to attack current cryptographic methods, which makes the development of quantum-resistant encryption methods (Waizel, 2024) of paramount importance. A search is underway for post-quantum cryptography, new encryption algorithms that are resistant to quantum attacks. IBM and Google are among the companies working on quantum-safe encryption. Meanwhile, the National Institute of Standards and Technology (NIST) is developing post-quantum cryptographic algorithms that will make it more secure for encryption in the quantum era (NIST, 2024). Implementing quantum-resistant cryptography will be crucial for Kenya, particularly when protecting its digital communication networks, financial systems, and national security. Such technologies are expected to become more widespread in the future, and their early implementation will avoid future weaknesses.

5.3 Workforce Development in Cybersecurity

The creation of a strong Cybersecurity workforce is essential to protect from the new cyber threats. But the demand for cybersecurity professionals has outstripped supply and is increasing worldwide. The Cybersecurity Workforce Study (2023) predicts there will be more than 3.5 million cybersecurity jobs available globally by 2025 that will go unfilled. The deficit of skills pertaining to cybersecurity is a pivotal issue in Kenya. The Kenya Cybersecurity Report (2023) states that there is a qualified personnel count of under 5000, far short of the demand that is over 20,000, which is a considerable shortfall affecting banks, government institutions, and private enterprises. They have difficulties finding personnel that can secure the digital infrastructure. This issue can be addressed by integrating specific training aimed at cybersecurity into the curricula of universities and other training institutions in Kenya. The credential programs like Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), and CompTIA Security+ should be implemented in a wide spread across the world to improve the skillsets of cyber security professionals. Furthermore, the industry-led training programs and government-sponsored cybersecurity boot camps can assist in addressing the skills gap (Ndichu & Gitonga, 2024). Gender inclusion is another important component of the workforce development. There is a lack of gender diversity, particularly among women, in cybersecurity, as women make up only 24% of the total cybersecurity workforce. There are organisations like Women in Cybersecurity Kenya (WiCyS-K) that are trying to increase the rate of women in cybersecurity positions.

5.4 International Collaboration in Cybersecurity

Cyber threats are not confined to any borders; can only be fought with cooperation, intelligence sharing and coordinated cyber defence between borders. Kenya is an active member of regional and international cyber security initiatives to effectively fight cybercrime. One such organization is AfricaCERT, a continental cybersecurity organization enabling threat intelligence sharing across Africa. Kenya further collaborates with Interpol's African Cybercrime Initiative to help police agencies fight against cybercrime. There are challenges to international collaboration, particularly concerning legal jurisdiction, disparate national cyber laws, and geopolitical tensions concerning crime in cyberspace. To bolster its position in international cybersecurity, Kenya ought to adopt the international cyber security systems, such as the NIST Cybersecurity Framework and ISO 27001, while ensuring that its policies align with international best practices (Okoth et al., 2023).

6. CONCLUSION, SUMMARY OF FINDINGS, AND RECOMMENDATIONS

6.1 Summary of Findings

This research analyses Cybersecurity in Kenya. It covers the different Cybersecurity threats, defensive mechanisms, international legal frameworks, and emergent trends. One finding states that Kenya has undergone rapid digital transformation, and this has increased potential cyber risks, especially in the mobile banking, e-government, and telecommunications sectors. Technological vulnerabilities, Weak security, and human error are the tools of cybercriminals to perpetrate cyber fraud, ransomware attacks, and ID theft. Regarding policy development in Cybersecurity, Kenya has made some progress and has laws that provide a framework to deal with cyber threats, such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019). Nonetheless, there are challenges in enforcement, lack of awareness and training for personnel. There is also a shortage of cybersecurity professionals, with less than 5,000 trained personnel compared to an estimated demand of over 20,000 (Kenya Cybersecurity Report, 2023). This skills gap has exposed financial institutions, businesses, and government agencies to potential cybercrime attacks. Most organisations lack the necessary tools to implement sophisticated cyber security solutions because many of the tools are expensive and include advanced measures such as multi-factor authentication, firewalls, encryption, and artificial intelligence (AI) based threat detection. Emerging technologies such as blockchain security, Zero Trust architectures, and quantum-resistant encryption offer new opportunities for strengthening Kenya’s Cybersecurity. However, for the country to develop Cybersecurity sustainably for resilient systems, investments must be made in Cybersecurity training, public awareness, and international collaboration.

6.2 Conclusion

Kenya is at a critical juncture with regard to cyber security. The nation has rapidly adopted digital technologies, made notable progress in areas including mobile money, digital government services, and cloud computing. However, this rapid digital adoption has created new vulnerabilities for consumers and businesses. The emerging digital landscape has made consumers and businesses susceptible to fraud, data breaches, financial fraud, and cyber espionage. The study reveals that cyber security is both a national

security concern and a technology concern. Also, it requires a multi-stakeholder approach involving government, private sector, academic, and civil society actors. The study also shows that while Kenya has established legal and institutional frameworks for cyber security, there are still gaps in enforcement, investment, and knowledge. Many organisations do not have adequate cyber security policies and the general public has little awareness of cyber hygiene practices, making them an easy target for cyber criminals. There is also a shortage of cybersecurity experts to make Kenya more resilient to the increasing volume and sophistication of cyber threats. The study also highlights the fact that the nature of the cyber threats is constantly evolving and the attackers are using artificial intelligence, automation and social engineering techniques to evade traditional security measures. In light of these challenges, Kenya's strategy needs to be forward-looking and embed the concept of cybersecurity in the country's national economic and technological policies. To safeguard the Kenyan economy, investments in cybersecurity infrastructure, workforces, and collaborations between countries will all be vital.

6.3 Recommendations

The following recommendations are made to improve the cybersecurity resilience of Kenya:

- **i.** Improve Cybersecurity Laws and Enforcement - Kenya should improve funding for cybersecurity agencies, update the cybercrime laws to cover emerging cyber crimes threats, and harmonise its policies with other global standard policies such as the Budapest Convention and ISO 27001.
- **ii.** Improvement of Cybersecurity Workforce Development - Universities provide degrees and certifications in cybersecurity; government funds scholarships and collaborates with international businesses to educate and certify cybersecurity personnel. Reduction of cyber risks through
- **iii.** Enhance Public Awareness and Cyber Hygiene encompasses the nationwide awareness campaigns, incorporation of cybersecurity education in schools, and improved customer education by the banks and financial institutions, which can assist in reducing cyber risks, including phishing and social engineering fraud.
- **iv.** Utilize Cybersecurity Infrastructure Innovations - Utilize, incorporate AI for threat identification, aid implementation of blockchain security and promote organizational Zero Trust adoption; encourage basic cybersecurity measures within SMEs.
- **v.** Enhance International Collaboration on Cybersecurity- Kenya should partner with other international cyber security bodies to bolster cyber security cooperation, develop bilateral cyber security training and funding agreements, and participate in international cyber security drills.

7. REFERENCES

[1] Central Bank of Kenya (CBK). (2023). Annual Mobile Banking Report 2023: Trends, Risks, and Regulatory Strategies. Nairobi: CBK.
[2] Communications Authority of Kenya (CAK). (2023). Kenya Cyber Threat Report 2023. Nairobi: CAK.
[3] Communications Authority of Kenya. (2024). Cybersecurity Report Q4 2023-2024.
[4] Cybersecurity Strategy for the Nation (2022-2027). (2022). Kenya's National Cybersecurity Vision and Roadmap. Published by the Ministry of ICT, Kenya.
[5] Cybersecurity Workforce Study. (2023). Global Cybersecurity Workforce Gap and Future Employment Trends. Cybersecurity & Infrastructure Security Agency (CISA).
[6] Directorate of Criminal Investigations (DCI). (2023). Cybercrime Investigations Report 2022: Trends in Digital Financial Fraud. Nairobi: DCI.
[7] Goswami, A., Safitra, A., & Oruj, B. (2023). Cybersecurity in the Digital Age: Emerging Threats and Strategies. Journal of Information Security, 18(3), 112–129.
[8] Kariuki, P. (2023). Cybersecurity Trends in Kenya: An Analysis of Threats and Countermeasures. East African Journal of Information Security, 9(2), 76-98.
[9] KE-CIRT/CC (Kenya National Computer Incident Response Team Coordination Center). (2023). Cybersecurity Incident Analysis and National Response Framework. Nairobi: Communications Authority of Kenya.
[10] Kenya Cybersecurity Report. (2023). Bridging the Cybersecurity Skills Gap in Kenya. Published by the Kenya ICT Authority.
[11] Kenya Power and Lighting Company (KPLC). (2021). Incident Response Report: Ransomware Attack on Kenya Power Billing Systems. Internal Report.
[12] Mwangi, P. (2023). Cybercrime in Kenya: The Growing Digital Threat. African Journal of Technology and Policy, 10(1), 88-104.
[13] National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography: Developing Future-Proof Encryption Standards. Washington, D.C.: U.S. Department of Commerce.
[14] Ndichu, E., & Gitonga, R. (2024). The Impact of Emerging Technologies on Cybersecurity: A Kenyan Perspective. Journal of Digital Security, 12(4), 99-117.
[15] Okoth, J., Mugambi, N., & Ndwiga, P. (2023). Kenya's National Cybersecurity Strategy: Progress and Challenges. East African Cybersecurity Review, 7(2), 132-148.
[16] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the Attack Surface of Blockchain: A Systematic Overview. arXiv preprint arXiv:1904.03487.
[17] Saidi, I. C., Kimuyu, J. J., & Handa, S. (2024). The Implications of Cybercrime on Economic Security: The Case of Kenya. International Journal of Research and Innovation in Social Science, 8(10), 2464-2471.
[18] Serena, L., D'Angelo, G., & Ferretti, S. (2021). Security Analysis of Distributed Ledgers and Blockchains through Agent-based Simulation. arXiv preprint arXiv:2109.08358.
[19] Serianu Ltd. (2018). Africa Cybersecurity Report: Cybersecurity Readiness of SACCOs in Kenya.