The Implications of Cybercrime on Economic Security: The Case of Kenya

Issa Chochote Saidi, James J. Kimuyu, Steve Handa

National Defence University - Kenya

DOI: https://dx.doi.org/10.47772/IJRISS.2024.8090204

Received: 05 September 2024; Accepted: 10 September 2024; Published: 15 October 2024

ABSTRACT

The research study examined the evolving landscape of cybercrime and its significant implications on economic security within Kenya. As the digital economy rapidly grows, cyber threats have become increasingly sophisticated and pervasive, posing significant risks not only to individual entities but also to national security. In Kenya, a nation at the forefront of digital transformation in Africa, these threats have escalated, challenging the ability to safeguard vital economic infrastructures. The study used a mixed-methods approach, combining qualitative and quantitative techniques to analyze Kenya's cybercrime landscape. The theoretical framework was based on securitization, deterrence, and routine activity theories, offering a strong foundation for understanding cybercrime's impact on economic security. Data was collected through an extensive literature review and engagement with professionals from various sectors, including government, security agencies, and academia. Participants, with 1 to 30 years of experience, provided key insights into Kenya's cybersecurity state. An 80% response rate was achieved, ensuring the findings were valid, reliable, and representative of the broader cybersecurity landscape. The study reveals critical issues in Kenya's cybersecurity landscape. Despite digitalization efforts and security policies, there remains a significant gap in public cyber threat awareness, leaving many vulnerable to attacks. The 2017 cyber-attack on the National Bank of Kenya, resulting in the theft of KES 29 million ($280,000), highlights the need for stronger cybersecurity measures and public education. The study also identifies the asymmetric nature of cybercrime, which, unlike traditional crimes, transcends borders, making it harder to predict and mitigate. The global interconnectedness of the internet exacerbates this challenge, necessitating a shift from reactive to proactive cyber threat strategies. The study recommends immediate implementation of comprehensive cyber literacy programmes for the public, focusing on common threats, safe practices, and basic cybersecurity, with tailored content for different demographics. Cybersecurity education should be integrated into the national curriculum from the primary level to foster early awareness. It also highlights the need for collaboration among all stakeholders - government, private sector, academia, and civil society to share information and best practices. Organizations, especially in critical sectors like banking, healthcare, and government, should adopt robust security measures, including advanced detection systems and regular audits. The study also suggests further that the government should consider employing local ethical hackers to identify vulnerabilities and counter cyber threats, particularly in government and critical infrastructure.

Keywords: Cyber-security, Kenya, National Security, Information Technology, Internet.

INTRODUCTION

Cybercrime poses a significant threat to economic security for many countries across the world specifically through various avenues, including financial losses, disruption of critical infrastructure, and erosion of trust in digital systems. At present, the Africa continent is experiencing a surge in various aspects, including population, economic development, and global influence. Presently, the continent is home to 1.21 billion people, a significant increase from 800 million in 2000, with a median age of 19.5 years, making it the youngest population globally. This youthfulness brings diversity, as the population seeks productive employment, social engagement, freedom of expression, and enhanced global connectivity. Despite challenges such as the impact of declining global commodity prices on African economies, nearly every African nation is positioned for growth in the coming years.

These changing dynamics in Africa have led to a rise in the adoption of technology, marked by the exponential growth in mobile device ownership, increased use of social media, and the rapid emergence of the Internet of Things (IoT). Conservative estimates suggest that Africa is on the verge of significant progress, contributing to global growth. Alongside this economic expansion, the e-commerce sector has experienced rapid rise to the point that it is expected to reach an estimated $75 billion USD by 2025 (Mitchell, 2022). However, as prosperity and digitization has increased, new risks and vulnerabilities have also emerged that are potentially hindering progress. One major concern is the global surge in cybercrime. As Africa's economy transitions to the online realm, citizens, their computer systems, and the continent's information technology (IT) infrastructure become attractive targets for an increasingly sophisticated group of cybercriminals.

Latest research shows that over the past decade, Africa's international internet bandwidth experienced a tenfold increase to 12 terabits per second (Tbps). The International Finance Corporation (IFC), a division of the World Bank, anticipates a substantial 11% surge in internet users in Africa over the next decade, accounting for 16% of the global total. Additionally, the transition from 3G to 4G is underway, with 4G expected to surpass 28% of the continent's mobile phone connections by 2025, up from 12% in 2020, according to GSMA, the lobby organization for mobile communication companies. Research conducted by the IFC and Google suggests that Africa's digital economy is poised to contribute $180 billion to the overall economy by 2025, reaching $712 billion by 2050 (Sukumar and Amoozad, 2023).

Research further shows that at the end of 2020, mobile service subscriptions in sub-Saharan Africa had already reached 495 million, representing 46% of the region's population and marking a nearly 20 million increase from 2019, according to GSMA, a telecommunications association. Simultaneously, 303 million individuals in the region had access to mobile internet. The tally of registered mobile money wallets in Africa surpassed 621 million in 2021, reflecting a 17% rise from 2020. The value of mobile money transactions in Africa surged by 39% to reach $701.4 billion in 2021 (Mitchell, 2022).

The rapid digital transformation driven by globalization has brought unprecedented opportunities, but it has also unleashed severe threats, particularly in the form of cybercrime. The scale of this threat is alarming, with cybercrime costing Africa an estimated $4 billion annually and contributing to a staggering global total of $450 billion. In Kenya alone, the focus of this research, the economic losses due to cybercrime are around $36 million annually. This is a significant figure, especially when compared to other leading African economies such as South Africa, which loses approximately $570 million annually, and Nigeria, which faces losses of $500 million. These figures illustrate the vast economic damage inflicted by cybercrime across the continent, highlighting an urgent need for a comprehensive and robust response.

As internet traffic in Africa doubles every 18 months, the urgency for bolstering cybersecurity measures becomes even more critical (Sukumar & Amoozad, 2023). The rapid increase in digital connectivity, while driving economic growth, simultaneously opens new avenues for cybercriminals to exploit vulnerabilities. African governments and businesses are now confronting the necessity of substantial investments in digital security to counter these escalating threats. The growing sophistication and complexity of cyber-attacks further exacerbate this situation, making it clear that without immediate and strategic intervention, the economic consequences could become even more devastating.

Despite the rising complexity of cybercrime and its profound impact on economies worldwide, including Kenya, there has been a notable lack of scholarly focus on the specific effects of cybercrime on economic security. This study seeks to fill that gap by examining cybercrime as a significant threat to economic security in Africa, with a particular focus on Kenya. The primary objectives are to assess the impact of cybercrime on Kenya's economic security and to evaluate the effectiveness of the response mechanisms that have been initiated by the Kenyan government. The findings of this study aim to provide critical insights that can inform policymakers and stakeholders in their efforts to strengthen cybersecurity and protect economic interests in Kenya and beyond.

Theoretical Framework

In examining cybercrime within a dynamic digital landscape, theoretical research spans two primary dimensions: theoretical and logical construction from an analytical perspective and empirical and functional substantiation

from a practical approach. Theoretical research involves coming up with ideas and theories on natural or social occurrences while empirical research seeks to challenge or defend theoretical ideas with real findings to enhance it (Bhattacherjee, 2012). This becomes a useful hermeneutical cycle, in that it serves to refine such theoretical constructs against the grain of practical experience and then to translate them back into practice.

Deterrence Theory and Cybersecurity

The deterrence theory aids in the study of cybercrime as it clarifies how specific countermeasures enhance security by employing forceful methods. The theory largely focusses on conditional threats to control adversaries, something that unveals significant discrepancies in Africa's digitization, particularly in the fight against cybercrime that was elaborated by Possony in 1946. It is therefore necessary for organizations to employ adequate measures to protect their business data from cybercriminals, as cybercrime has implications for economic security (Kshetri, 2019). Some of the past incidents, including those that occurred in Estonia in 2007 and Georgia in 2008/2009, are evident of the disastrous effects of poor cybersecurity (Powell, 2008). In the context of this research, the theories of deterrence and securitization are most relevant and fundamental to understanding the lack of cyberspace protection, which threatens economic and security consequences on a large scale (Schelling, 1980; Angela & Martin, 2012). Therefore, using these theories for the analysis of cybercrime in Africa shows the importance of elaborating on the coherent strategies for the efficient prevention of this type of crime that take into consideration the conditions of the region. In this way, the deterrence theory aids policymakers in understanding how to implement prevention and security measures that align with the technological and socio-economic factors contributing to cybercrimes. However, the increase in cybercrimes and, more importantly, the involvement of multiple actors, from hackers to states, make it difficult to protect cyberspace (Broadhurst, 2017; Fitzgerald, 2017). This has highlighted the importance of consistently elaborating counter-active measures and cooperation at the international level.

Routine Activity Theory and Cybercrime Trends

Routine Activity Theory helps to understand why cybercrime occurs frequently by highlighting the availability of opportunities and the lack of proper safeguards as primary factors for cyber threats (Gagliardone, 2014). The advancement in ICT and growing adoption of IT assets in Africa have offered more room for cybercriminals to work, resulting in an increase in crimes like ATM fraud and malware (Kshetri, 2019). The revolutionary changes that the internet brings to communications and business, along with its potential and attractiveness to the illicit actors, create problems for its regulation and security (Fitzgerald, 2017; Bremner, 2017). The increased level of risk implies the importance of multifaceted counteractions, both at the technological and legal levels. This involves legal reforms and improvement of cybersecurity measures to safeguard economic and infrastructure assets (Chatterjee 2019; Mwiburi 2018). Even though the Kenyan government has attempted to improve cybersecurity policies and legal frameworks, cybercriminal activities are ever-evolving, sophisticated, and transnational, necessitating international coordinated approaches and timely adjustments to security measures (Government of Kenya, 2014; Okongo, 2021). Routine activity theory shows that cybercriminals use open gaps in protection and opportunities that are not protected by law, requiring local and international cybersecurity cooperation. This means that there is a need for increased awareness and contingency in order to confront new threats and protect digital and economic values.

METHODOLOGY

The research study adopted the use of mixed methods that blends the use of qualitative and quantitative data collection techniques. It is important to appreciate that the acts of cybercrime transcend global, regional, sub-region national and local boundaries. Whereas the quantitative aspect of the research adopted the use of descriptive statistics in form of means, mode, standard deviations and percentages in the analysis, the qualitative aspect of the research was concerned with subjective phenomena that cannot always be numerically measured. Hence the primary data was deliberately collected through interview guide. As noted by Kothari, qualitative data are 'most often' are best collected by researchers through interviews (Kothari, 2011). As a result, this study employed Key Informant Interview (KII) as a more powerful tool in eliciting narrative data that allows researchers to investigate respondents' views in greater depth.

The KII is a form of qualitative research where questions are asked about their perceptions attitudes, beliefs, opinion or ideas. In addition, secondary data was being collected from cyber experts related sources such as, books, reports, journals, articles and periodicals. This greatly helped capture precise information that would make it possible to generate new insights or simply verify and confirm from previous analyses on cybercrime.

The study's target population was made up of key experts in cyber technology, crimes, economic, defense and national security. More specifically, the respondents included personnel drawn from the Kenya Defence Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affair, National Intelligence Service. Throughout the research exercise, the researcher observed high standards of ethical practices. For instance, consent was sought from respondents during the interviews and also during the administration of the questionnaires. The respondents were informed of their right to choose not to take part in the research. Full confidentiality was maintained especially when dealing with questionnaires and the identity of the respondents were kept private and confidential.

LITERATURE REVIEW

Implications of Cybercrime on Kenya's Economic Security

According to Broadhurst (2017), cyberspace is a global environment that fosters unlawful conduct, and a strong cybersecurity approach is therefore crucial. As much as this line of thinking is helpful, this particular focus does not address the economic aspects of cybercrime in Kenya. To fill this gap, the current study adopts Broadhurst's framework to evaluate the effect of cybercrime on the Kenyan economy and organisations. In this study, cyber threats lead to a loss of economic security by compromising financial systems, harming business reputations, and destroying consumer trust. Therefore, this study narrows down Broadhurst (2012)'s generalised analysis by focussing on Kenya to fill the existing gap and appreciate how cyber threats implicate economic security. Expanding on these concepts, Broadhurst (2012) explores the networks, while Gagliardone (2014) distinguishes the political considerations for gathering intelligence in the cyberspace environment. While the study provides a rather exhaustive outlook of the global threats mapped out by Gagliardone (2014), it does not pay adequate attention to the economic insecurity consequences in Kenya. The current study builds on Gagliardone (2014)'s work by concentrating on how changes in technology have created new economic risks in Kenya. The study examines the impact of cybercrime on various sectors, such as e-commerce and sensitive infrastructure, as well as an evaluation of Kenya's current cybersecurity mechanisms.

Likewise, Kshetri (2019) discusses the issue of cyber terrorism and the various negative impacts that it may have, including identity theft and financial imbalance. Although Kshetri (2019)'s work provides insight into cyber terrorism, it does not provide a real-life perspective on the economic effects of cyber terrorism on the Kenyan economy. Using this framework, this paper also looks at the direct cost of cyberattacks, including punitive losses and business interruptions. This study aims to investigate how cybercrime affects Kenya's economy and why there is a need to develop specific cyber security measures.

Risk Levels of Cybercrime on Kenya's Economy

According to the United Nations Office of Drugs and Crime (2012), Web 2.0 and the social networking sites have grown to cover the world; this is despite acknowledging the fact that the use of cyberspace attracts cybercrime risks. Their analysis, however, does not highlight the various risks that will affect Kenya's economy. This study, therefore, extends the UNODC's findings by expounding on how the rise of digital platforms has created new economic risks in Kenya. Through the analysis of occurrences of cybercrime and its effects on financial systems, businesses, and consumers' behaviour, the studies can go further in defining the risk rates of cyber threats in Kenya. Similar to the idea mentioned above, Sayigh (2023) investigates regional cyber threats with an emphasis on the distribution of radical ideas. Although this viewpoint can be helpful for analysing the dynamics of various regions, it does not contain a specific section on economic security. The following study builds on Sayigh (2023)'s analysis by focusing on the economic aspect of regional cyber threats in Kenya. Therefore, the study concentrates on the impact of extremist activities and intricate cybercrimes on economic stability, thereby illustrating the risk levels associated with cybercrime and emphasizing the need for strategies tailored to specific regions.

Angela and Martin (2012) explore the interdependence of the global village through the lens of cybersecurity, highlighting the significant impact on most local economies. While their analysis adds a degree of context, the authors do not focus on economic security in Kenya. In light of this research gap, the current study uses Angela & Martin's (2012) concepts to assess the impact of cybercrime on the economic security of Kenya. This study strengthens understanding of the global trends' effect on local economies by highlighting the economic factors of cybercrime; it reaffirms the necessity of specific strategies.

Response Mechanisms to Cybercrimes in Kenya

Due to rising cybercrime cases, Kenya has developed various intervention measures. But these measures have been largely laughed off for their inability to arrest or even reduce the incidence of cyberattacks. This paper makes an assessment of Kenya's cybersecurity policies, particularly in the context of the country's economic security. ng response mechanisms also have their flaws, the research seeks to find out where they are lacking and come up with specific recommendations that could help Kenya be more secure against cyber risks. The unavailability of electronic services in Kenya has created a number of vices and losses in the financial sector, as Chuipka (2016) points out. However, there are few IT security specialists, which seems to be a huge drawback even with the best efforts to enhance cybersecurity. Based on Chuipka (2016)'s findings, this study seeks to investigate how preparedness response mechanisms in Kenya offset these vulnerabilities and assess the efficiency of current measures in safeguarding the economic interest. Thus, the research is constructed to discuss the identified weaknesses of the existing strategies and make relevant recommendations for enhancing Kenya's cybersecurity environment.

In the same way, Okongo (2021) explains the various cyber risks affecting organisations and households in Kenya, including, but not limited to, scams and advanced attacks. Of course, Okongo (2021)'s work fills the need for a general analysis of local context, but it is not targeted at economic security at all. The current paper builds on Okongo (2021)'s work and examines Kenya's resilience operating mechanisms in maintaining economic capital. In so doing, this research helps fill the existing knowledge gap about how Kenya can address its specific economic security threat to bolster its cybersecurity. Ouma (2021) looks at various kinds of cyber threats that threaten the confidentiality and integrity of information at a local level. While Ouma (2021)'s work can be useful in identifying local threats, it is not exactly helpful in terms of economic security. This research, therefore, extends Ouma (2021)'s analysis by establishing how various cyber threats affect Kenya's economy. Because it focusses on the effects of cybercrime on data-sensitive assets such as infrastructural and financial fields, the study provides specific interventions for strengthening Kenya's fighting methods and, in turn, economic protection.

FINDINGS

The research achieved an 80% response rate, with 35 individuals out of the targeted 50 respondents successfully completing the interview guide. According to the criteria outlined by Borg and Gall (1996), the respondents' return rate can be characterized as outstanding. The researcher took precautions to ensure that a significant majority of participants (17%) had service tenure of 25 to 30 years, while the smallest proportion had served for 1 to 6 years (8%). This approach was employed to ensure that the participants possessed substantial experience and understanding of the field of study, thereby enhancing the reliability of the gathered data. The implications of extended periods of employment, particularly within the same organization, were also considered.

The outcome from a population of 35 the main respondents revealed that, strongly agree (55%), Agree (20%), Undecided (15%) and finally Disagree (10%). This research finding were confirmed by Internet Security Threat Report (2013), that revealed that cyber threats is an increasing global phenomenon, the crime is increasing at a faster rate in Kenya than in any part of the world. Most experts approximate that 80% of individual computers on the African continent are infected with viruses together with other malicious software, (Ranz-Stefan Gacy, 2010). The cyber threats rate in Kenya is associated with digital use especially in the social media and the face book which is the highly visited website has been identified as the most popular crime zone. The major crimes perpetuated include cyber bulling hate speech in form of short text messages, hacking, phishing and many others are a serious threat to national economic security.

The research indicates a rising trend in cyber threats affecting various organizations. Among the government's top priorities is harnessing the capabilities of the e-economy to generate employment and wealth, aligning with the national development strategy outlined in Kenya Vision 2030's ICT flagship, specifically focusing on the security of individuals and property. Achieving this objective involves leveraging technologies such as mobile banking, internet connectivity, and broadband communication to integrate the country into the global village. Notably, the majority of cyber-attacks identified in this study encompass cyber fraud (23%) and phishing (17%), aligning with the research data's interconnectedness with the study's findings. This section aimed to discern the prevalent types of cyber-attacks experienced by key respondents in their respective organizations. The study's findings are consistent with a similar investigation conducted by PWC (2015), highlighting the increasing opportunities and motivations for committing fraud in today's volatile economic environment.

The study demonstrates that Kenya has taken proactive measures to address the increasing cybersecurity threats by aligning with globally recognized standards. Recognizing the pivotal role of ICT in economic growth, Kenya has opted to collaborate with digital stakeholders to devise a strategy informed by their experiences with cyber risks. A spate of cyber incidents in 2023 tested Kenya's cybersecurity resilience amid its rapid digitalization, impacting government services and the digital financial ecosystem. While not the first cyberattacks faced by the country, they were the most severe to date, preceding incidents like defaced websites and alleged breaches by foreign entities. Financial systems, banks, and services like M-PESA have all faced cyber threats and vulnerabilities, leading to legal action against entities like Safaricom and the Communications Authority of Kenya for SIM-swap fraud.

The study highlights a significant rise in cyber threats alongside advancements in information technologies, which pose intricate challenges. These threats, known for their severe societal repercussions, especially when targeting critical national infrastructures, underscore the pressing need for robust cyber-security measures. Kenya maintains its leadership in mobile money usage among Kenyan banks despite facing a spectrum of cyber threats ranging from insider breaches to phishing and ransom-ware attacks. Vulnerable web applications and banking platforms have made banks' prime targets for cybercriminals, necessitating investments in proactive cybercrime prevention measures encompassing anticipation, detection, recovery, and containment.

While Kenya's financial landscape expands with the rapid growth of cooperatives and microfinance institutions, their focus on customer satisfaction and cost reduction often leads to neglect of cyber-security investments. The escalating prevalence of cyber threats in Kenya is increasingly recognized as a significant national security issue, exacerbated by the heightened vulnerability of critical infrastructure due to increased cyber connectivity. The banking industry, in particular, ranks just below the government in vulnerability to cybercrime due to the vast amount of data exchanged during transactions and the complex network infrastructure involved. Challenges in cybercrime litigation persist, primarily in identifying perpetrators, underscoring the nation's need for enhanced technical expertise, tools, and resources to bolster investigations and legal proceedings.

The research aimed to investigate the response mechanisms to cybercrime as a threat to Kenya's economic security. A majority of participants acknowledged the presence of measures, policies, and strategies on cybersecurity, offering guidance and safety measures. Specifically, 60% strongly agreed that the Cyber Security Policy has been effective in mitigating cyber-attacks, while 20% agreed, and 10% were unaware. Additionally, 15% could identify the Cyber Security Policy and Strategy of 2014, while 70% of respondents couldn't name any policy precisely, and 20% were uncertain.

The data reveals that Kenya, along with several other African states such as Uganda, Cameroon, and Botswana, has implemented policies and strategies to address cyber threats. Efforts are being made to enact cyber legislations and establish sub-regional collaboration instruments to combat cybercrime. Senegal and Morocco are considering joining the AU Convention, while ECOWAS nations are contemplating adopting the "Commonwealth Model Law on Computer Related Crime" and the "Budapest Convention on Cybercrime" along with the "Directive on Fighting Cybercrime" from the Council of Europe.

On the contrary, respondents who were undecided indicated that Kenya's cyber space vulnerabilities stem from rapid digitalization without commensurate defense capabilities. The level of cyber risks is directly correlated with the pace of global digitalization growth. These concerns align with the observations of Serianu Consultants

in Cyber Security (2015), who noted that institutions addressing cyber-security are lagging behind the rapid advancements in digital technologies.

According to some participants, a significant cyber-attack occurred in Kenya in 2017, targeting the National Bank of Kenya (NBK) and resulting in the theft of KES 29 million ($280,000) from the bank's infrastructure. The hackers utilized advanced techniques like phishing emails to gain unauthorized access to the bank's system, facilitating the transfer of funds to multiple accounts. This incident was corroborated by Okongo (2021), who highlighted another cyber-attack in 2018 where the Kenya Revenue Authority (KRA) reported a substantial loss of KES 4 billion ($40 million). Using the WannaCry malware, the attackers breached the authority's system, compromising sensitive data. To mitigate further damage, the KRA had to suspend its operations, leading to significant financial losses.

The research highlights the vulnerability of most Kenyans to attacks due to inadequate institutional security measures. It reveals a significant lack of awareness about cyber threats among internet users, enabling criminals to attack without detection. Consequently, both the government and financial institutions suffer substantial losses of funds and valuable information due to this lack of situational awareness. The existing cyber security measures are insufficient to tackle these issues effectively, as organizations lack the necessary security practices to safeguard critical cyber infrastructure. Therefore, Kenya must reassess its current measures and develop robust national cyber security strategies emphasizing threat management practices to anticipate, detect, respond to, and contain cyber threats.

CONCLUSION

The findings presented in this research underscore the emerging and acute danger cybercrime poses to Kenya's economic security. The study revealed that cyberattacks are becoming frequent and severe, especially against financial institutions, government services, and critical national infrastructure, for which this research achieved an 80% response rate from experienced respondents. The expansion of Kenya's digital economy and weak cybersecurity measures fuel the identified threats, which include cyber fraud, phishing, ransomware, and insider breaches.

Several of the evaluated policies, such as the Cyber Security Policy and Strategy of 2014, were unknown to the respondents, with the majority expressing ignorance of such policies. Hence, the study demonstrates that, though Kenya has progressed through harmonising with international cybersecurity standards and establishing stakeholders' collaborations, the response mechanisms remain inadequate. It challenges the nation's legal and technical competence in prosecuting cybercrimes and providing institutional resilience.

RECOMMENDATIONS

To address the increasing threat of cyber threats, the research suggests the need to develop adequate and effective cyber security measures, increased knowledge regarding cyber risks, and more effective cyber security policies. Furthermore, there is a need to emphasize the importance of better cooperation between African states, as can be seen, for example, in regional actions such as the signing of the Budapest Convention. Due to a lack of improvements in threat detection, response, and containment, the real potential of cybercrime in Kenya will remain a critical risk to economic security.

REFERENCES

1. Angela G and Martin R. (2012). Assessing Cyber Threats to Canadian Infrastructure. Report prepared for the Canadian Security Intelligence Service, pp. 8-10.
2. Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices, Carlifonia, USA
3. Brenner, S. (2017). Law in an Era of Smart Technology, Oxford: Oxford University Press, p. 375.
4. Broadhurst, R. (2017). Cyber Terrorism: Research Review, Australian National University, Cybercrime Observatory, Canberra, DOI, pp. 9-11.
5. Buzan, B. (1998). Security: A New Framework for Analysis, p. 23.
6. Chatterjee, D. (2019). "Should Executives Go to Jail for Cyber Security Breaches?" Journal of

Organizational Computing and Electronic Commerce, 29(1), 1–3.
7. Chuipka, A. (2016). "The Strategies of Cyber-terrorism." Graduate School of Public and International Affair, University of Ottawa, pp. 4-5.
8. Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016.
9. Gagliardone, I. (2014). Media Development with Chinese Characteristics. Global Media Journal, Government of Kenya. 2014. Cyber-security Strategy. Ministry of Information Communications and Technology, p. 6.
10. Kothari, C. (2011). Research Methodology-Methods and Techniques, New Age International Publishers, p. 11.
11. Mitchell, J. (2022) 'Africa faces huge cybercrime threat as the pace of digitalisation increases' available at https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/?cf-view (accessed 10th March 2024).
12. Okongo, C. (2021). "Evaluating the Challenges and Opportunities of the Use of Military Diplomacy in Intrastate Conflict Management in Horn of Africa." International Journalof Scientific Research, (2021), p. 2.
13. Ouma, C. (2021). "Effective Cyber Incident Response Capacity Framework for County Government in Kenya: A Case of Migori County." Department of Computing and Informatics, University of Nairobi, Nairobi, Kenya, pp. 2-4.
14. Paula, K. (2014). Kenya Cyber Security Report, 2014. Nairobi, (2014), p. 91-95.
15. Possony, S. T. (1946). Atomic power and world order. The Review of Politics, 8(4), pp. 533 535.
16. Powell, R. (2008). Nuclear deterrence theory: the search for credibility, Digitally printed version. Paperback Re Issue. Cambridge: Cambridge University Press.
17. Sayigh, Y. (2023). "Retain, Restructure, or Divest? Policy Options for Egypt's Military Economy." Annual Report, Carnegie Middle East Center, Cairo, Egypt, p. 13.
18. Schelling, T. C. (1980). The strategy of conflict: [with a new preface]. Cambridge, Mass: Harvard Univ. Press.
19. Sukumar, A and Amoozad, H. (2023). "Cyber Risk Assessment in Small and Medium-Sized Enterprises: A Multilevel Decision-Making Approach for Small E-Tailors." Wiley Publishers, p. 7.
20. The Government of Kenya. (2014). Cyber-security Strategy. Ministry of Information Communications and Technology, (2014), p. 76.
21. The United Nations Office on Drugs and Crime. (2012). Calculation from Study cyber crime questionnaire. Q30 and Symantec. Norton Cybercrime Report, pp. 121-12.
22. Zagare, F. C., & Marc Kilgour, D. (2000). Perfect deterrence. Cambridge Studies in International Relations. Cambridge: Cambridge University Press.
23. Zdzikot, T. (2021). "Cyberspace and Cyber security." Springer Link, pp. 29-32.
24. Ziewitz, M and Brown, I. (2013). A prehistory of Internet governance. In Brown, I. Research Handbook on Governance of the Internet Cheltenham: Edward Elgar, p. 17.