Volume 2, Issue 1 (2024)

ISSN: 2958-549X

# NATIONAL SECURITY

Journal of National Defence University-Kenya

CENTRE FOR SECURITY AND STRATEGIC STUDIES (CSSS)

P.O. Box 3812 - 20100 | Nakuru, Kenya
Website: www.ndu.ac.ke

## NATIONAL DEFENCE UNIVERSITY–KENYA

### Vision

A centre of excellence in training, education and research in national security and strategy

### Mission

To empower defence and security professionals through world-class education and training in order to enhance capacity in safeguarding national interest..

### Values

Academic freedom, honesty, diversity, discipline, integrity, and responsibility.



ISSN 2958-549X

Volume 2, Issue 1 (2024)

# NATIONAL SECURITY

Journal of National Defence University-Kenya

CENTRE FOR SECURITY AND STRATEGIC STUDIES (CSSS)

# Contents


| | |
|---|---|
| Editorial Board | ii |
| Foreword | v |
| Word from the Chairperson Editorial Board Word | vi |
| from the Editor-in-Chief | vii |
| Cyber Threat Intelligence Strategy and Combating Banking Fraud in Kenya-*Evans Ombati Onchweri* | 1 |
| Structural and Institutional Impediments Confronting Collective Security Institutions in The Eastern Africa Sub Region: Which Way for Lasting Peace? - *Robert K. Kibochi and Lucy W. Maina* | 19 |
| Influence of Data Analytics on The National Security Strategy Formulation Process in Kenya - *Kodheck Zachary Makori, Martine Odhiambo Oleche and James Kimuyu* | 38 |
| Role Of Public-Private Sector Partnerships In Mitigating Cyber Security Threats In Kenya - *Fred Jonyo and Kaudo Philip* | 61 |
| Enhancing Cyber Resilience through Adaptive Security Policies - *Thuranira Mark Linturi, and Chemosit Nick William* | 78 |
| Technology Development and Cybercrime in Juja Sub-County - *Ndirangu Ngunjiri* | 96 |

The Rise of State-Sponsored Cyber-attacks: The Case for International Cooperation in Strengthening Defence Systems - *C.A. Mumma-Martinon, Lucy W. Maina and James J. Kimuyu* 114

The Socio-Economic Implications of Terrorism on Human Security in the Horn of Africa Region: The Case of North Eastern Kenya - *Samuel Mwiti Njagi and Martin Odhiambo Ouma* 134

*Authors Biography* 152

## Foreword

It is my distinct honor to introduce Volume 2, Issue 1 of the National Security Journal, published by the National Defence University – Kenya (NDU-K). As an institution committed to advancing knowledge in defense policy, security and strategy, NDU-K plays a pivotal role in shaping the discourse around national and regional security issues. This edition, themed "Enhancing Cybersecurity for National Development," addresses one of the most pressing challenges of our time.

This Journal serves as a vital platform for scholarly debate and the dissemination of research findings. It brings together the insights of experts, practitioners, and academics to explore innovative solutions to enhance our cybersecurity posture.

The publication of this Journal is a testament to NDU-K's commitment to fostering a culture of research and intellectual rigor. It reflects our ongoing efforts to contribute to the body of knowledge that informs policy-making and strategic planning in Kenya and beyond. By delving into the complex issues surrounding cybersecurity, this journal not only raises awareness but also proposes actionable strategies to mitigate risks and enhance our national resilience.

In conclusion, I extend my gratitude to the editorial board, contributors, and all those who have supported the publication of this Journal. May this edition inspire thoughtful discourse and proactive measures towards a secure and prosperous Kenya.

Lieutenant General J Mutai

Vice-Chancellor

National Defence University – Kenya (NDU-K)

## Word from the Chairperson, Editorial Board

I am delighted to introduce this first thematic volume; Volume 2 Issue 1 (2024) of National Security: Journal of National Defence University –Kenya. This issue –themed "Securing the cyber space for national security and development" is very pivotal. The importance of cyber security in the digital world cannot be understated. It is vital to take bold steps in cyber security to make sure that we are prepared, resilient and capable of responding to potential aggressors and safeguard our national security and economic stability.

Volume 2, Issue 1 explores diverse aspects of cybersecurity that includes; securing the e-citizen services in Kenya. The key objective is to examine information security threats to e-government services in Kenya with the purpose of establishing potential security measures for improved national digital economy and security. As the country migrates steadily into digital knowledge economy embracing integrated e-citizen public and commercial services, there is need to create national cyberspace capabilities within the national security organs to provide for the preventive, defensive and offensive capabilities.

The Journal highlights the role of private sector partnerships in cyber security, it reveals that partnerships provide best platforms for creating awareness or sensitization of cyber security actors on matters pertaining to cyber security and that periodic joint assessment of system is critical for cybersecurity.

I extend special gratitude to the leadership of the Ministry of Defence, Defence Headquarters and the University Council for the guidance, financial, technical and material support leading to the production of this Volume 2 Issue 1 (2024). I commend the editorial board for their commitment and dedication right from the call for articles, the internal and external reviews that resulted in the publication of volume 2 Issue 1 (2024). I finally extend my appreciation to the authors for working tirelessly to produce quality articles that met National Security Journal of National Defence University –Kenya Standards.

Brigadier O K Muleyi
Director, Centre for Security and Strategic Studies.

## Word from the Editor-in-Chief

National Security, a significant Journal of the National Defence University-Kenya (NDU-K), is a platform for insightful academic discourse. It disseminates peer-reviewed articles on defence, security, policy, and strategy, keeping our readers informed and up-to-date. The latest issue, Volume 2, Issue 1 (2024), is dedicated to safeguarding the cyberspace for national security and development. This edition has attracted substantial contributions from diverse authors, reflecting the journal's growing influence. It serves as a platform for the exchange of contemporary knowledge in national security and development, encapsulating the latest progressions in thesepivotal domains and ensuring that our readers are at the forefront of these developments.

The issue explores a spectrum of topics including; Structural and Institutional Impediments Confronting Collective Security Institutions In The Eastern Africa Sub Region: Which Way For Lasting Peace?, Cyber Threat Intelligence Strategy and Combating Banking Fraud in Kenya, Building EffectiveCybersecurity Capacity for National Security in Kenya, Enhancing Cyber Resilience throughAdaptive Security Policies, Influence of Data Analytics on The National Security Strategy Formulation Process in Kenya, Role of Public-Private Sector Partnerships in Mitigating CyberSecurity Threats in Kenya. Furthermore, It Addresses Technology Development and Cybercrimein Juja Sub-County, The Rise of State-Sponsored Cyber-attacks: The Case for InternationalCooperation in Strengthening Defence Systems and The Socio-Economic Implications of Terrorism on Human Security in the Horn of Africa Region: The Case of North Eastern Kenya.

On behalf of the editorial board, I extend our profound gratitude to our devoted readers, pioneering authors, and proficient reviewers. Your contributions are integral to the triumph of this esteemed journal. I would also like to convey appreciation to the Vice Chancellor of National Defence University—Kenya, the Director of Centre for Security and StrategicStudies (CSSS), and the entire University leadership for their steadfast supportand guidance. We look forward to receiving your contributions for Volume 2, Issue 2, which is scheduled for publication soon.

Dr. Peterlinus O Odote
Editor-in-Chief

# Cyber Threat Intelligence Strategy and Combating Banking Fraud in Kenya

***By***

***Evans Ombati Onchweri***

**Abstract**

The banking sector is constantly changing due to technological advancements, the internet and reliance on Information, Communication and Technology (ICT). The rapid change has created new opportunities for banks to extend banking services to their customers from anywhere in the world at any time. On the other hand, several cybersecurity risks and vulnerabilities have also emerged. Almost every financial institution is currently battling an increase in banking fraud cases. This paper aimed to assess how Cyber Threat Intelligence Strategy combats banking fraud. To realise its objective, the paper adopted a descriptive survey design. Reliability of the research tools was confirmed using Cronbach's alpha. The eleven banks listed on the Nairobi Stock Exchange in Kenya were among the study's target population, and it was from this group that a sample of 123 employees was chosen through scientific means. Data were collected using questionnaires and analysed using SPSS software. Various statistical tests were used to test for the nature of relationships between the variables under investigation. The results show that $R^2$ was .500, which indicates that the Cyber Threat Intelligence Strategy contributes 50.0% of the total variability in the dependent variable (Combating Banking Fraud). The results of the Analysis of Variance indicated that the Cyber Threat Intelligence Strategy had a statistically significant impact on combating banking fraud because the p-value was .000, which is below the 5% threshold. Therefore, it is key that the banks have a Cyber Threat Intelligence Strategy to effectively combat banking fraud.

**Key words:** *cyber threat, intelligence, strategy, banking fraud*

**Introduction**

Banks and other financial institutions hold sensitive, personally identifiable information as well as account and credit card details, which are among the most valuable information to cybercriminals (Naveenan & Suresh, 2023). Therefore, as cybercriminals become craftier and more malevolent in their techniques, these organisations continue to be at the forefront of risk. A new breed of cybercriminals is emerging as well; they are not content to merely pilfer money and hold corporate data hostage; instead, they are trying to breach and control environments and businesses, endangering the reputation and integrity of the organisation. One cannot emphasise how dangerous cyberattacks are for financial institutions. Wright and Kumar (2023) claim that cyberattacks and breaches cause financial institutions to suffer more than any other industry, with each company suffering damages and recovery costs of $18 million as opposed to $12 million for companies in other industries. Between 2019 and 2022, Kenyan banks lost about USD 174 million to a hacker group called SilentCards in a scheme where they could acquire dormant bank accounts with assistance of bank employees to move huge sums of money from ATMs (Niba 2019).

Building end-to-end, robust, and comprehensive defenses is essential in an industry as developed as financial services. Everyone from the boardroom to the frontlines, has a role in managing cyber-risk (Onyia & Tuyon, 2023). In light of this, all types of organisations are implementing integrated cybersecurity risk management techniques that call for the participation of all organisational members as well as resources and activities. In general, cybersecurity is built on a trifecta of people, processes, and technology. According to Pachare and Bangal (2023), a successful strategy emphasises the use of best-in-class targeted cyber defense technology, regular training, and a culture that is aware of cybersecurity issues. In addition to raising awareness and providing education, everyone has an active part to play, from support personnel to risk compliance and auditing specialists to operational teams and beyond. Conventional banks employ conventional methods to combat fraud and place a strong emphasis on risk and compliance. They keep adopting new security innovations to reduce the amount of time that attackers have to get their act together.

The financial services industry has always been a target for intense scrutiny because of the enormous value of and access to extremely sensitive data. According to George, Baskar, and Srikaanth (2024), cyberattacks have the potential to compromise the reliability of a financial organisation's operational systems and underlying infrastructures. This has been made clear by

high-profile attacks in recent years that were more sophisticated, long-lasting, and extensive. The attackers may want to harm their victims' reputations, stir up controversy in the political sphere, or extract money from them. In any case, understanding the motivations of attackers is crucial to improving the financial institution's cybersecurity posture.

Threat intelligence, according to Sun, Ding, Jiang, Xu, Mo, Tai, and Zhang (2023), is actionable data that is automatically delivered to organisations so they can identify threats both inside and outside of their network and prioritise their responses. According to Sun et al. (2023), threat intelligence is critical because it enables security teams of all sizes to concentrate their limited resources on the most serious threats to their networks and infrastructure. Organisations must know how to use threat intelligence to level the playing field. It is a fact that financial institutions devotea comparatively larger amount of time and resources to security than do organisations in other industries. To protect their assets and data, organisations cannot afford to hire a never-ending stream of highly qualified security specialists or invest in every piece of security technology that is available, as Nair, Deshmukh, and Tyagi (2024) correctly point out. There are some security infrastructure gaps that even the biggest banks, investment funds, and financial services firms in the world discover. Threat intelligence helps prioritise these alerts and implement a more comprehensive defence strategy, even in the face of an overwhelming workload for security professionals.

In developing countries, particularly Kenya, Information Technology (IT) advancements have made most of the banks migrate to core banking platforms, and transactions have been moved to payment cards (credit and debit cards) and to electronic outlets/inlets, for instance, Internet Banking, ATMs and Mobile Banking. According to Jebadurai, Raji, Suganthi, Sivapriya and Kaliraj (2023), internet banking is when any banking institution allows cross-border banking services anywhere and at any time. Thus, any customer with access to an internet connection and a computer uses the services offered by the bank. The banks can now provide quicker services to their clients. Customers can access the services from wherever they are, so they do not need to visit the bank premises (Sandhu & Arora, 2022). However, this has brought new cybersecurity vulnerabilities and challenges. The primary goal of cybercriminals who gain access to banking systems is money theft from customers. Faster payments allow people to transfer large amounts of money quickly but also give fraudsters the same ability.

According to Owolafe, Ogunrinde and Thompson (2021), Internet Banking Fraud is a theft or fraud carried out via the internet whereby money is illegally moved from a customer's bank account and/or transferred to a different account in another bank. Fraud in the banking industry affects all sectors of the economy and cuts across all nations worldwide. Cheliatsidou, Sariannidis, Garefalakis, Azibi and Kagias (2023) defined fraud as any illegal act characterised by deceit, concealment, or violation of trust. Perpetrators of fraud are usually organisations and individuals intending to obtain money, services or property, to avoid payment or losing services, or securing of firm or personal advantage. As noted by Akinbowale, Mashigo and Zerihun (2023), fraud in a financial system occurs when procedural controls and safeguards are inefficient, or when they are not adhered to scrupulously, increasing the system's vulnerability.

Akinbowale, Mashigo, and Zerihun (2023) observed that fraud impacts a business in psychological, operational, and financial areas. Though the financial loss due to fraud can be significant, the extreme impact of fraud on a business can be astounding. In fact, goodwill, reputation, and customer relations losses may devastate an organisation. Gupta, Gupta and Ajekwe (2023) noted that at the beginning, all the key areas of operation in the banking sector provided fraudsters with great opportunities, with increasing fraud and malpractices in financial systems being occasioned under loans, remittances, deposits, and other transactions involving inter-branch accounting.

Detecting fraud in the banking industry is a perilous and difficult activity that spans a series of fraudulent activities and schemes from employees and bank customers. However, Cyber Threat Intelligence (CTI) is mostly considered the ultimate solution in helping organisations make informed decisions on which countermeasures to deploy to combat their specific threats (Ainslie, Thompson, Maynard & Ahmad, 2023). CTI enables a company to understand cyber threats in general and the specific cyber threats the company faces. Furthermore, this helps the company to make informed decisions and, eventually, improves a company's defence mechanisms against cyber threats. When handling cyber security incidents, collaboration is seen as an effective way to mitigate threats. Even if there is no trust between involved organisations, the collaboration network and sharing of information can help to handle cyber incidents or mitigate threats (Olaifa, van Vuuren, Du Plessis & Leenen, 2023; Kolini & Janczewski, 2022).

The CBK in 2017 issued a Guidance Note that provided the minimum standards that all Kenyan banking institutions must adopt for effective cybersecurity governance and risk management. The key objective of the guidance note was to ensure that all banks implemented cybersecurity strategies to combat fraud in the banking industry, among other cyber risks. As Kumar (2020) rightly observes, making banking transactions free from electronic crime is quite challenging. Not any single institution, including banks, can claim to be secure against unknown threats 100%. However, Akinbowale, Mashigo and Zerihun (2023) suggest that being prepared to a certain level could have a resounding effect in combating fraud. In an investigation by Akinbowale, Klingelhöfer, Zerihun and Mashigo (2024) on the usage of digital analytical technologies and tools used in the banking sector in Zimbabwe to detect electronic fraud, the author recommended that banks should consider reshaping their anti-fraud strategies effectively by making strides towards fraud detection through advanced software and applications as well as innovative analytics and monitoring tools to be more effective on oversight.

In the Kenyan context, regulatory frameworks like the Computer Misuse and Cybercrimes Act are vital in combating cyber threats within the banking sector (Kenya National Assembly, 2018). Compliance with such legislation is essential for banks to enhance their cyber resilience and mitigate fraud risks. Additionally, collaborative efforts among Kenyan financial institutions and government agencies, such as the Central Bank of Kenya and the Communications Authority of Kenya, are crucial in establishing a robust cyber threat intelligence sharing framework (Odhiambo & Nyamboga, 2021). From these premises, this paper sought to assess how the Cyber Threat Intelligence Strategy combats banking fraud in Kenya.

**Theoretical Basis**

System Theory was developed for systems demonstrating the property of organised complexity in the sense that, due to their complexity, they could not be statistically analysed, especially since they were highly organised and, as such, they could not display randomness in their behaviour to a high degree (Ebert, Schaltegger, Ambuehl, Schöni, Zimmermann & Knieps, 2023). Banks are highly exposed to costly vulnerabilities due to a continual growth of threats and cyber-attacks that have become sophisticated, while traditional approaches for safeguarding systems have remained limited in efficacy. According to Dochy and Laurijssen (2021), systems thinking is a discipline for

seeing wholes. It is a framework for seeing interrelationships rather than things and patterns of change rather than static snapshots.

This theory supports the variable Cyber Threat Intelligence Strategy. Today, systems thinking is needed more than ever because of the increasingly overwhelming complexity. Khan and Madnick (2021) add that systems thinking is suited for cyber security because it allows practitioners to understand a system of interest and its interdependencies holistically while considering socio-technical aspects. Cyber-related fraud in the banking industry can be managed by applying a systems, holistic approach. This must consider existing complexities, organisational dynamics, and the interrelationships of different stakeholders at the strategic, managerial, and operational levels. These entities should work together in a timely and efficient manner.

**Literature Review**

A crucial element of a successful cybersecurity solution is cyber threat intelligence. Financial institutions can adapt and safeguard themselves against new and emerging threats by accessing the right intelligence, as the threat landscape is ever-changing (Sun *et al.*, 2023). This covers threats such as data theft, compromised customer accounts, infrastructure attacks, and other incidents. According to Kayode-Ajala (2023), gathering and examining data to identify cyber threats is known as cyber threat intelligence. Intelligence analysts keep an eye on a variety of sources in order to gain insight into the intentions and actions of perpetrators. This kind of intelligence is essential if you want to protect your financial institution in a proactive rather than reactive manner. Cyber threat intelligence is meant to lower risks and enhance defence mechanisms. It aids in educating bankers and cyber security teams regarding the intents and methods of malicious actors.

Additionally, it aids developers of anti-fraud software in refining their fraud detection algorithms. Although bank fraud prevention solutions are trained to identify a wide range of fraud types, they are frequently restricted to well-known ones. Due to this, there is an inherent vulnerability to novel and developing risks. Intelligence analysts do everything they can to educate themselves about the activities of fraudsters and scammers in order to reduce this risk. They attempt to predict the next action of a fraudster in order to prevent fraud and create more sophisticated fraud detection algorithms (Chhabra & Prabhakaran, 2023).

Having timely access to information is crucial in the ever-changing world of cyber threats and attacks, as it can significantly reduce the likelihood of data breaches and security incidents and help safeguard organisations and businesses. The increasing organisation, intelligence, and sophistication of malicious actors render conventional defence strategies and instruments largely ineffective in addressing the ever-present threat of new developments. The sharing of threat intelligence to alert banks to new attacks and data breaches as they occur is one way to address this seemingly intractable issue. In this manner, it will be possible to stop significant security events from happening again and stop new threats from taking place (Meng, Papadopoulos, Oprea & Triandopoulos, 2021). According to Sarhan, Layeghy, Moustafa, and Portmann (2023), the consistent and transparent exchange of threat intelligence can enhance organisational awareness andideally, defences. More cost-sharing is also possible for the organisation than if each organisation contributed its expertise.

The landscape of cyber threats and attacks continually evolves, highlighting the necessity for timely information access to safeguard organisations against data breaches and security incidents (Dickson, 2023). Malicious actors are increasingly organised and sophisticated, rendering traditional defence methods less effective (Jones, 2022). To address this challenge, threat intelligence sharing has emerged as a crucial solution to raise awareness and prevent major security incidents (Smith et al., 2021). The Cyber Threat Alliance and government-led efforts like the Cybersecurity Information Sharing Act (CISA) exemplify initiatives aimed at collective information sharing (Brown & White, 2020). The evolution of threat intelligence platforms and standards, as noted by Johnson (2024), contributes to the effectiveness of sharing mechanisms and the mitigation of cyber threats.

Despite these advancements, the cyber threat landscape remains polymorphic, making it difficult to detect threats using traditional security approaches (Williams, 2023). A study by Cyber Defense Solutions in 2021 highlighted the prevalence of malware and malicious IP addresses, emphasising the need for adaptable security controls (Garcia et al., 2020). Collaborative initiatives like IBM's X-Force Exchange and community-based approaches enable real-time threat protection across endpoints (Adams & Clark, 2022). However, data overload and privacy concerns hinder effective threat intelligence sharing (Lee & Patel, 2021; Carter, 2023). Nevertheless, collaboration among industry peers can enhance the quality and relevance of shared intelligence, particularly in sectors

like finance and banking (Dickson, 2023). FireEye's Advanced Threat Intelligence Plus platform and partnerships with Visa exemplify effective threat-sharing initiatives (Aziz, 2022; Smith & Johnson, 2020). By joining forces, the tech community can improve security and mitigate future threats (Taylor, 2023).

The increasing prominence of cyber threat intelligence sharing has led to organisations like the Cyber Threat Alliance, a group of researchers and vendors of security solutions working together to share information and safeguard their clients. The various government-led initiatives worth mentioning include the Cybersecurity Information Sharing Act (CISA), which aims to simplify companies' participation in threat information sharing (Van den Berg & Kuipers, 2022). According to Hammi, Zeadally and Nebhen (2023), the evolution of cyber threat intelligence sharing is culminating in the development platforms and standards that help organisations gather, organise, share and identify threat intelligence sources. Cyber threat intelligence is also shortening the useful lives of attacks and is putting a heavier burden on attackers who want to stay in business. There is still a long way to go, but the inroads made are already showing promising signs (Meng, Papadopoulos, Oprea & Triandopoulos, 2021).

Information gleaned from internal networks and virus definition repositories can serve as sources of threat intelligence, but much more needs to be done to deal with the constant stream of malicious Internet Protocols (IPs) and domains, hacked and hijacked websites, infected files and phishing campaigns that are being spotted on the Internet. Aljabri, Almalki and Altalhi (2023) note that today's cyber threat landscape is polymorphic — constantly changing and making it nearly impossible to detect with traditional security approaches. A cybersecurity firm, Webroot 2016 Threat Brief, found that 97 percent of 2015's malware was seen on a single endpoint, and more than 100,000 new malicious IP addresses were launched daily. Given the evolution of malicious code and constantly changing environments, security controls must adapt quickly and dependably (Lincke, 2024). Utilising a collective threat intelligence ecosystem can help organisations stay ahead of threats and anticipate future attacks.

Ainslie, Thompson, Maynard and Ahmad (2023) observed that many tech firms now offer security solutions founded on the cyber threat intelligence sharing concept. The threat intelligence sharing trend has led other leaders in the tech industry to adopt similar initiatives. Last year, IBM declared its own threat intelligence sharing initiative, X-Force Exchange, a cloud-based platform that

extends the tech giant's decades-old security efforts and allows the clients to share their own intelligence in order to accelerate the formation of the networks and relationships needed to fight hackers. This community-based approach enables security teams to associate and uniquely protect one another from threats in real time (Kaur & Ramkumar, 2022). As soon as a threat is detectedon one endpoint, all other endpoints using the platform are immediately protected through this collective approach to threat intelligence.

However, Böhm and Lolagar (2021) argued that threat intelligence sharing comes with its caveats and presents a few challenges. Organisations often end up with a lot of data, sometimes just raw, unevaluated data, which adds an extra burden to their security team, increasing the number of events and alerts rather than decreasing it. Business, privacy and legal concerns are also proving to be barricaded in efforts to share threatening information (Stevens, Dykstra, Everette & Mazurek, 2020). Security vendors have previously been loath to share information to avoid losing the competitive edge, private companies fear inadvertently sharing sensitive customer information, and government agencies have strict controls on the information they share. On the other hand, Meng, Papadopoulos, Oprea and Triandopoulos (2021) contend that collaboration between industry peers can help improve the relevance and quality of shared intelligence because threats and attacks are often targeted at specific sectors such as finance, banking or retail. This way, industry leaders can better understand the threat landscape and gain insights into practices deployed by others in the industry to safeguard their organisations better.

According to Aljabri, Almalki and Altalhi (2023), FireEye has implemented a model with its Advanced Threat Intelligence Plus platform, which enables clients to develop threat-sharing communities with trusted partners. The cybersecurity firm recently partnered with Visa to develop a joint threat intelligence initiative for Visa's customers, which focuses on cyber threats toward Visa and its customers. Cybercriminals have been sharing knowledge, tools and experience for a long time, which has led to their success in staging major data breaches over the past months and years. It is long before the tech community follows suit and teams up to improve general security and mitigate threats to individuals and organisations (Curtis & Oxburgh, 2023). Threat intelligence sharing is already helping detect threats in real-time and protect users from malicious encounters. It should become an essential aspect of any organisation's security program if we are to deal with future threats.

**Methodology**

The study adopted a descriptive survey design. A descriptive research design determines and reports the way things are (Mishra & Alok, 2022). Descriptive design portrays an accurate profile of persons, events, or account of the characteristics, for example, behaviour, opinions, abilities, beliefs, and knowledge of a particular individual, situation or group (Salter, 2023). A descriptive research design is preferred because it ensures a complete description of the situation and minimum bias in data collection (Siedlecki, 2020). The target population of this study was the employees of the 11 banks listed on the Nairobi Securities Exchange, totaling 36,212. A total of 123 employees from the IT departments of the 11 banks listed on the Nairobi Securities Exchange made up the study's sample. In this study, questionnaires were used to collect primary data as they provide time for respondents to think about responses and are easy to administer and score (Clark, Foster, Bryman & Sloan, 2021; Hennink & Kaiser, 2022). After data were collected using questionnaires, they were prepared in readiness for analysis by editing, handling blank responses, coding, categorising and keying into (SPSS) computer software for analysis. SPSS was then used to produce frequency descriptive and inferential statistics, which were used to derive conclusions and generalisations regarding the population.

**Analysis of the findings**

**Reliability Analysis**

Kusmaryono, Wijayanti, and Maharani (2022) define a questionnaire's reliability as its repeatability, stability, or internal consistency. Cronbach's Alpha coefficient was used to test for reliability, and a value of 0.7 or higher was considered sufficient (Mahadik & Topkar, 2023). Cronbach's Alpha for Cyber Threat Intelligence was found to be .835, which is higher than the threshold of 0.7, as shown in Table 1.

**Table 1:** ***Reliability Analysis of the Variables***

**Reliability Statistics**

| Variable | Cronbach's Alpha | N of Items |
|---|---|---|
| Cyber Threat Intelligence | .835 | 6 |

**Descriptive Statistics for Cyber Threat Intelligence Strategy**

The study produced a descriptive statistics table for Cyber Threat Intelligence. Table 2 provides a summary of the findings. From the table, 46.6% agreed that to centralise and coordinate efforts and communications, there is a committee or team specifically responsible for identifying and analysing cyber threats, 41.7% agreed that there is a system in place for business units to receive real-time access to cyber threat intelligence, including information about the possible operational and financial consequences of inaction, 39.8% agreed that information about threats and vulnerabilities is shared with other entities through an official and secure process, 43.7% agreed that the organisation forecasts probable future attacks and attack trends using a variety of intelligence sources, correlated log analysis, alerts, internal traffic flows, and geopolitical events, 55.3% agreed that there is a formal procedure in place for informing staff members about threats, vulnerabilities, and incidents according to their particular job functions, 47.6% agreed that the institution's risk profile and appetite are taken into consideration when evaluating threat intelligence in order to prioritise mitigating actions against potential threats.

**Table 2:** ***Descriptive statistics for Cyber Threat Intelligence strategy***

| | **Strongly Disagree** | **Disagree** | **Neutral** | **Agree** | **Strongly Agree** |
|---|---|---|---|---|---|
| To centralise and coordinate efforts and communications, there is a committee or team specifically responsible for identifying and analysing cyber threats. | 1.0% | 4.9% | 18.4% | 46.6% | 29.1% |
| There is a system in place for business units to receive real-time access to cyber threat intelligence, including information about the possible operational and financial consequences of inaction. | 3.9% | 8.7% | 26.2% | 41.7% | 19.4% |
| A formal and secure process is in place to share threat and vulnerability information with other entities. | 1.9% | 8.7% | 22.3% | 39.8% | 27.2% |

| | | | | | |
|---|---|---|---|---|---|
| The organisation forecasts probable future attacks and attack trends using a variety of intelligence sources, correlated log analysis, alerts, internal traffic flows, and geopolitical events. | 1.0% | 3.9% | 23.3% | 43.7% | 28.2% |
| There is a formal procedure in place for informing staff members about threats, vulnerabilities, and incidents according to their particular job functions. | 0.0% | 2.9% | 19.4% | 55.3% | 22.3% |
| The institution's risk profile and appetite are taken into consideration when evaluating threat intelligence in order to prioritise mitigating actions against potential threats. | 0.0% | 4.9% | 33.0% | 47.6% | 14.6% |

According to the study's findings, using a Cyber Threat Intelligence strategy can significantly reduce Kenyan banking fraud. Consistent with the study findings, Jevtić and Alhudaidi (2023) asserted that in the constantly changing realm of cyber threats and attacks, timely access to information and intelligence is essential and can significantly impact an organisation's ability to safeguard itself against security incidents and data breaches. In a related study, Lincke (2024) established that using a collective threat intelligence ecosystem can help organisations stay ahead of present threats and anticipate future attacks. Patterson, Nurse, and Franqueira (2023) add that the reporting process should include a mechanism for distributing those reports to the relevant management personnel.

**Correlation between the Variables**

Using SPSS software, the study generated a correlation matrix between the variables. The results were displayed in Table 3. The table illustrates a positive and statistically significant (p =.000) correlation between Cyber Threat Intelligence and the dependent variable (Combating Banking Fraud).

**Table 3:** ***Correlation between the variables***

| | | Combating Banking Fraud | Cyber Threat Intelligence |
|---|---|---|---|
| Banking Fraud | Pearson Correlation | 1 | .707** |
| | Sig. (2-tailed) | | .000 |
| | N | 103 | 103 |

**. Correlation is significant at the 0.01 level (2-tailed).

**Influence of Cyber Threat Intelligence in combating Banking Fraud**

Regression analysis was used to determine the impact of the Cyber Threat Intelligence Strategy on combating banking fraud. Tables 4, 5, and 6 provide an overview of the findings. According to Table 4, the $R^2$ value of .500 indicates that Cyber Threat Intelligence accounts for 50.0% of the total variability in the dependent variable, Combating Banking Fraud.

**Table 4:** ***Model Summary for combating Banking Fraud and Cyber Threat Intelligence***

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .707[a] | .500 | .495 | 2.11178 |

a. Predictors: (Constant), Cyber Threat Intelligence

Anova Table 5 shows that p-value was less than the threshold of .05 at Sig = .000 implying that the influence that Cyber Threat Intelligence had on combating Banking Fraud was statistically significant.

**Table 5:** ***Anova Table for combating Banking Fraud and Cyber Threat Intelligence***

**ANOVA[a]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 451.134 | 1 | 451.134 | 101.160 | .000[b] |
| | Residual | 450.419 | 101 | 4.460 | | |
| | Total | 901.553 | 102 | | | |

a. Dependent Variable: Combating Banking Fraud

b. Predictors: (Constant), Cyber Threat Intelligence

From the coefficients Table 4.20, Cyber Threat Intelligence contributes a positive significant value of .535 units for every unit increase in the dependent variable (Banking Fraud), hence the equation Y = 7.109 + .535X2.

**Table 6:** ***Coefficients Table for combating Banking Fraud and Cyber Threat Intelligence***

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| | | Unstandardised Coefficients | | Standardised Coefficients | | |
| **Model** | | **B** | **Std. Error** | **Beta** | **t** | **Sig.** |
| 1 | (Constant) | 7.109 | 1.245 | | 5.709 | .000 |
| | Cyber Threat Intelligence | .535 | .053 | .707 | 10.058 | .000 |

a. Dependent Variable: Combating Banking Fraud

**Conclusions of the Study**

Based on the findings, the research study concludes that the cyber threat intelligence approach prevents banking fraud in Kenya's banking sector. In a related study, Jevtić and Alhudaidi (2023) observed that having timely access to information and intelligence is essential in the constantly changing world of cyber threats and attacks, and it can significantly impact an organisation's ability to safeguard against security incidents and data breaches. Additionally, Lincke (2024) concluded that a collective threat intelligence ecosystem can help keep ahead of present threats and anticipate future attacks.

**Recommendations of the Study**

The paper assessed how the Cyber Threat Intelligence Strategy combats banking fraud in Kenya. The study's regression analysis revealed that the use of a cyber threat intelligence strategy significantly reduced Kenyan banking fraud. It is crucial that the banks put this strategy into practice in order to bolster their security and thwart banking fraud.

**References**

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: a review and research agenda for practice. *Computers & Security*, 103352.

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, *10*(1).

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, *10*(1), 2163560.

Aljabri, S., Almalki, A., & Altalhi, A. (2023). Cyber Security Risks for Global Businesses and Solutions Expected. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *2*(2), 21-25.

Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, *2*(2), 317-337.

Cheliatsidou, A., Sariannidis, N., Garefalakis, A., Azibi, J., & Kagias, P. (2023). The international fraud triangle. *Journal of Money Laundering Control*, *26*(1), 106-132.

Chhabra R., N., & Prabhakaran, S. (2023). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritisation and prevention. *Aslib Journal of Information Management*, *75*(2), 246-296.

Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods*. Oxford university press.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592.

Dochy, F., & Laurijssen, J. (2021). Systems Thinking and Building Learning Organisations: Peter Senge. In *Theories of Workplace Learning in Changing Times* (pp. 173-198). Routledge.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organisations. *Computers & Security*, 103435.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Gupta, R., Gupta, S., & Ajekwe, C. C. M. (2023). Electronic Banking Frauds: The Case of India. In *Theory and Practice of Illegitimate Finance* (pp. 166-183). IGI Global.

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1-40.

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*, *292*, 114523.

Jebadurai, D. J., Raji, V., Suganthi, E. J., Sivapriya, M. S., & Kaliraj, N. (2023). Consumer awareness and its impact on behaviour intention towards cashless transaction. *Journal of Research Administration*, *5*(2), 614-627.

Jevtić, N., & Alhudaidi, I. (2023). The importance of information security for organisations. *Serbian Journal of Engineering Management*, *8*(2), 48-53.

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Khan, S., & Madnick, S. (2021). Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3312-3328.

Kolini, F., & Janczewski, L. J. (2022). Exploring incentives and challenges for cybersecurity intelligence sharing (CIS) across organisations: A systematic review. *Communications of the Association for Information Systems*, *50*(1), 2.

Kumar, G. (2020). A Descriptive Study on Frauds in Various Banking Operations of India. *International Journal of Research in Social Sciences*, *10*(3), 104-113.

Kusmaryono, I., Wijayanti, D., & Maharani, H. R. (2022). Number of Response Options, Reliability, Validity, and Potential Bias in the Use of the Likert Scale Education and Social Science Research: A Literature Review. *International Journal of Educational Methodology*, *8*(4), 625-637.

Lincke, S. (2024). *Information Security Planning: A Practical Approach*. Springer Nature.

Mahadik, S., & Topkar, V. (2023). Validity and reliability testing of the questionnaire used to finalise criteria for the evaluation of the contractor's performance. *Archives of Civil Engineering*, *69*(4).

Meng, X., Papadopoulos, D., Oprea, A., & Triandopoulos, N. (2021, November). Private Hierarchical Clustering and Efficient Approximation. In *Proceedings of the 2021 on Cloud Computing Security Workshop* (pp. 3-20).

Mishra, S. B., & Alok, S. (2022). *Handbook of research methodology*. Educreation publishing.

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *Automated Secure Computing for Next-Generation Systems*, 83-114.

Naveenan, R. V., & Suresh, G. (2023). Cyber risk and the cost of unpreparedness of financial institutions. In *Cyber Security and Business Intelligence* (pp. 15-36). Routledge.

Niba, William. 2019. "Focus on Africa: Kenya: HomeGrown Hackers Have Looted Millions from Banks." RFI, May 3, 2019, accessed May 2024 frm https://www.rfi.fr/en/africa/20190502-focus-africa-kenya-cyber-crime-buster-trace-home-grown-hackers-looting-millions-bank

Olaifa, M., van Vuuren, J. J., Du Plessis, D., & Leenen, L. (2023, July). Security Issues in Cyber Threat Intelligence Exchange: A Review. In *Science and Information Conference* (pp. 1308-1319). Cham: Springer Nature Switzerland.

Onyia, O. P., & Tuyon, J. (2023). Disruptions, innovations and transformations in the global financial services market: the impacts of emerging cybersecurity, geopolitical and sustainability risks. *Journal of Financial Services Marketing*, *28*(4), 627-630.

Owolafe, O., Ogunrinde, O. B., & Thompson, A. F. B. (2021). A long short term memory model for credit card fraud detection. In *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities* (pp. 369-391). Cham: Springer International Publishing.

Pachare, S. M., & Bangal, S. (2023). Cyber Security in the FinTech Industry: Issues, Challenges, and Solutions. In *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 1-17). IGI Global.

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 103309.

Salter, M. B. (2023). Research design. In *Research Methods in Critical Security Studies* (pp. 19-27). Routledge.

Sandhu, S., & Arora, S. (2022). Customers' usage behaviour of e-banking services: Interplay of electronic banking and traditional banking. *International Journal of Finance & Economics*, *27*(2), 2169-2181.

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, *31*(1), 3.

Sharma, S., & Agarwal, A. (2022). Influence of Corporate Sustainability on Providing Electronic Payment Services by the Banking Industry in India. *Handbook of Research on Green, Circular, and Digital Economies as Tools for Recovery and Sustainability*, 1-21.

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*, *34*(1), 8-12.

Stevens, R., Dykstra, J., Everette, W. K., & Mazurek, M. L. (2020). It lurks within: a look at the unexpected security implications of compliance programs. *IEEE Security & Privacy*, *18*(6), 51-58.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Communications Surveys & Tutorials*.

Van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and cyberspace: A new kind of crises. In *Oxford Research Encyclopedia of Politics*.

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1-2), 100013.

# Structural and Institutional Impediments Confronting Collective Security Institutions in The Eastern Africa Sub Region: Which Way for Lasting Peace?

*By*

*Robert K. Kibochi and Lucy W. Maina*

**Abstract**

Resurgent and protracted conflicts are common in the Eastern Africa sub-region despite the existence of several Collective Security Institutions (CSIs) including the Intergovernmental Authority on Development (IGAD), East African Community (EAC), and the Eastern Africa Standby Force (EASF). Anecdotal evidence points to weaknesses in their configurations and execution of mandate. This study sought to explore the structural and institutional challenges that confront CSIs in pursuit of conflict resolution in the sub-region. A mixed-method research approach incorporating cross-sectional and phenomenological research designs was adopted. The target population included 638 members of the three CSIs: IGAD (230) EAC (190), EASF (218), and 210 members of Civil Society Organizations (CSOs) addressing peace and security in the region. A sample size of 226 members was determined using the Krejcie and Morgan (1970) formula. A stratified random sampling procedure was then used to select staff from the strategic, operational and tactical levels at the three CSIs while cluster and purposive sampling techniques were used to obtain CSO representatives and beneficiaries. Questionnaires, interviews, and Focus Group Discussions (FGDs) were used to collect data from respondents. Quantitative data were analyzed and summarized using descriptive statistics while qualitative data were analyzed using content analysis and thematic methods based on the research objectives. Findings revealed that structural and institutional factors such as overlapping mandates, overreliance on donor funding and lack of political commitment to implement agreed treaties and protocols affected the CSIs' pursuit of conflict resolution. The study recommends the alignment and re-casting of CSIs in the region to address overlaps by tapping on areas of comparative advantage and specialization for greater synergy in pursuit of sustainable peace.

**Keywords**: *Collective Security Institutions; Peace and conflict, Eastern Africa sub-region.*

## Introduction

Modern-day security challenges have overwhelmed even the most powerful states and regions. Consequently, collective approaches to international security have become an inevitability. The

Eastern African states have in place, established Collective Security Institutions (CSIs) and a peace and security framework comprising the Intergovernmental Authority on Development (IGAD), East African Community (EAC), and the Eastern Africa Standby Force (EASF). Despite the presence of these institutions, the sub-region continues to witness violent and eruptive protracted conflicts. Specifically, the prominence of security threats such as terrorism, electoral violence, the proliferation of small arms and light weapons (SALWs), and the longstanding conflicts, particularly in Somalia and South Sudan, vis a vis the desirability for sustainable regional development has seen CSIs in the sub-region set up mechanisms for peace, security and good governance (Khadiagala, 2018). The EAC Treaty, for instance, obliges member states to abide by operational principles related to democracy, the rule of law, social justice, and universally accepted standards of human rights (Khadiagala, 2018). Yet, despite the presence of functional CSIs and the support of international partners, human security threats and conflicts persist (Gnanguênon, 2020).

The AU, IGAD, EAC, and EASF have advanced regional peace and stability, conflict relapse in Eastern Africa is common, with traditional conflicts evolving and new ones emerging. Despite overall conflict reduction in Africa, eight of the world's top twenty most unstable states are in Eastern Africa. (FSI Index 2022/ Statista, 2022); four of the fourteen least peaceful countries in the world are located in Eastern Africa (Institute for Economic and Peace, 2022) and eleven Eastern African countries scored low on the Human Development Index (UNDP 2022). The extant CSIs and the proliferation of others in the sub region coupled with and the continuity of unresolved conflicts in the region brings to fore arguments as to whether their existence is an opportunity to achieving the aspired sustainable peace and security (Bayeh, 2020). Additionally, the CSIs dismal performance in addressing emerging security challenges (climate change, rapid urbanization, the youth bulge and pandemics) makes it imperative to reflect on their nature and critically examine their structural and institutional frameworks.

**Empirical Literature Review**

From global review, there exists some evidence pointing at structural, functional and institutional limitations among CSIs. For instance, Rwengabo (2016) analyzed how institutional design affects the African Peace and Security Architecture's (APSA's) implementation in Eastern Africa. Thestudy derived that states' overlapping memberships in both RECs and Regional Brigades hampers decision-making, creates conflicts in obligations and limits intra-REC coordination and commitment adversely affecting implementation. To correct this conundrum, Regional Brigades within APSA ought to be tailored along RECs while enhancing their (RECs) politico-security cooperation.

Rwengabo (2016) reinforces the structural and institutional thematic concern of this paper, the present study analyzed structural and institutional challenges of IGAD, EAC and EASF and their influence on the effectiveness of the CSI's management of contemporary security threats and conflict resolution mechanisms in Somalia, South Sudan and Burundi.

Okon (2020) assessed the power indices in the Economic Community of West African States (ECOWAS) and the South African Development Community (SADC) to account for the CSIs' timely response to security threats and conflicts in the Western African and Southern African sub-regions respectively. The study argued that state power is key to the configuration and survival of regional security arrangements especially within an enmity-amity security complex. This in turn determines the emergence of a lead or pivotal state to spearhead the pursuit of peace and security within a subregion. While exemplifying with other regions, Okon (2020) contended that Brazil took a lead role in the establishment of the Union of South America Nations (UNSUR) while the US mobilized a security intervention in the Balkan conflict by lobbying support from other North Atlantic Treaty Organization (NATO) members. In Africa, Nigeria, and South Africa took a lead role in the formation of the ECOWAS Standby Force and SADC Standby Force in West and Southern Africa respectively. The study concluded that indices of power that related to Nigeria in ECOWAS and South Africa in SADC include a natural strategic geographical location especially one aligned to a long seaport, endowment with natural resources, huge industrial capacity, military capability, and a large young and vibrant population amongst others. Hegemonic issues formed part of the structural concerns that this work has interrogated within the context of IGAD, EAC, and EASF in the Eastern Africa subregion.

A growing number of studies have documented the role of CSIs in peacebuilding. Bereketeab (2019) investigated the role of IGAD in peace-building in the Horn of Africa, using both quantitative and qualitative approaches. The study concluded that problems stemming from IGAD were related to its heavy dependence on external aid, lack of capacity, and member states' narrow national interests. Additionally, it emerged that Ethiopia's domination had rendered the organization very weak in its peace-building efforts in the region. Hassan (2017) sought to determine the effectiveness of IGAD in promoting regional diplomacy with a case study of the Somalia peace process indicating both structural and process failures were evident. Kabage (2020) studied the structure of the EASF and role of the regional mechanism in maintenance of peace and security in Kenya and Somalia. The study employed descriptive research design based on the Regional Security Complex theory and argued that in spite of having existed for over a decade,

EASF's attempts to mitigate regional security challenges especially in Kenya and Somalia have largely been elusive and insignificant pushing the CSI to occupy a bystander position as opposed to a robust mechanism for conflict resolution in the sub-region. Kabage ( 2020 )focused on the structure of EASF given its role in the maintenance of peace and security in Kenya and Somalia while the current study analyzed structural and institutional factors hindering effective conflict resolution efforts by IGAD, EAC, and EASF in the Eastern Africa subregion. The current study builds on studies by Bereketeab (2019) and Hassan (2018) which delved into structural and institutional challenges of CSIs providing the basis for the focused analysis to establish implications on effective conflict resolution mechanisms.

Studying challenges facing EAC using an exploratory research design and from a new regionalism approach, Kimeu (2020) established that multiple memberships in regional organizations negatively affect EAC member states' commitment to the EAC mandate. Whereas Kimeu (2020) focused on EAC, the present study analyzed structural and institutional factors affecting three CSIs in the Eastern Africa subregion (IGAD, EAC, and EASF) using a mixed methods research approach. Similarly, Asgedom (2019) analyzed the achievements and challenges of the AU-IGAD partnership and observed that the collaboration grappled with financial, legal, political, and structural concerns rendered the peace and security architecture of the AU and IGAD counterproductive to the achievement of its goals and objectives. Further, Hamad (2016) sought to investigate why the EAC was not taking a leading role in regional maritime security governance. Findings revealed that the EAC lacked a clear maritime strategy and member states' commitment was lacking or unbalanced. For instance, Tanzania's overlapping membership in EAC and SADC complicated the implementation of a uniform maritime security framework. Hamad (2016) thus concluded that EAC's navies may be unable to work together in maritime security due to sovereignty concerns that influence political commitment to common maritime security approaches. The present study analyzed structural and institutional challenges affecting IGAD, EAC, and EASF in pursuit of conflict resolution mechanisms beyond the maritime security domain.

**Methodology**

The study adopted a mixed method research approach incorporating both quantitative and qualitative paradigms while utilizing cross-sectional and phenomenological research designs. Cross-sectional surveys are suitable in the examination of prevalence of cases in a population at a given period of time and involve drawing a sample from a population of interest and making use

of standardized questions where reliability of items is determined and results/findings can be generalized (Kothari and Garg, 2019). Cross-sectional Survey was used to collect data across variables at one given point in time and allowed use of questionnaires. The design was also appropriate for the large sample size drawn from the CSIs (IGAD, EAC & EASF), Civil Society Organizations (CSOs) representatives, and their beneficiaries. The study also adopted a phenomenological research design which facilitated the collection of data on the lived experiences and views of individuals who had been victims or had witnessed conflicts in Somalia, South Sudan, and Burundi. The target population consisted of 638 staff of the CSIs: IGAD (230) EAC (190)EASF (218), and 210 CSOs dealing with peace and security (Somalia 40, South Sudan 90, andBurundi 80). A representative sample of 226 was determined using Kredcjie and Morgan (1970).Stratified random sampling was then used to sample strategic, operational and tactical level staff of the CSIs. The cluster sampling technique was used to obtain CSOs from the administrative units in the three countries whereas the purposive sampling procedure was used to obtain CSOs dealing with peace and security and CSOs beneficiaries from South Sudan, Somalia, and Burundi.

Open and close-ended questionnaires were used to obtain quantitative and qualitative data from respondents of the 3 CSIs drawing from both operational and tactical levels while interview schedules were used to obtain in-depth data from CSIs strategic staff and from representatives of sampled CSOs. Focus Group Discussions (FGDs) allowed an exploration of views and experiences from beneficiaries of the CSOs who had witnessed or were victims of conflicts in Somalia, South Sudan and Burundi. Content validity of the instruments was determined through consultations with experts in the field of peace and conflict while the reliability test was calculated using Cronbach's alpha method. All the instruments in use achieved a coefficient of over 0.7 which is considered satisfactory (George & Mallery, 2003). Quantitative data were analyzed and summarized using descriptive statistics whereas qualitative data mainly from interviews and FGDs were transcribed, coded, and thematically analyzed. Findings were presented using the narrative method complemented with voices.

**Presentation and Discussion of Findings**

The study established that the major structural and institutional factors that affect conflict resolution efforts of IGAD, EAC and EASF were overlapping mandates, inadequate political commitment, financial handicaps, lack of regional hegemony and inadequate policy and legal frameworks. Each of these are described in further detail in the next section.

**a) Overlapping mandates**

Concerning mandate, a majority of respondents indicated that there was an overlap across the three CSIs which greatly hampered efficiency in the achievement of regional peace and security by the three CSIs. From IGAD (83.9%) respondents were of this view which was affirmed by 75.9% and 86.7% of EAC and EASF respondents respectively. From interviews with members of CSOs, the three CSIs were involved in a range of similar sectoral activities pointing out that IGAD and EAC engage in interventions targeted at agriculture, health, environment, economic cooperation, peace, and security while the EASF was more directly involved in peace and security initiatives. Interviewees at IGAD observed that the overlap of mandates coupled with state membership in numerous CSIs affected the degree of member commitment to CSI objectives.

Further, a section of interviewees drawn from the EAC revealed that overlapping mandates on one hand caused unhealthy competition amongst states and on the other hand created multiple financial responsibilities leading to fatigue and lack of commitment to the organization's goals. Respondents at the EASF and among CSO interviewees viewed overlapping mandates as responsible for low member states' commitment towards the different regional security arrangements since funding all three to perform the same role was burdensome to most. Further, respondents reported that multiple memberships led to divided loyalties that compromised commitment to mandates of some CSIs at the expense of others. The majority of interviewees in the 3 studied CSIs were in agreement that duplication of roles drains the budgets of the CSIs and leads to reduced commitment and loyalty to respective regional security arrangements. Additionally, member states felt that the CSIs presented multiple objectives and this overstretched their resources.

The findings of this study are in agreement with a study conducted by Rwengabo (2016) which observed that interlocking arrangements hinder the IGAD, EAC, and EASF from attaining their regional stabilization mandates. The study also indicated that overlapping mandates caused by the duplicity of membership into various CSIs and bureaucratic decision-making processes hindered the effective implementation of APSA. The study blamed negative duplication of efforts, poor implementation and harmonization, and under-utilization of scarce resources to the overlapping mandates. This aligns with Byiers (2016) who states that IGAD has been hindered from achieving its peace and security mandate because it had numerous specialized institutions with 15 different

offices spread across member states and posing the challenge of integration of functions. It was evident from the current study that sometimes these specialized institutions sought donor aid independently, a factor that may compromise unity of purpose and voice in seeking a common approach for the IGAD agenda.

These findings imply that Eastern African CSIs operate within a region with multiple regional organizations, overlapping memberships, and commitments resulting in conflict of interests and this could expose them to unhealthy competition in conflict management. Consequently, IGAD, EAC, and EASF may never properly function in the context of an environment of several regional organizations and member countries pursuing varied interests.

**b) Political Commitment**

The study investigated the factor of political commitment of the three CSIs under study. A total of 80.7 % (IGAD), 79.3 % (EAC), and 51.5 % (EASF) of respondents indicated that political commitment is a key factor affecting the success of the CSIs in their pursuit of regional stabilization in the subregion. Further analysis from interviews conducted at IGAD reveals that CSIs represented states whose state interests may supersede the collective interests of a region implying that CSI did not operate independently but were oriented to what the political leadership approved of. CSO interviewees reported that owing to a lack of autonomy and independence, civil servants seconded to serve in various capacities in IGAD affirm their loyalty to their mother countries and not exactly to the CSI agenda.

Respondents noted a lack of political commitment in South Sudan's peace process, with leaders ignoring ceasefire agreements and IGAD member states failing to empower the IGAD secretariat for effective administration. As reported by one CSO informant:

> …even though the Secretariat ought to independently administer the regional body, the IGAD Secretariat has no capacity to implement decisions but relies on direction provided by the Council of Ministers and the Assembly. In such circumstances, political interference from respective states may not be ruled out and as a result, the role of the Secretariat is so downgraded that at times, it does not even attend meetings of the council of ministers… (CSO informant 04, South Sudan, 2021).

CSO informants in South Sudan noted that IGAD member states lack commitment, withholding executive independence from the IGAD secretariat. They highlighted that the IGAD Executive

Secretary is politically appointed, with decision-making power residing with national leaders, rendering the Secretariat largely irrelevant. Strategic level interviewees at the EAC echoed concerns about partner states' lack of political commitment, noting that national sovereignty makes the security sector sensitive. Consequently, states resist collective peace policies that conflict with their interests, often invoking sovereignty to avoid regional interventions. Citing an example, the interviewees indicated that the 2015 Burundi crisis was a result of the failure of the political class to commit to the full adherence and implementation of the Arusha Accord. Additionally, informants drawn from CSOs during an FGD highlighted that the EAC had mechanisms for preventive diplomacy but these policies may not be fully implemented due to existing political differences of opinion between member states. They observed that political dispositions made some EAC members desire or shun alliances.

Tactical-level respondents at the EASF reported that political support deficiencies hinder decision implementation, including troop deployment and funding. They noted suspicion and rivalry among member states, who prioritize national security objectives over EASF goals, thereby limiting peace and security efforts in Eastern Africa. The findings agree with those of Nantulya (2016) who asserts that a lack of strategic political harmony among EAC members led to the failure of the CSI to provide a roadmap to return to constitutional order in Burundi. Members' disunity coupled with a lack of focused dialogue led to states boycotting emergency summits in Burundi. This was a show of lack of political commitment as opined by Elowson and Albuquerque (2017). This view is also supported by Apuuli (2017) who established that the issue of protecting the perceived national interests of every member state also influences the strategies which should contribute to peace and stability in the region. IGAD, EAC and EASF member states make political considerations before acceding to any regional security arrangements and this hurts regional stabilization.

From the foregoing, it can be argued that Governments bypassing regional security organizations hinder their success, as political differences impede strategy and policy formulation for peace and security. IGAD, EAC, and EASF struggle to act independently due to member states' political interests, highlighting the need for unified leadership to strengthen regional peace efforts.

**c) Adequacy of Financial Resources**

Respondents noted that the financial capacity, including availability, reliability, and timely

disbursement of funds, significantly influences the implementation of CSI programs and security initiatives in Eastern Africa. Majority of respondents (87.1 %) were of the opinion that financial challenges hinder IGAD from handling complex security operations with 83.9 % of them stating that IGAD had a huge deficit in its operational budget. Additionally, 67.7% of respondents concurred that IGAD over relies on donor funding which is not only insufficient but granted with conditions.

Further, through interviews, the study established that IGAD runs several programmes grouped into various pillars and that the CSI has to solicit donor funding to bridge the fund deficit, which in itself poses challenges.

An interviewee at the IGAD strategic level asserted:

> …we carry out several programs and I can tell you that, though insufficient, 70 % of the funds are obtained from donors. Member states' annual contributions are inconsistent. Out of 8 member states, 3 do not consistently contribute, that is Somalia, Eritrea and South Sudan. This now explains why 90% of IGAD's programs are supported by donors. However, donors provide funds based on their interests. This affects the sustainability of the peace and security mandate of IGAD… (IGAD strategic level interviewee 008, 2020).

The study, through EAC interviewees, established that the financial situation of the EAC was unstable because partner states had not been remitting their contributions in time and that the Council of Ministers had not invoked legal provisions to push defaulters to pay. In the words of one interviewee at EAC strategic level:

> …the EAC is under financial crisis and the East African Civil Society Organizations Forum through EALA in October 2019 filed a petition recommending the Council of Ministers to consider invoking Article 143 or 146 to impose sanctions against partner states that default on payments because it is tantamount to display of non-commitment to the integration process. EALA also wants the Alternative Financing Mechanism which could include an import levy finalized and effected ... (EAC strategic level interviewee 05, 2020).

These sentiments are indications that EAC cannot fund regional peace initiatives independently due to insufficient donor support. Member states' failure to pay annual contributions makes the EAC budget unsustainable, undermining the CSI's ability to implement its programs.

The issue of financial incapacity was also observed in EASF. A total of 88.2% of respondents viewed EASF member states as unwilling to contribute financially, especially when state interests

are at stake. The same view was also shared by 73.5% of respondents who concurred that EASF funding is mainly from donors. EASF respondents attributed these financial challenges to failure by partner states to honour their financial obligations thereby making the Regional Mechanism seek donor support to implement its regional peace and security initiatives. In addition, EASF respondents acknowledged that while majority of EASF member states were in arrears with their contributions, the CSI lacked modalities of forcing member states to honour payments with donor funds being unsustainable because donors gave funds based on their assessment of what they considered a threat.

The study reveals that IGAD, EAC, and EASF face funding shortages, impacting their regional stabilization efforts. Member states' dependency on donor funding and inadequate contributions compromise the sustainability and ownership of CSI programs.For instance, if member states' assessed contributions cannot fund even half of their annual budgets, ownership of institutional agenda gets compromised. Findings of the current study in regard to financial challenges are in tandem with Badmus (2015) who argues that African regional security organizations are institutionalizing the peace and security arrangements in line with their mandates but have to rely on international partners for funding which compromises ownership of peace and security initiatives.

In contrast, best practices in ECOWAS indicate that the CSI has established a Community Levy. Through this levy, ECOWAS has been able to fund up to 85% of its operational budget. Arthur, (2017) portrays ECOWAS as ahead of the AU in terms of generating resources from member states for its programmes. The EA region has much to learn from other RMs and alliances such as the North Atlantic Treaty Organization (NATO) which operate on the principle of common funding where all 30 members contribute according to an agreed cost-sharing formula, based on their Gross National Income (GNI).

From the analysis of the findings, it is evident that IGAD, EAC and EASF are far from being financially independent. The institutions' programs cannot be effectively and locally financed and thus the over-reliance on donor funds. Findings of this study echo provisions of the social constructivism theory that a security structure operates both on material and social components. Lack of a reliable funding stream also hinders implementation of programmes according to set priorities and needs thereby hindering success of peace activities. This goes against effectiveness

of long-term stabilization of the target states.

The implication are that CSI consider to prioritize programmes that address the socio-economic condition of many African states which makes them vulnerable to donor condition-based interventions because of the loans, aid and foreign assistance to poor African nations. This impacts on sustainability, relevance and ownership of peace and security processes at the regional level.The CSI also need to implement strategies that will drive more effective mobilization of fundsfrom member states for effective running of the CSI peace and security programmes and also adopt policies that employ divisions of financial responsibilities according to the abilities of its members.

**d) The Regional Hegemony Dilemma**

The study investigated respondent's perspectives concerning the member states power and dominance on one hand and pursuit for peace and security initiatives by all three CSIs on the other. From the findings, a total of 67.7% (IGAD), 72.4% (EAC) and 66.2% (EASF) of respondents consider the Eastern Africa subregion as challenged by state dominance issues and this affects the CSIs in their achievement of stabilization. From interviews, it emerged that the Horn of Africa (HoA) did not have a leading power that could drive IGAD peace and security policies single handedly like is the case for South Africa (SADC) and Nigeria (ECOWAS). Acknowledging that the Eastern Africa sub region lacks a visibly distinct hegemon/lead state, IGAD respondents however intimated that Ethiopia appears to portray a pivotal influence on conflict prevention compared to other members. According to informants from the CSO cohort, Ethiopia's lofty position is evidenced by the conglomeration of security related specialized institutions in the country including IGAD which elevates Ethiopia's pivotal state status.

Interviewees at the EAC cited lack of a hegemonic state negatively impacting the CSI mandate delivery. Additionally, majority of interviewees at the strategic level argued that no EAC partner state had the ability to economically, militarily or diplomatically garner full support of all other member states in pursuit of a common peace agenda. Giving an example of the Burundi crisis, one interviewee drawn from strategic level at the EAC observed:

> …during the 2015 Burundi crisis, none of the EAC partner states was able to assert herself in negotiating an acceptable political settlement to the crisis. When negotiations for peace in Burundi began under the EAC auspices, partner states entered into silent alliances based

> on interests with Burundi and Tanzania on one hand while Uganda and Rwanda were on the other with Kenya remaining neutral… (EAC strategic level interviewee, 01, 2020).``

This demonstrates the complex states relations in the Great Lakes Region as earlier alluded to. This political schism has had a huge impact on peace and conflict in the region occasioning a spread of alliances to other African counties such as DRC, Angola and South Africa as witnessed in previous regional conflicts.

The study found that the EASF's stabilization efforts are hampered by the absence of a lead state to champion its agenda. Ethiopia and Kenya, potential candidates due to their military, economic, and diplomatic strength, face internal challenges. Ethiopia contends with Somalia's expansionist threat and poor relations with Eritrea, while Kenya grapples with terrorism and a maritime dispute with Somalia. Additionally, CSO interviewees noted that silent supremacy wars, rivalry, and suspicion among EASF member states undermine institutional cohesion and prompt decision-making during conflicts.

This study findings are in consonance with a study by Adetula *et al.,* (2016) who posits that suspicion and rivalry within IGAD compromises achievement of IGAD's peace and security mandate while Ethiopia is seen as dominating the CSI. For instance, the 2006 intervention by Ethiopia in Somalia to annihilate the ICU militia was a unilateral move yet it was backed by IGAD. This was a non- authorized military intervention and Ethiopia justified its legitimacy on the grounds of its right to individual and collective self- defence against a terrorist threat and as a reply to an invitation from a legitimate government. Somalia took the invasion negatively and in response to IGAD's support for Ethiopian intervention, Eritrea suspended its membership in April 2007.

The dominant posture assumed by Ethiopia in terms of being home to numerous institutions is also noted by El-Fassi and Maru (2015) who write that Ethiopia hosts the AU Headquarters for the Peace and Security Committee and has chaired IGAD since 2008, it has been elected three times as member of the PSC and has influence on the AU organs and representative of AU Member States in Addis Ababa. In addition, Ethiopia hosts a number of IGAD offices and specialized institutions and thus apparently seems better suited to push the IGAD regional mandate.

Bayeh (2015) also identified lack of a regional hegemon, overlapping membership into other RECs

and lack of funding as factors affecting the EASF in pursuit of regional peace. The study findings are in consonance with those of Thobejane and Yitay (2018) who contend that Kenya and Ethiopia stand out as pivotal states to push the regional stabilization agenda but engagement with internal issues including terrorism and border disputes deter their assertiveness. From the above findings, it could therefore be inferred that no single IGAD, EAC or EASF member state has come out to take up political and military accountability for peace and security in the Eastern Africa subregion and this affects prompt decision-making required whenever conflict arises.

**e) Weak Policies**

A total of 66.7 % of respondents reported that IGAD lacks effective and efficient policies to mitigate against regional insecurity. These sentiments were shared by 95.5% and 80.6% of EAC and EASF respondents respectively. Further analysis centred on respondents views on the soundness of defence and security policy of IGAD, EAC and EASF. A total of 69.7 % of respondents (IGAD), 83.4 % (EAC) and 61.7 % (EASF) stated that the respective CSIs did not have a sound defence policy for intervention in regional conflict.

Interviews revealed IGAD prioritizes conflict management over long-term prevention. The existing defense policy is managerial, not preventive. Without a Common Peace and Security Policy, IGAD states respond to threats on an ad hoc basis rather than a unified regional approach.

Study findings revealed that the East African Community (EAC) lacks strong policies for conflict intervention. Despite having an early warning system, defence cooperation, and preventive diplomacy on paper, these systems are weak and non-operational. The EAC lacks a comprehensive defence policy, with the Mutual Defence Pact still unratified by all partner states. Draft policies on illegal drug trafficking, terrorism, refugees, and maritime security exist but face implementation challenges due to resource scarcity. Thus, the study established that the CSI had not operationalized the EAC Peace and Security Protocol. Elucidating challenges related to the implementation of a mutual defence pact, an interviewee at the EAC strategic level had this to say:

> …institutionally, the EAC has different member states (compared to IGAD and EASF) with different structures of addressing peace and security. Basically, therefore, the EAC is a collection entity whose implementation of policies is by bilateral partnership. Implementing a comprehensive defence policy for the EAC could be impeded by the fact that each EAC member state has its own unique security history… (EAC strategic level

interviewee 04, 2020).

Despite the above challenges, progressive efforts bringing together relevant agencies in the military, police and judiciary have been ongoing in the EAC to implement the EAC Mutual Defence Protocol and Mutual Peace and Security Protocol. A number of EAC military exercises, for instance, have been undertaken to improve mutual operability.

Interviewees indicated that the East African Standby Force (EASF) lacks a clear conflict intervention policy, with decisions driven by politics rather than necessity or threats. Implementation of its defence policy is hindered by differing military doctrines and member states' reluctance to delegate sovereign security interests to a supranational body.These findings are in concurrence with a study by Miranyi (2018) who points out the need to harmonize operational structures at the EASF and fast track policy approval by member states to enable joint implementation and to gain from integration, create synergy and enhance the CSI effectiveness, and that for a defence policy to be effective and efficient, it should be geared more towards prevention rather than erratic response to conflict.

The study found that IGAD, EAC, and EASF face implementation challenges due to resource constraints and differing military doctrines. Existing peace and conflict policies focus more on conflict management than prevention. Effective CPMR and peace-building are hindered by the low capacity of CSIs. For sustainable stabilization, CSIs need to build durable capacity and secure political commitment from member states for harmonized policy implementation.

**f) Inadequate Legal Framework**

The study established that 86.9% (IGAD), 86.4% (EAC) and 64 % (EASF) of respondents were of the view that a legal framework to support the respective CSIs in their endeavour to achieve peace and security in the East African subregion existed. However, through indepth key informant interviews, it emerged that the existing legal framework was ineffective and not responsive to the current realities. For instance, interviewees drawn from strategic level staff at IGAD observed that the applicable legal framework did not have a strong requirement to commit member states to the IGAD mandate. This was evident in cases where member states failed to honour obligations to the IGAD kitty and there being no legal provisions, making them pay up was not possible and neither were there any applicable sanctions. The interviewees further reported that IGAD lacked

an effective legal framework guiding the CSI chairmanship and even convening of Summits. Similar sentiments were raised by interviewees drawn from the EAC who affirmed that the CSI lacked a binding legal reference that could enforce membership commitment to the Community's agreements. Key informants indicated that the EAC Protocol on Peace and Security was yet to be institutionalized and its ratification by the member states was slow. They attributed this to sovereignty issues, lack of political commitment from partner states and resource constraints. An interviewee at EAC strategic level further explained:

> …member states have not fully ratified the EAC protocol on peace and security. This is because states may be politically uncomfortable to cede their sovereignty and individual security interests to a joint collective security arrangement. Although the EAC protocol is a good framework, the EAC lacks sufficient financial resources, adequate public participation and enough consensuses from member states for its ratification and hence the failure to operationalize the protocol … (EAC strategic level interviewee, 01, 2020)

Interviews revealed that EASF operates under outdated policies from 2004 and 2005, lacking legal provisions for mandatory contributions or troop deployment. The Agreement on Establishment of EASF (2014), addressing funding and logistics, relies heavily on member states' political goodwill, impacting its effectiveness. Findings in this study echo Byiers (2016) who avers that the lack of a robust legal basis for staff appointments is manifest in the office of the IGAD Executive Secretary which is a political appointment. Noting that CSIs in the subregion have not implemented tangible strategies to mitigate conflicts, Byiers (2016) observes that although frameworks for regional cooperation are in place, regional integration and conflict prevention has been poor. Further, Kidane (2018) argues that ensuring fairness and putting in place working legal frameworks will be pivotal in ensuring successes of RECS.

The study findings are also in agreement with Manyolo (2017) who argues that the East African Protocol on Peace and Security lacked the necessary buy - in from politicians and the public (especially marginalized communities) and the necessary institutional framework for its implementation. Elowson and Lins de Albuquerque (2017) also contends that one of the obstacles to effective EASF's intervention in Burundi conflict was the weak legal framework asserting that the EASF policy framework had been structured on a non-binding MoU and thus, had less legal basis to compel members to contribute to EASF, or to enforce peace and security.

It may thus be argued that the CSIs lack robust legal provisions which can be used to compel member states to commit themselves to regional stabilization initiatives. Equally, there is no strong legal backing that can be invoked by IGAD, EAC and EASF to deploy forces or intervene in conflict without the consent of the host nation and member states. The weak legal frameworks greatly undermine IGAD, EAC and EASF by not committing member states to organizational goals thereby affecting the achievement of their objectives.

**Conclusion**

This study anchored on the question of elusive peace and security in the EA region despite the existing CSIs with direct mandates to establish peace. It provides a situational analysis reflecting the dismal performance of the CSIs focusing on their structural and institutional frameworks. Through the lens of the Regional Security Complex theory, the shortcomings of the three entities are explored and analysed. From the findings of this study, it emerged that achievement of effective conflict resolution in the EA region by IGAD, EAC and EASF was hampered largely by structural and institutional bottlenecks. These include thematic and geographic overlaps, a common feature in IGAD, EAC and EASF resulting into competition over scarce resources, financial over stretchand divided loyalties. A general lack of political commitment on agreed treaties and policies by member states coupled with unclear and non-binding legal frameworks, financial and human resource constraints, over reliance on donor funds, weak logistical capacity, cumbersome bureaucracy as well as heavy political interference and lack of a lead state to provide unity of direction largely hampered implementation of the CSIs policies and subdued regional stabilization programmes. The next section considers emergent policy recommendations and makes some suggestions for future research.

**Policy Recommendations, Caveats and Future Research Initiatives**

In a region characterized by endemic conflict and where close to 50% of the countries rank high on the fragility index heavily impacting negatively on development, there is an urgent need for a structured institutional CSI framework that encompasses multidimensional approaches of diplomacy, security and development to effectively manage security threats and conflicts. In this regard, the ongoing AU efforts to align APSA with RECs should address overlaps through tapping on areas of comparative advantage and specialization. This paper suggests that streamlining of

mandates will be required to achieve an effective peace and security structure. In light of this, the following recommendations are thus proposed:

- To eliminate overlaps in mandate, IGAD should be reconfigured to specialize on peace and conflicts in the Horn of Africa while EAC leverages on its economic integration experience and inter-state cohesion to strengthen member states commitment to mutual peace and security pact and mutual defence agreements. EASF can be advanced as a specialized PSO (Peace Support Operation) tool for peacekeeping and peace enforcement in the sub region.
- The study recommends Kenya adopt a more assertive foreign policy to strengthen IGAD's response to regional threats, emphasizing strong institutionalization, resourcing, and leadership. Kenya's pivotal location positions it to lead and galvanize state cooperation in crises.
- The AU's financial autonomy initiative should be fast-tracked, with EAC, IGAD, and EASF developing local fundraising strategies like ECOWAS. This will boost accountability, reduce donor dependency, and increase autonomy in peace and security agendas. Enhancing legal and political compliance, basing decision-making quorums on paid memberships, and granting veto powers to well-paying members will incentivize adherence to agreements.
- On new research initiatives, comparative studies between the regions' mechanisms and other region's structures will unearth weaknesses and direct efforts to more feasible approaches. For instance, a study between IGAD and ECOWAS could bring to the fore contextual and institutional factors that determine the effectiveness and efficiency of the latter's performance despite its myriad concerns.

**References**

Apuuli, P.K. (2017). *Promoting Security in Africa through Regional Economic Communities (RECs) and the African Union's African Peace and Security Architecture (APSA).* 9 (1), Dalhousie University, Halifax, Nova Scotia, Canada

Arthur, P. (2017). Economic Community of West African States, Regional Security and the Implementation of Humanitarian Intervention and the Responsibility to Protect: Rhetoric or Reality? *Insight on Africa.* SAGE.

Badmus, I.A. (2015). *The African Union's Role in Peacekeeping: Building on Lessons from Security Operations.* Basingtoke: Palgrave Macmillan.

Bayeh, E. (2015). Eastern Africa Standby Force: An Overview, *International Journal of Research (IJR) 2(1).*

Bereketeab, R. (2019). Regional Economic Communities and Peacebuilding: The IGAD experience. *South African Journal of International Affairs, Nordic Africa Institute 26(1), 137-156.*

Byiers, B. (2016). *The Political Economy of Regional Integration in Africa: Synthesis Report.* European Centre for Development Policy Management (ECDPM). Maastricht: ECDPM.

El-Fassi and Maru. M. (2015). The Regional Economic Communities and Implementation of the African Governance Architecture (AGA). *ECDPM Discussion* Paper 181, Maastricht: ECDPM.

Elowson, C., & de Albuquerque, A. L. (2016). Challenges to Peace and Security in Eastern Africa: The Role of IGAD, EAC and EASF. S*tudies in African Security*. Swedish Research Agency, 1-4.

George, D. & Mallery, P. (2003). SPSS for Windows Step by Step: A Simple Guide and Reference. (4th Ed.). Boston: Allyn and Bacon.

Gnanguenon, A. (2020). *African Union RECs Cooperation of variable geometry.* ANU-CRIS.

Hamad, H. (2016). Maritime Security Concerns of the East African Community (EAC)*Western Indian Ocean Journal of Marine Science, Volume 15(2), pp. 75-92.*

Hassan, A. (2018). *The Effectiveness of IGAD in Promoting Regional Diplomacy: A Case Study of the Somalia Peace Process.* 10.13140/RG.2.2.22600.06406.

Kabage, R. (2020). Eastern Africa Standby Force's Efforts In Execution of Its Mandate in Maintaining Peace And Security In Kenya And Somalia. International Journal of Scientific and Research Publications 10 (11):444-453. DOI:10.29322/IJSRP.10.11.2020.p10756.

Khadiagala, G.M. (2018). Europe-African Relations in the Era of Uncertainty. In: Nagar D., Mutasa C. (eds) Africa and the World. Palgrave Macmillan, Cham.

Kothari, C.R. and Garg, G. (2019). *Research Methodology: Methods and Techniques.* New Delhi: New Age International Publishers.

Krejcie, R. V., and Morgan, D.W. (1970). "Determination of Sample Size for Research Activities" *Educational and Psychological Measurement, Vol 30, page 607-610.*

Manyolo, O. O. (2017). *Operationalization of Regional Protocols: The Case of the East African Community Protocol on Peace and Security*; Unpublished Master's Thesis: IDIS, University of Nairobi.

Maru, M.T and El Fassi, S. (2015). Can the Regional Economic Communities Support Implementation of the African Governance Architecture (AGA)? The Case of

Intergovernmental Authority on Development (IGAD). ECDP *Discussion Paper* 181. Maastricht: European Center for Development Policy Management.

Miranyi, W. M. (2018). *An Analysis on the Impact of Regional Integration in Africa: The Case Study of the East African Community* (EAC). University of Nairobi, Unpublished Thesis.

Nantulya, P. (2019). Burundi, the Forgotten Crisis, Still Burns. Retrieved from: *https://africacenter.org/spotlight/burundi-the-forgotten-crisis-still-burns/*

Okon, E. N. (2020). Power and regional security: A comparative discourse on ECOWAS and SADC. *African Social Science and Humanities Journal*, *1*(1), 36-51. https://doi.org/10.57040/asshj.v1i1.15.

Rwengabo, S. (2016). "Institutional Design and the Implementation of the African Peace Security Architecture in Eastern Africa."*Africa Development Vol*. 41, No. 4: 107-38. CODESRIA.

Thobejane, T and Yitay, B (2017). Regional Integration in the Horn of Africa: Some Findings. *European Journal of Social Science Education and Research*. Vol. 4, No. 5, p. 77-88.

UNDP (2022), *Human Development Report 2022,* available at hdr.undp.org, accessed 29 August 2022.

# Influence of Data Analytics on The National Security Strategy Formulation Process in Kenya

***by***

***Kodheck Z achary Makori, Martine Odhiambo Oleche and James Kimuyu***

**Abstract**

This study investigates the application of data analytics techniques in the formulation process of National Security Strategies (NSS) in Kenya, examining its influence and strategies for enhancement. The research is grounded in open systems theory (OST), which conceptualizes the NSS formulation process as a dynamic system interacting with its environment. The study used a descriptive research design to collect primary data through close-ended questionnaires from key stakeholders in Kenya's national security organs and agencies. The data analysis, employing both descriptive and inferential statistics, revealed a significant positive correlation between data analytics and the NSS process. Key findings indicate that despite this positive correlation, the utilization of data analytics is minimal due to limited proficiency among personnel and inadequate formal training. Integrating data analytics into the NSS process enhances environmental scanning, real-time monitoring of security threats, technological advancements, and socio-political dynamics. Challenges identified include a lack of skilled professionals, insufficient data infrastructure, and poor inter-ministerial collaboration. Recommendations to overcome these challenges include government incentives, regulatory clarity, the establishment of Data Analytics Centers of Excellence, investments in modern data infrastructure, comprehensive training initiatives, awareness campaigns, and partnerships with academia and industry. The study concludes that integrating data analytics into Kenya's NSS formulation process is essential for improving the effectiveness and responsiveness of national security strategies to address evolving security challenges. This integration demands adaptive policies, informed decision-making, and a paradigm shift in NSS formulation to leverage data analytics capabilities fully.

***Keywords:*** *Security, strategy, data, analytics, threats*

## Introduction to the Study

The formulation of effective national security strategies has grown increasingly complex in today's

dynamic environment, marked by diverse threats and exponential data growth (Ogundipe, 2024). Policymakers and security agencies must leverage advanced analytical techniques to extract actionable insights from vast datasets. Data analytics has emerged as a powerful tool, processing large volumes of structured and unstructured data to identify patterns, trends, and predictive models that inform decision-making. Integrating data analytics into the National Security Strategy (NSS) formulation presents opportunities and challenges in Kenya. While data analytics can enhance situational awareness, threat detection, and proactive response planning, its adoption requires addressing organizational, technological, and human resource factors.

This study examines the current state of data analytics integration in Kenya's NSS formulation process to identify factors influencing its successful adoption. The hypothesis suggests a significant relationship between variables like data analytics infrastructure, personnel proficiency, techniques, and strategies, and the effectiveness of the NSS process. By exploring these relationships, the study provides insights and recommendations to policymakers and security agencies on enhancing data analytics integration, ultimately contributing to more responsive and informed national security strategies (Hadžić, 2020). The introduction outlines the research context, emphasizing the importance of data analytics in national security strategy formulation and the associated opportunities and challenges while presenting the guiding research hypothesis.

**Background to the Study**

Developing effective National Security Strategies (NSS) is a complex and challenging task, especially in today's dynamic environment with diverse threats and the exponential growth of data from multiple sources (Long & Zhang, 2024). Traditional data collection and analysis methods have led to incomplete and ineffective strategies. However, data analytics has emerged as a powerful tool for processing big data enhancing the collection, collation, and analysis of massive unstructured data. This shift towards data analytics is driven by its ability to scale, operate quickly, handle complexity, and adapt to evolving requirements. Integrating data analytics into the NSS process can be understood through the lens of open system theory (OST), which views the NSS as a dynamic entity engaged in continuous interaction with its environment (Fang et al., 2021). Data analytics techniques, combining statistical techniques, machine learning algorithms, artificial intelligence, and automation, provide a superior alternative to traditional data collection and analysis methods. They extract meaningful information from large datasets, enabling countries to develop data-driven strategies responsive to emerging threats and security challenges. In Kenya,

this study seeks to investigate approaches to enhance the integration of data analytics into the NSS formulation process from an architectural perspective. By focusing on the architectural aspects of this integration, the study aims to identify structural and procedural challenges that hinder effective integration and propose solutions to overcome these challenges.

**Statement of the Problem**

In the era of big data, nation-states face the challenge of formulating responsive strategies informed by real-time, relevant, and contextualized data. This requires comprehensive situational analysis and advanced techniques for collecting, analyzing, and interpreting data to uncover patterns and predict trends. However, Kenya's national security agencies struggle to integrate data analytics effectively into their strategy formulation processes. Traditional methods have produced deficient, ambiguous, and unresponsive strategies inadequate for contemporary security challenges (Hatcheret al., 2022). The massive volume, velocity, variety, and veracity of big data further complicate this integration, as traditional techniques are insufficient. Limited technological infrastructure, a shortage of skilled personnel in data analytics, and inadequate data governance frameworks also hinder progress. Additionally, privacy and ethical concerns, such as potential misuse, bias, and lack of transparency, require careful consideration and robust regulation. Addressing these challenges is crucial for Kenya to develop data-driven, proactive national security strategies to counter evolving threats effectively.

**Study Objective**

This study aims to critically assess the adoption and integration of data analytics techniques in the National Security Strategies (NSS) formulation process in Kenya, aiming to identify strategies and approaches that can enhance their effective utilization. This involves examining the current state of data analytics adoption within Kenya's NSS framework, evaluating its impact on strategic decision-making processes, and proposing recommendations to optimize its use for developing responsive and well-informed security strategies that address evolving threats and challenges.

**Empirical Literature Review**

**Data Analytics and National Security Strategy Formulation Process: Global Perspectives**

The formulation of National Security Strategies (NSS) has traditionally relied on human intelligence and conventional surveillance methods. However, the rise of digital technologies and data analytics has introduced a paradigm shift, enabling the processing of large datasets quickly

and efficiently. This literature review examines the role of data analytics in NSS formulation, focusing on global, regional, East African, and Kenyan contexts.

Globally, data analytics has significantly influenced NSS formulation. The Congressional Research Service (2020) highlights the role of AI in U.S. national security, noting its capabilities in intelligence gathering, cyber operations, and command control. AI facilitates more efficient data analysis, improving target recognition and decision-making capabilities. Similarly, Chi (2017) emphasizes that Australia's adoption of big data analytics has enhanced its national security community's ability to organize and analyze large datasets, identifying potential threats proactively.

In another study, Van Puyvelde et al. (2017) explore how big data influences decision-making processes within U.S. national security. The study found that data analytics technologies, including machine learning, enable national security strategists to detect fraudulent activities and potential threats, creating a more robust NSS. The European Defence Agency (2022) has leveraged AI and data analytics to improve situational awareness and decision-making within the European Union (EU). Integrating these technologies into the NSS formulation process helps address modern threats more effectively.

Countries like Australia and Singapore have made significant strides in the Asia-Pacific region. Australia's Integrated Command and Control (IC2) program utilizes data analytics to enhance national security, while Singapore's Data Science and Artificial Intelligence Program (DSAI) improves situational awareness and decision-making capabilities (Department of Defence, Australia, 2021).

Integrating data analytics into national security strategies is becoming increasingly important in Africa, but it faces significant challenges. South Africa, for instance, has initiated the Data Science for Impact and Decision Enhancement (DSIDE) program to leverage data analytics for national security, disaster management, and policy development (DSIDE, 2022). This program uses data-driven insights to improve decision-making processes and predict potential security threats.

Additionally, Nigeria has started incorporating data analytics to address security challenges such as terrorism and cybercrime. A study by Akinyemi and Siyanbola (2018) discusses using big data analytics to enhance intelligence gathering and threat prediction in Nigeria's fight against Boko

Haram. The study highlights the potential of data analytics to provide timely and actionable intelligence, although infrastructure and expertise remain significant barriers. East Africa has gradually integrated data analytics into national security strategies.

In Kenya, data analytics in NSS formulation is still emerging. Njoroge (2020) argues that rapid technological changes in Kenya have created an environment for evolving national security gaps. Integrating data analytics is necessary to enhance analytical capabilities and extract insights and predictive patterns crucial for responsive NSS. A study by Moses et al. (2018) in Kenya revealed initiatives to integrate data from diverse sources to build a predictive security landscape, focusing on cyberattacks and terrorism. Similarly, Akello (2020) found that AI applications are becoming significant in Kenya, impacting various sectors, including national security.

Wambua (2020) highlighted the need for the Kenyan government to reevaluate the role of social media in NSS formulation due to its rapid growth. The study emphasized the importance of incorporating data analytics to effectively manage social media's implications on national security. A study by Saura et al. (2022) notes that Kenya faces significant challenges in adopting AI and data analytics, such as insufficient regulatory capacity and a lack of STEM courses promoting AI knowledge. This shortage of expertise hampers the successful implementation of AI-driven strategies in national security. Despite these challenges, Kenya is making progress. Moses et al. (2018) report ongoing projects aimed at leveraging data analytics tools to predict and manage security threats. These initiatives reflect a growing recognition of the importance of data analytics in enhancing national security.

**Challenges and Limitations in Data Analytics Adoption**

While data analytics holds promise for enhancing national security strategy formulation, several challenges impede its effective adoption and implementation. Chief among these is ensuring data quality and integrity. Incomplete, inconsistent, or inaccurate data can yield flawed insights and decisions (Van Puyvelde et al., 2019), particularly when integrating data from diverse sources with varying formats and standards. Without robust data governance frameworks and quality assurance mechanisms, the accuracy and reliability of data-driven insights are compromised, undermining the effectiveness of national security strategies.

Effective data analytics hinges on robust infrastructure, encompassing high-performance computing resources, storage capabilities, and advanced software tools. However, many organizations, especially in developing nations, lack the technical infrastructure and expertise to effectively utilise data analytics (Mikalef et al., 2021). This deficiency impedes adoption and implementation of data analytics solutions for national security strategy formulation, resulting in capability disparities between nations and hindering global security efforts. Moreover, successful data analytics initiatives rely on a skilled workforce proficient in advanced analytical techniques, result interpretation, and insight translation into actionable strategies. However, there is a global shortage of data scientists, analysts, and professionals with expertise in data analytics and related fields (Wilson, 2018). Bridging this skill gap through training and education presents a formidable challenge, requiring substantial investments in human resource development and specialized educational programs.

Integrating data analytics into national security raises ethical and legal concerns regarding privacy, civil liberties, and potential data misuse (Bormida, 2021). Organizations must navigate complex regulatory landscapes and develop robust governance frameworks to ensure ethical data use while safeguarding individual rights. Failure to address these concerns risks eroding public trust and legitimacy, leading to legal and reputational consequences.

Moreover, national security operations often require secrecy, yet data analytics, particularly advanced algorithms, can introduce opacity in decision-making (Moses & De Koker, 2018). Striking a balance between secrecy and transparency is crucial for maintaining public trust and accountability while protecting sensitive information.

These challenges highlight the multifaceted nature of data analytics adoption in national security strategy formulation. Addressing them requires a holistic approach involving technological advancements, capacity building, regulatory frameworks, and ethical considerations. Collaborative efforts among nations and stakeholders are crucial to harnessing the full potential of data analytics to enhance global security capabilities.

**Theoretical Model**

The integration of data analytics into the NSS formulation process can be explained through the lens of open systems theory (OST). OST views organizations as dynamic entities constantly

interacting with their environment, exchanging information and resources. The NSS formulation process operates as an open system within a complex environment influenced by security threats and technological advancements. Data analytics is crucial in processing external information, enabling the NSS process to adapt to changing circumstances (Benson, 2024).

The NSS process can improve its ability to collect, process, and analyze data from various sources by employing data analytics techniques. This aligns with OST principles, emphasizing environmental scanning and real-time data analysis for informed decision-making. Integrating data analytics fosters a feedback loop where insights inform strategy refinement, facilitating continuous adaptation and improvement—a core tenet of OST, which views organizations as dynamic systems responding to environmental changes.

## Study Methodology

The study employed a descriptive research design to analyze data analytics integration practices within Kenya's National Security System (NSS) framework (Mutonyi & Sirera, 2020). The target population consisted of stakeholders involved in NSS formulation across ministries and agencies in Kenya, with a sample of 60 participants selected using stratified random sampling. Data were collected through a close-ended questionnaire covering aspects like familiarity with data analytics, training, utilization of techniques, organizational structure, challenges, and strategies for integration. The analysis involved descriptive statistics (frequencies, percentages, means, and standard deviations) and inferential statistics, including regression analysis, to explore relationships between factors and NSS formulation effectiveness.

## Findings of the Study

### Structure of Data Analytics Function in Ministries/Agencies

The study emphasizes the critical role of organizational structure and placement of data analytics functions within ministries and agencies for effective data-driven National Security Strategy (NSS) formulation (Chatterji & Mukkai, 2024). It highlights that 91.6% of respondents place data analytics within IT departments, indicating a heavy reliance on existing IT infrastructures for data initiatives, which suggests recognition of the technical expertise needed for data management and analysis.

However, concerns arise regarding aligning data analytics with the specific needs of NSS formulation. While IT departments possess technical skills, NSS formulation requires understanding geopolitical dynamics and strategic considerations beyond IT functions. The study shows limited dedicated data analytics personnel or units supporting NSS formulation, with only 4.2% reporting part-time staff and an equal proportion integrating data analytics within the NSS unit. This highlights a potential disconnect between technical capabilities and strategic NSS objectives.

The predominant placement of data analytics functions within IT departments raises questions about strategic alignment in national security strategy formulation. While IT expertise is valuable, effective integration of data analytics may require a more interdisciplinary approach, combining technical proficiency with deep domain knowledge and strategic understanding.

Ministries and agencies can address this disconnect by reconsidering their organizational structures and establishing dedicated data analytics teams or units. These specialized units can collaborate closely with NSS formulation teams, translating complex data insights into actionable intelligence tailored to national security strategy development. Additionally, fostering cross-functional collaboration and breaking down silos between IT departments, strategic planning units, and domain experts can facilitate seamless integration of data analytics into NSS formulation processes. By promoting interdisciplinary teamwork and knowledge-sharing, organizations can enhance the effectiveness of data-driven approaches in developing robust national security strategies.

Table 1 summarizes the structure of the data analytics function within Ministries/Agencies, presenting the frequency and percentage distribution across six categories. The findings reveal that many respondents (91.6%) indicated that the IT department's data analytics function is housed, suggesting a predominant reliance on existing IT infrastructures for data analytics initiatives. Additionally, a small percentage of respondents (4.2%) reported having part-time staff dedicated to data analytics, while an equal proportion (4.2%) stated that data analytics is an integral part of the NSS unit.

**Table 1**

*Summary of Data Analytics Function in Ministries/Agencies*

| Variable | Observations | Percent (%) | Cumulative Percent (%) |
|---|---|---|---|
| Fully Pledged Department | 0 | 0 | 0 |
| Has Full-Time Staff | 0 | 0 | 0 |
| Has Part-time Staff | 2 | 4.2 | 4.2 |
| Integrated All Levels | 0 | 0 | 4.2 |
| Integral Part of NSS Unit | 2 | 4.2 | 8.4 |
| Part of the IT Department | 44 | 91.6 | 100.0 |
| **Total** | **48** | **100.0** | |

**Source: Research Data, (2024)**

***Familiarity with Data Analytics***

The study's findings reveal a concerning lack of familiarity with data analytics among the respondents, highlighting a significant knowledge gap that could hinder the effective integration of data-driven approaches into national security strategy formulation processes. Specifically, a substantial 20.8% of respondents reported being "very unfamiliar" with data analytics, while an additional 25% acknowledged unfamiliarity with the subject matter. While a notable 31.3% claimed some level of familiarity and 14.6% indicated being "somewhat familiar," the overall picture suggests that most employees within the National Security Council lack the requisite knowledge, skills, and expertise in data analytics techniques and applications.

**Table 2:** ***Familiarity with Data Analytics***

| *Variable* | *Observations* | *Percent* | *Cumulative Percent* |
|---|---|---|---|
| Very Unfamiliar | 10 | 20.8 | 20.8 |
| Unfamiliar | 12 | 25.0 | 45.8 |
| Somehow | 15 | 31.3 | 77.1 |
| Familiar | 7 | 14.6 | 91.7 |
| Very Familiar | 4 | 8.3 | 100.0 |
| **Total** | **48** | **100.0** | **100.0** |

**Formal Training in Data Analytics**

Table 3 presents the respondents' level of data analytics training, revealing a significant disparity in formal education. The majority (83.3%) lack formal training, while only 12.5% and 4.2% have diploma and degree-level training, respectively. Notably, no respondents possess postgraduate qualifications in data analytics. This substantial gap in structured training among the participants underscores potential barriers to effectively integrating data analytics techniques into the National Security Strategy (NSS) formulation process, as the absence of formal education may hinder the optimal utilization of these critical tools and methodologies.

**Table 3: Level of Data Analytics Training**

| Variable | Observations | Percent | Cumulative Percent |
|---|---|---|---|
| Diploma | 6 | 12.5 | 12.5 |
| Degree | 2 | 4.2 | 16.7 |
| Post graduate | 0 | 0 | 16.7 |
| No Training | 40 | 83.3 | 100.0 |
| **Total** | **48** | **100.0** | **100.0** |

**Source: Research Data, (2024)**

**Utilization of Data Analytics Techniques in NSS Formulation**

The National Security Strategy (NSS) formulation process utilizes diverse data analytics techniques and tools to address the complex challenges of statistical analysis within its framework. Tableau emerges as the most widely employed data visualization tool, while Power BI and Ggplot2 also find significant use. SPSS dominates statistical analysis, accounting for over a third of NSS tasks. Data management and graphics techniques play a vital role, being utilized in more than 37% of NSS activities. SQL proves indispensable for data manipulation and analysis, with machine learning tools like Scikit-Learn and TensorFlow contributing to a substantial portion of NSS tasks. Text analytics and natural language processing tools also find notable applications alongside the prevalent use of cloud platforms such as Amazon AWS, Microsoft Azure, and Google Cloud Platform. This multifaceted toolkit underscores the importance of leveraging diverse and complementary approaches to effectively navigate the intricacies of data analytics within the NSS framework.

**Table 4: Utilization of Data Analytics Techniques in NSS Formulation**

| Data Analytics Techniques | 1 | 2 | 3 | 4 | 5 | Mean | SD |
|---|---|---|---|---|---|---|---|
| **Data Visualization Tools** | | | | | | | |
| Tableau | 55% | 40% | 5% | 0% | 0% | 3.61 | .982 |
| Power BI | 30% | 45% | 10% | 5% | 0% | 3.88 | 1.515 |
| Ggplot2 | 65% | 20% | 10% | 5% | 5% | 3.48 | 1.479 |
| **Statistical Analysis** | | | | | | | |
| SPSS | 10% | 15% | 10% | 45% | 0% | 3.60 | 1.49 |
| Statistical Analysis System (SAS) | 20% | 30% | 27.5% | 35% | 0% | 3.41 | 1.49 |
| Data Management & Graphics | 7.5% | 10% | 35% | 27.5% | 20% | 3.77 | 1.51 |
| **Data Manipulation and Analysis** | | | | | | | |
| Excel | 5% | 5% | 10% | 30% | 50% | 3.49 | 1.49 |
| Structured Query Language | 35% | 20% | 25% | 10% | 10% | 3.92 | 1.52 |
| Apache Spark | 45% | 25% | 15% | 15% | 0% | 3.33 | 1.02 |
| **Machine Learning Tools** | | | | | | | |
| Scikit-Learn | 7.5% | 15% | 22.5% | 35% | 40% | 3.36 | .35 |
| TensorFlow | 10% | 12.5% | 20% | 27.5% | 42.5% | 3.36 | .45 |
| **Text Analytics & Natural Language** | | | | | | | |
| Natural Language Toolkit | 70% | 15% | 10% | 5% | 0% | 3.24 | .56 |
| Text Blob | 60% | 20% | 15% | 5% | 0% | 3.26 | 1.35 |
| **Cloud Platforms** | | | | | | | |
| Amazon AWS | 35% | 25% | 30% | 10% | 0% | 3.40 | 1.41 |
| Microsoft Azure | 65% | 10% | 10% | 15% | 0% | 3.48 | 1.45 |
| Google Cloud Platform | 50% | 20% | 25% | 5% | 0% | 1.37 | 1.20 |
| **Data Pre-Processing** | | | | | | | |
| Open Refine | 65% | 15% | 10% | 15% | 10% | 2.38 | 0.98 |
| Trifacta | 45% | 30% | 15% | 10% | 0% | 2.61 | 1.41 |
| **Web Analytics** | | | | | | | |
| Google Analytics | 50% | 25% | 25% | 0% | 0% | 2.84 | 1.25 |
| Adobe Analytics | 50% | 17.5% | 27.5% | 0% | 0% | 2.61 | .67 |

**Source: Research Data, (2024)**

**Levels of Investment and Challenges Faced in Implementation**

The study reveals varying levels of awareness regarding data analytics among ministries and agencies. While some show moderate to high awareness, indicating a solid understanding, others display low or no awareness, suggesting potential gaps that may require targeted interventions or educational initiatives to improve overall comprehension. Implementation of data analytics faces challenges, including data quality, lack of skilled personnel, privacy/security concerns, constrained budgets, insufficient top management support, and difficulties in data integration. Investment in data analytics varies, with a quarter reporting high investment, a third indicating moderate investment, and over a quarter acknowledging low investment. These findings emphasize the importance of addressing awareness gaps, overcoming implementation challenges, and optimizing investment to utilize data analytics within surveyed entities fully.

**Table 5: Levels of Investment and Challenges Faced in Implementation**

| Aspect | Percentage |
|---|---|
| **Awareness Levels** | |
| Completely Unaware | 12.4% |
| Partially Aware | 27.1% |
| Moderately Aware | 29.1% |
| Very Aware | 21.0% |
| Fully Knowledgeable | 10.4% |
| **Challenges Faced in Implementation** | |
| Data Quality | 60.7% |
| Lack of Skilled Staff | 48.4% |
| Data Privacy and Security | 45.3% |
| **Level of Investment** | |
| High Level | 25.5% |
| Moderate Level | 34.5% |
| Low Level | 28.6% |

**Adoption of Data Analytics in Ministries/Agencies**

The study evaluates the integration of data analytics in governmental bodies' operations and decision-making processes. It reveals a concerning situation, with 22.5% of respondents indicating no adoption of data analytics. The remaining respondents reported either timely or moderate

adoption, with 17.5% indicating excessive adoption and 17.5% indicating fully integrated adoption. The findings highlight the need for improved data analytics integration in national security strategy formulation.

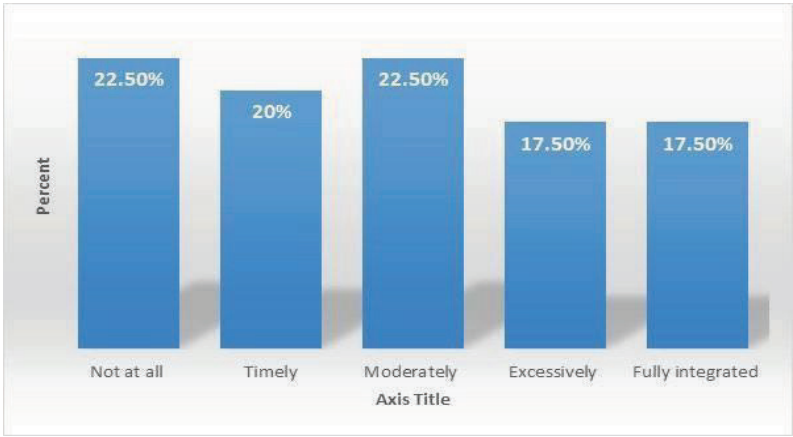


**Figure 1:** *Adoption of Data Analytics in Ministries/Agencies*

**Source: Research Data, (2024)**

**Programs to Enhance Personal Data Analytics Skills**

The study delves into evaluating programs designed to enhance personal data analytics skills within Ministries/Agencies, aiming to shed light on the availability and efficacy of training initiatives to bolster individual competencies in this crucial domain. By analyzing the frequency and distribution of respondents' perceptions regarding these programs, the research seeks to illuminate the organizational endeavours undertaken to cultivate and nurture data analytics capabilities among personnel in formulating national security strategies.

**Figure 2** presents a comprehensive overview of the distribution of programs focused on enhancing personal data analytics skills within Ministries/Agencies, showcasing the frequency and percentage distribution across five distinct categories. The findings reveal that a substantial portion of respondents reported limited (22.5%) or moderate (25%) training initiatives, while an equivalent percentage indicated the presence of extensive training programs.

Furthermore, a smaller proportion of respondents noted the complete absence of training (20.0%), and only 10.0% highlighted the existence of continuous training programs. These results underscore the diverse landscape of efforts to improve data analytics skills among personnel involved in national security strategy formulation, emphasizing the need for more comprehensiveand sustained training initiatives to foster data-driven capabilities within Ministries/Agencies and ensure the effective utilization of data analytics in this critical domain.


**Figure 2:** ***Programs to Enhance Personal Data Analytics Skills***

**Source: Research Data, (2024)**

**NSS Formulation and Data Analytics Integration Enhancement Approaches**

The researcher explores strategies to improve the integration of National Security Strategy (NSS) formulation with data analytics. They identify challenges data analytics faces in the effective formulation process within ministries/agencies. The study ranked various strategies, with the highest perceived effectiveness being the availability of skilled data analytics professionals. The establishment of Data Analytics Centres of Excellence was also effective. However, the training of employees in data analytics was found to be moderately effective.

**Table 6:** *NSS Formulation and Data Analytics Integration*

| Variable/Data Analytics Strategies | 1 | 2 | 3 | 4 | 5 | Mean | SD |
|---|---|---|---|---|---|---|---|
| Incentives for Data Analytics Adoption | 5% | 8% | 17% | 25% | 45% | 3.85 | 1.47 |
| Regulations for Data Sharing and Integration | 7% | 13% | 20% | 27% | 33% | 3.90 | 1.53 |
| Establishment of Data Analytics Centres | 8% | 12% | 18% | 23% | 38% | 4.10 | 1.62 |
| Dev't of Data Infrastructure and Technology | 0% | 15% | 23% | 28% | 23% | 3.75 | 1.49 |
| Skilled Training of employees on Data Analytics | 13% | 17% | 22% | 25% | 23% | 3.55 | 1.48 |
| Awareness Campaigns within Gov't | 12% | 18% | 20% | 22% | 28% | 3.70 | 1.38 |
| Increased Investment in Data Infrastructure | 8% | 13% | 17% | 30% | 32% | 4.00 | 1.61 |
| Collaboration between Industry-Academic | 10% | 15% | 18% | 27% | 30% | 3.80 | 1.56 |
| Availability of Data Analytics Skilled Professionals | 7% | 10% | 15% | 33% | 35% | 4.15 | 1.62 |
| Affordability of Data Analytics Tools/Technologies | 12% | 20% | 25% | 28% | 15% | 3.75 | 1.44 |

Source: Research Data, (2024).

**Regression Analysis**

Regression techniques were used to analyze the relationship between the independent variable (Source of Data, Order of Preference, Data Analytic Techniques, Data Analytic Strategies and Order of Preference) and the dependent variable (Formulation of Effectiveness NSS). The hypothesis guided this section; there is no significant relationship between the independent variables (Data analytics techniques, personnel data analytics proficiency, data analytics aspects, data analytics challenges, data analytics strategies) and the dependent variable (Effective NSS Formulation Process).

**Table 7:** *Model Summary*

| Model | R | R Squared | Adjusted R Squared | Std. Error of Estimate |
|---|---|---|---|---|
| | .764[a] | .757 | .574 | .759 |

**A. Predictors (Constant):** DATA ANALYTICS TECHNIQUES, PERSONNEL DATA ANALYTICS PROFICIENCY, DATA ANALYTICS ASPECTS, DATA ANALYTICS STRATEGIES AND DATA ANALYTICS CHALLENGES

**Source: Research Data, (2024)**

The Model Summary table (Table 8) reveals crucial insights into the regression model's performance regarding the effectiveness of the NSS (National Statistical System) formulation process. With an impressive R-value of 0.764a, signifying a strong positive correlation between the predictors and the dependent variable, the analysis suggests a robust relationship between the included variables such as data analytics infrastructure, personnel data analytics proficiency, techniques, strategies, and aspects, and the effectiveness of NSS formulation.

Moreover, the R Square value of 0.757 indicates that approximately 75.7% of the variability in the effectiveness of the NSS formulation process can be accounted for by the predictors considered in the model. This substantial proportion underscores the significance of the selected predictors in explaining the variance observed in the dependent variable. These findings imply that the chosen regression model provides a compelling framework for understanding and predicting the factors influencing the effectiveness of the NSS formulation process, thus offering valuable insights for enhancing statistical processes and decision-making within the system.

**Table 8:** ***ANOVA[a]***

| Model | Sum of Squares | DF | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Residual | 179.985 | 4 | 44.996 | | |
| Regression | 228.600 | 43 | 6.712 | 14.920 | 0.000 |
| **Total** | 308.585 | 47 | | | |
| **Dependent Variable**: Effectiveness Formulation Process of NSS | | | | | |
| **Predictors (Constant)**: Data Analytics Techniques, Personnel Data Analytics Proficiency, Data Analytics Aspects, Data Analytics Strategies & Data Analytics Challenges. | | | | | |

**Source: Research Data, (2024)**

**Hypothesis Testing**

**Null hypothesis (H0):** There is no significant relationship between the predictors (Data Analytics Infrastructure, Personnel Data Analytics Proficiency, Data Analytics Techniques, Data Analytics Strategies, and Data Analytics Aspects) and the dependent variable (Formulation of Effectiveness NSS).

**Alternative hypothesis (H1):** There is a significant relationship between the predictors (Data Analytics Infrastructure, Personnel Data Analytics Proficiency, Data Analytics Techniques, Data Analytics Strategies, and Data Analytics Aspects) and the dependent variable (Formulation of Effectiveness NSS).

Based on the ANOVA table, the F-statistic is 14.920 with a corresponding significance level (Sig.) of 0.000. Since the significance level (0.000) is less than the conventional threshold of 0.05, we reject the null hypothesis, indicating a statistically significant relationship between the predictors (Data Analytics Infrastructure, Personnel Data Analytics Proficiency, Data Analytics Techniques, Data Analytics Strategies, and Data Analytics Aspects) and the dependent variable (Formulation of Effectiveness NSS). Furthermore, the F-statistic value of 14.920 suggests that the included predictors collectively explain variation in the dependent variable, underscoring their meaningful impact on the formulation of effectiveness within the National Statistical System (NSS).

**Table 9: *Coefficients*[a]**

| Variable Parameter (Aspect) | Coeff (β) | R-Squared | Std. Error | t | p |
|---|---|---|---|---|---|
| Data Analytics Techniques | 1.481 | 0.244 | 0.248 | 5.97 | 0.036 |
| Personnel Data Analytics Proficiency | .859 | 0.403 | 0.243 | 3.53 | 0.048 |
| Data Analytics Aspects | 0.614 | 0.698 | 0.194 | 3.16 | 0.024 |
| Data Analytics Strategies | 1.170 | 0.646 | 0.210 | 5.57 | 0.036 |
| Data Analytics Challenges | -0.497 | 0.854 | 0.205 | -2.42 | 0.027 |
| Constant ($QQQQ_{0000}$) = **1.387**; Number of Observations 48 | | | | | |

**Source: Research Data, (2024)**

The Regression Model presented as: $YYYY = QQQQ_{0000} + QQQQ_{1111}XXXX_{1111} + QQQQ_{2222}XXXX_{2222} + QQQQ_{3333}XXXX_{3333} + QQQQ_{4444}XXXX_{4444} + QQQQ_{5555}XXXX_{5555}$.....(i)

**Y** = 551.979 + 232.546 x **Data Analytics Techniques** + 133.389 x **Personnel Data Analytics Proficiency** + 533.230 x **Data Analytics Aspects** + 544.143 x Data **Analytics Challenges** - 987.079 x **Data Analytics Strategies .....**(ii)

Table 10 displays the unstandardized coefficients (B) alongside their respective significance levels (Sig.), offering crucial insights into the relationships between independent variables and the effectiveness of the NSS (National Statistical System) formulation process.

**Data Analytics Techniques (B = 232.546, Sig. = .008).** The coefficient for Data Analytics Techniques indicates that for every unit increase in the utilization of data analytics techniques, there is an associated increase of 232.546 units in the effectiveness of the NSS formulation process. The significance level of .008 suggests that this relationship is statistically significant at the 0.05 level, emphasizing the importance of incorporating diverse data analytics techniques to enhance NSS formulation.

**Data Analytics Aspects (B = 133.389, Sig. = .002).** The coefficient for Data Analytics Aspects signifies that each unit increase in the consideration of various aspects related to data analytics leads to a corresponding increase of 133.389 units in the effectiveness of NSS formulation. With a significance level of .002, this relationship is statistically significant at 0.05, underscoring the significance of comprehensively addressing different aspects within the NSS formulation process.

**Data Analytics Challenges (B = 533.230, Sig. = .006).** The coefficient for Data Analytics Challenges suggests that for every unit increase in addressing challenges related to data analytics, there is an associated increase of 533.230 units in the effectiveness of NSS formulation. With a significance level of .006, this relationship is statistically significant at 0.05, highlighting the importance of identifying and mitigating challenges to optimize NSS formulation outcomes.

**Data Analytics Strategies (B = 554.143, Sig. = .013).** The coefficient for Data Analytics Strategies indicates that each unit increase in the implementation of strategies related to data analytics results in a corresponding increase of 554.143 units in the effectiveness of NSS formulation. While this relationship is statistically significant at the 0.05 level, as indicated by a significance level of .013, it is essential to note the relatively higher p-value, suggesting a slightly weaker significance level than other variables.

**Personnel Data Analytics Proficiency (B = 551.976, Sig. = .003).** The coefficient for Personnel Data Analytics Proficiency implies that for every unit increase in the proficiency of personnel in data analytics, there is a corresponding increase of 551.976 units in the effectiveness of NSS formulation. This relationship is statistically significant at the 0.05 level, with a significance level of .003, underscoring the importance of personnel expertise in driving effective NSS formulation processes.

**Constant (B = 987-.079, Sig. = .007).** The constant term represents the intercept of the regression equation. In this case, it suggests that when all independent variables are held at zero, the estimated effectiveness of the NSS formulation process is 987-.079. With a significance level of .007, this constant term is statistically significant at 0.05, indicating its relevance in the regression model.

These coefficients and their associated significance levels provide valuable insights into the relative importance and statistical significance of different factors influencing the effectiveness of NSS formulation, guiding policymakers and practitioners in optimizing data analytics practices within the NSS framework.

**Discussion and Summary of the Key Findings**

The current research builds upon previous studies on data analytics adoption in governmental organizations for national security strategy formulation, expanding insights into key challenges like data quality, staffing, and security concerns (Muiga, 2019; Njoroge, 2020). It quantifies the frequency of these obstacles within ministries and agencies, offering specific percentages for a nuanced understanding of implementation challenges. These findings enable policymakers to tailor interventions and allocate resources more effectively to address identified gaps and needs. Regarding awareness levels and investment trends in data analytics, this study confirms prior literature findings of diverse awareness and investment levels across organizational contexts (Maj, 2020; Moses & De Koker, 2018). However, it provides a more detailed analysis of awareness and investment distribution within government organizations. This specificity enables decision-makers to develop targeted strategies that address unique requirements within surveyed ministries and agencies.

On data analytics adoption, the study's findings of mixed adoption levels align with previous research, indicating that while some organizations fully embrace data analytics, others lag due to barriers (Heale & Twycross, 2018; Cabrera-Sánchez & Villarejo-Ramos, 2020). The analysis underscores a significant gap in complete data analytics integration into governmental processes, emphasizing the need for immediate action to bridge this divide.

Furthermore, examining data analytics roles within ministries and agencies resonates with prior research, highlighting the critical role of organizational structure in data analytics adoption (Akello, 2020; Cristea, 2020). By revealing the distribution of data analytics functions across departments and units, the study provides insights into organizational dynamics, identifying areas where structural adjustments and capacity-building initiatives could enhance data analytics integration into national security strategy formulation processes.

**Summary of the Key Findings**

The study reveals that governmental bodies' organizational structure and data analytics capacity are crucial for effective adoption in National Security Strategy (NSS) formulation. Many organizations house data analytics within IT departments, relying on existing infrastructure, but often lack a dedicated department, highlighting potential organizational gaps. There is also a significant knowledge gap among employees, indicating a need for increased training to enhance data analytics proficiency, which is linked to more effective national security strategies.

Most respondents reported a lack of formal data analytics training, showing a gap in utilising these techniques in NSS processes. This underscores the necessity for structured training programs to equip personnel with the necessary skills. The research also shows disparities in adopting various data analytics techniques, suggesting a need for a balanced approach to utilize available tools fully. The regression model indicates that employing diverse techniques is important for effective NSS formulation.

Investment and challenges in implementing data analytics within governmental organizations vary. Key challenges include data quality, lack of skilled staff, privacy concerns, limited budgets, insufficient top management support, and data integration issues. These factors highlight the need for strategic interventions.

The adoption of data analytics varies across ministries and agencies, emphasizing the importance of better integration into government processes for effective NSS formulation. Organizational factors such as structure, culture, and leadership significantly influence the success of data analytics adoption.

The research underscores the integration of data analytics into governmental organizations for NSS formulation. It emphasizes the need to address organizational structure, capacity, and training, promote diverse techniques, and overcome implementation challenges. Regression analysis highlights these factors' significance, offering guidance for policymakers to optimize data analytics and improve decision-making in national security strategy.

Prioritizing initiatives to enhance organizational structures and capacity-building and address challenges is crucial for effective data analytics integration that bolsters national security efforts. The study emphasizes investing in capacity-building initiatives to enhance personnel skills, as proficiency in data analytics correlates with the effectiveness of national security strategies. The survey reveals a significant gap in formal data analytics training among respondents, indicating the underutilization of data analytics techniques in NSS formulation processes.

**Recommendations for Future Research or Practice**

To advance data analytics in National Security Strategy (NSS) formulation, future research should focus on longitudinal studies tracking its adoption within governmental organizations over time. This can reveal trends and the effectiveness of interventions. Comparative studies across different countries or regions can highlight the influence of cultural, political, and socio-economic factors on data analytics adoption and its impact on NSS.

In-depth qualitative research is also needed to explore the factors influencing data analytics adoption. Methods like interviews, focus groups, and case studies can uncover organizational dynamics, challenges, and success factors that quantitative analysis may miss. These insights can provide a more comprehensive understanding of the interplay between organizational culture, structure, and data analytics adoption.

Governmental organizations should invest in robust data analytics infrastructure, including technology, tools, and human resources, to handle large data volumes while ensuring security and privacy. Enhancing personnel proficiency through targeted training programs and continuous learning initiatives is also crucial for fostering a data-driven culture and improving evidence-based decision-making.

Furthermore, greater collaboration between governmental agencies, academic institutions, and industry partners is needed to share best practices and resources. Collaborative initiatives can facilitate knowledge exchange, capacity-building, and the development of innovative solutions, accelerating the adoption and integration of data analytics in NSS formulation.

**References**

Akello, J. (2020). Artificial intelligence: policy brief. Paradigm Initiative.

Biden, J. R. (2021). Interim national security strategic guidance. *The White House*, *8*.

Bormida, M. D. (2021). The big data world: Benefits, threats and ethical challenges. In *Ethical Issues in Covert, Security and Surveillance Research* (pp. 71-91). Emerald Publishing Limited.

Cabrera-Sánchez, J. P., & Villarejo-Ramos, A. F. (2020). Factors affecting the adoption of big data analytics in companies. *Revista de Administração de Empresas*, *59*, 415-429.

Chatterji, T., & Mukkai, A. R. (2024). Driving Urban Digitalisation through a National Mission–a multilevel governance perspective of India's data smart cities strategy. *Asia Pacific Journal of Public Administration*, 1-30.

Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of accounting and management information systems*, *19*(2), 351-378.

Fang, S., Mu, L., & Tu, W. (2021). Heat and mass transfer analysis in a solar water recovery device: experimental and theoretical distillate output study. *Desalination*, *500*, 114881.

Hassani, H., & MacFeely, S. (2023). Driving Excellence in Official Statistics: Unleashing the Potential of Comprehensive Digital Data Governance. *Big Data and Cognitive Computing*, *7*(3), 134.

Hatcher, W. G., Qian, C., Liang, F., Liao, W., Blasch, E. P., & Yu, W. (2022). Secure Iot search engine: survey, challenges issues, case study, and future research direction. *IEEE Internet of Things Journal*, *9*(18), 16807-16823.

Heath, J. B. (2019). The new national security challenge to the economic order. The Yale Law Journal, 1022-1096.

Kuol, L., & Amegboh, J. (2021). Rethinking national security strategies in Africa. *International Relations and Diplomacy*, *9*(01), 1-17.

Long, J., & Zhang, T. (2024). Pillars of Space Traffic Management in the Era of LEO Mega-Constellations: A Global Perspective. *Advances in Space Research*.

Maj, R. (2020). *Assessing National Security Strategies in Combating Terrorism in Africa: Case Study of Kenya* (Doctoral dissertation, University of Nairobi).

Mikalef, P., van de Wetering, R., & Krogstie, J. (2021). Building dynamic capabilities by leveraging big data analytics: The role of organizational inertia. *Information & Management*, *58*(6), 103412.

Moses, L. B., & De Koker, L. (2018). Open secrets: Balancing operational secrecy and transparency in the collection and use of data by national security and law enforcement agencies. *Melbourne University Law Review*, *41*(2), 530-570.

Muiga, J. M. (2019). *The Role of State Inter-Agency Coordination in Countering Terrorism In Africa*. University of Nairobi).

Mutonyi, G. P., & Sirera, M. A. (2020). Evaluating the Effects of Commercialized Security on National Security in Nairobi County, Kenya. *Traektoriâ Nauki= Path of Science*, *6*(5), 2001-2022.

Njoroge, A. W. (2020). *Intelligence aspects of big data analytics for Kenya national security* (Doctoral dissertation, Strathmore University). Electronic Theses Dissertations.

Sarker, I. H. (2021). Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. *SN Computer Science*, *2*(5), 377.

Sayler, K. M. (2019). Artificial intelligence and national security. *Congressional Research Service*, *45178*.

Sjöberg, Daniel. "The European Defence Agency: A Success Story: A Qualitative Analysis On The Integration Efforts b Coyle, S. M. (2021).

# Role Of Public-Private Sector Partnerships In Mitigating Cyber Security Threats In Kenya.

*By*

***Fred Jonyo and Kaudo Philip***

**Abstract**

Increasing espionage, and technology-related crimes such as hacking have made cybersecurity a national priority in government and private sectors. Given the increasing vulnerabilities in cyber security and frequent attacks on both personal information and the realization that data protection and management is a shared responsibility, public-private partnerships in cybersecurity have been considered a viable approach to mitigating cybersecurity threats. This study therefore focused on assessing the role of public-private sector partnerships in mitigating cyber security threats. The study adopted both primary and secondary data in data collection. 15 key informants, purposively sampled will be involved in the study and their findings will be corroborated by the already existing literature that assesses the role of public-private sector partnerships on cybersecurity. The research found that addressing cyber security threats is a collective and shared responsibility that requires the partnership of both the private and public sectors. The study established that critical cyber issues including trust deficits, failure to standardize cyber policies and laws, and privacy concerns among others, continue to hinder public-private partnerships on cybersecurity. The study also found that public-private partnerships present viable opportunities for information sharing, innovation, and the development of effective regulatory frameworks to limit cyber-attacks. The research recommends development of effective and efficient systems of data sharing, cyber security inter-agencies and critical infrastructure protection. Other recommendations include conducting periodic joint audits and assessments, joint pooling of resources, joint training and sensitization on cyber security, establishment of a joint effective incident response and emergency management unit, strengthening frameworks and laws on cyber security and lastly further research is critical for cyber security.

**Key Words:** *Cyber Awareness, Cyber Security, Cyber Threats, Private Sector, Public Sector*.

## Introduction

In the contemporary world which is characterized by internet technology, cybersecurity is

emerging as a major concern. This is prompted by the fact that it has major implications for the state's national security, individual human rights and civil liberties, especially the rights to privacy and confidentiality and international legal frameworks. Globally, states and non-state actors continue to face cyber-security threats in the form of hacking and other forms, which have resulted in serious reputational and economic damages including phishing of critical information. For instance, in 2017, according to the USA Intelligence Community's World Wide Threat Assessment, cyber threats were considered as one of the greatest threats to global security. This has been manifested by the increasing rates of countries and private entities' networks being shut down, trade secrets being stolen, and even invasion of privacy of individuals and families, (US, 2017).

According to the Communication Authority of Kenya report published in October 2023, Kenya had witnessed a total of 860 million cyber security threats in the year 2022-2023 financial year. The report acknowledged that of the 860 million cyber security threats, 79% were a result of cyber criminals exploiting vulnerabilities and flaws in organizations' internal controls, system procedures, and information systems which they relied on to gain unauthorized access to critical organizational and personal information. Noteworthy, malicious software only accounted for 14% of the attacks while Distributed Denial of Services (DDOS) accounted for 6.5% of attacks, and attacks on web applications were also reported. The report noted that there is an increasing trend for cyber-attacks in Kenya, with the country experiencing more than 860 million cyber-attacks annually, against the 7.7 million annual attacks reported six years ago, (CAK, 2017).

In July 2023, Kenya suffered a high-profile cyber-attack that jeopardized the operations of government services including the e-citizen platform, and paralyzed access to more than 5000 government services. The attack was conducted by hackers who identified themselves as "Anonymous Sudan". Whereas the government held the view that no data was lost, the incident paralyzed government operations, (CAK, 2017). Subsequently, in July 2023, Microsoft released a report, notifying that a group of hackers had gained access to organizational email accounts of more than 25 organizations and government agencies.

Given the increasing trends in cyber security attacks, there is heightened focus, exemplified by establishing cyber security strategies and specialized cyber security agencies as mechanisms for mitigating the risks of cyber-security attacks. For instance, the North Atlantic Treaty Organization has already designated cybercrime as an official domain of warfare and warned member states against having vulnerable information system technologies that can be easily hacked. China on the other hand developed a cyber security law that prohibits any form of cyber space attack. The United

States also considered cyber security threats as key national security threats, (US, 2017).

Given the strong agreement that cyber security risk is a "shared risk", there is a growing need for the involvement of private sectors and individuals in managing cyber threats. The private sector is viewed as a critical actor in cyber governance. It becomes very disadantageoue when the private sector isolates itself from this partnership, Etzioni, (2014). As a result of this, most cyber security strategies, developed by governments have largely focused on the private sector. In the United Kingdom and the United States of America, public-private sector partnership has been considered as the cornerstone of cyber-security strategy. The public-private partnership in cyber security is viewed as a strategic approach to ensure inclusivity against fighting all forms of cyber threats.

The government of Kenya, owing to the centrality of cyber security in national security has developed several cybersecurity policies, strategies, and frameworks in an attempt to counter the menace. Based on the fact that the government of Kenya considers the ICT sector a key and instrumental contributor to the achievement of Vision 2030 and envisions transforming Kenya into a digital economy, the government on 5th August 2022 launched the National Cybersecurity Strategy, that draws a practicable roadmap for addressing new challenges and dynamics of cyber security, (NC4, 2022).

Whereas there has been a growing need for the integration of public-private partnerships as a mechanism for addressing cybersecurity challenges, this step has been frustrated by the prevalence of several systemic and technological issues. According to O'Halloran, (2017), limited trust between the government and the private sector on information sharing remains a major issue in public-private partnerships. This is reiterated by the arguments put forth by Tropina and Callanan, (2015), who argued that though cyber security is a shared concern, the state cannot blindly trust private actors to fulfill critical infrastructure protection obligations voluntarily. O'Halloran, (2017) argues that limited trust between the public and the private sector on cyber security issues has degenerated into information-sharing issues. The other critical issue that impedes effective cybersecurity collaboration is the question about obligations regarding the exposure and disclosure of important cyber information that can facilitate the identification of threats and vulnerabilities of the cyber system. This is exemplified by the fact that many organizations are reluctant to share their security vulnerabilities for fear of facing civil litigation and regulatory scrutiny. For instance, most private entities are quite reluctant to partner or contact the public sector for help in addressing a cybersecurity threat, for fear of reprisals including information leaking to the general public. Furthermore, regulatory gaps also impede the development of public-private partnerships.

As O'Halloran, (2017) observes that cyber security is an international threat whose effect is felt both locally and internationally. The researcher argued that across the globe, one of the systemic issues lies in the fact there exists diverse differences in law and policies that guide cyber security across borders. These differences in law and policy are manifested in the differences in the capacities, roles, and reach of governments on cybersecurity, legal and policy limits on self-help by organizations, laws governing how evidence on cyber threats are to be gathered and used, parameters and perceptions of privacy among other issues. These critical systemic issues on policies and laws continue to impact how the private sector and the public sector should respond both unilaterally and collaboratively to cyber threats. This is necessitated by the fact that there is a significant lack of clarity regarding the legal and policy parameters of public-private cooperation, which frustrates the mitigation of cyber threats across borders.

Subsequently, the conflicting laws and policies on cybersecurity across borders, continue to hinder cross-border data transfer activities, aimed at investigating or assessing the vulnerabilities of diverse systems. The jurisdictional scope of the different data privacy laws and the consequences that private companies are likely to face if they breach the privacy obligations have also limited public-private cooperation in so far as cyber security is concerned. As Carr (2016) observed, there exists a serious disjuncture of expectations from both the private sector and public sector on cyber security. For instance, whereas the public sector (government) regards the private sector as a key actor in cybersecurity, the government remains reluctant to grant the private sector the mandate to oversee network security. Conversely, the private sector is not willing or inclined to accept liability for national cyber security or even share their system vulnerabilities with the public sector.

Given the emergence of technological and systemic issues on cybersecurity partnerships including limited trust among cyber security actors, differing interpretations of cyber security laws and privacy rights among different states and organizations, lack of clarity on the parameters of public-private cooperation, and the issues of exposure and disclosure among others, this study aims to fill this research gap, by assessing the critical role of public-private partnerships, putting into considerations the critical issues that hinder public-private partnerships.

Noteworthy, despite the growing government commitment to prioritize cyber security, including developing partnerships with the private sector and individuals, cyber security attacks and risks remain pertinent. As a result, there is a critical need to outline the role of public-private sector partnerships in cyber security and highlight some of the gaps that need to be mitigated to limit cyber threats.

**Purpose and Objective of the Study**

The focus of this study is to assess the role of public-private sector partnerships in mitigating cyber security threats. The study is therefore guided by this research question; what is the role of public-private sector partnerships in addressing cyber security threats?

**Literature Review**

According to Carr (2016), cyber-security is a multifaceted concept that refers to the integrity of individuals' personal privacy online, electronic commerce, security of critical information infrastructure, military threats and the protection of intellectual property. Cybersecurity therefore is protection against any unauthorized access to critical information of individuals and entities. Carr (2016), the state has largely been viewed as the main actor in the provision of national security including the protection of cyberspace and national borders. However, new dynamics in security, including the rise of global terrorism, cybercrime, and transnational crime among others have necessitated the involvement of the private sector as a co-actor of the state in handling cyber threats. Therefore, the partnership of the public-private entities on crime has been propelled by the assumption that mitigating cyber threats requires a collective responsibility and a shared mission. This collaboration should focus on information sharing and expertise sharing, aimed at managing cyber-related threats including cyberbullying and hacking.

Public-private partnerships have several benefits for both the public and private sectors. For instance, both parties benefit from sharing expertise, resources, knowledge, and best practices to make cyberspace much safer and resilient and to enhance customer satisfaction in the use of information infrastructure. According to Carr (2016), the public sector is most likely to benefit from the resources of the private sector like in technology and innovation. On the other hand, the private sector could also gain from public sector in financial budgets and also aid in developing national legislation including policies, strategies, and laws that are geared towards cyber security.

Van and Easton, (2021), public-private partnership fosters innovation and knowledge creation, which is key to finding solutions to network or system vulnerabilities that necessitate cyber threats. Their study also noted that the partnership between the public and the private sector involves closer relationships and interactions, manifested in the form of information sharing and knowledge sharing aimed at mitigating the gaps that expose systems to cyber attacks. This will be very critical

in addressing the trust and confidence deficit, which stands out as a major challenge in cyber security, especially between the public and the private actors. Their findings corroborated the results of Carr, (2016).

Cyber forensics in smart cities require partnerships with both the private sector and the public sector, (Rao & Thatikonda, 2023). The resaerchers concluded their study by summaring the role of public-private sector partnerships so as to provide opportunities and platforms for sharing resources, knowledge, and expertise and complement the capacities of both the private and the public sectors. Further, they argued that the public-private partnership can result in the development of workable and agreeable regulatory frameworks that guide cyber security processes and also foster the building of public trust that is necessary for effective cyber forensics, (Rao & Thatikonda, 2023).

Juma, Arman and Hidayat, (2023), noted that public-private sector partnerships are very critical for fostering cyber security culture that encourages every actor to prioritize cyber security and also developing information-sharing channels on cyber threats. The researchers also noted that in cyber security, governments are the main protectors and regulators of cyber systems. As a result, collaboration between the public sector and the private sector is of essence because it helps fill the gaps including resource gaps, enforcement hurdles, and expertise challenges among others, that the public sector faces, (Juma, Arman & Hidayat, 2023).

**Methodology**

The study adopts mixed research methodologies including the use of questionnaires and interview guides. This integrates 15 purposively sampled respondents and analysis of documents that explore the discussion on public-private partnerships. The secondary data is collaborated with primary data which is obtained through in-depth interviews with cybersecurity. The respondents were drawn from both public and private sectors, while cognizance of the emerging issues on cybersecurity shared their expert knowledge on the opportunities for public-private partnerships in cybersecurity. The measurable variables involved were; information sharing, innovation, sensitization, and awareness creation, data sharing and development of cyber security regimes.

All the secondary data obtained for this study were analyzed thematically, which involved the extraction of key themes from the respondent's interview transcripts as well as secondary sources.

To conform with ethical standards, the respondents are anonymized while the secondary data were cited and referenced.

**Findings**

The Computer Emergency Response Team (CERT) acknowledges that addressing cyber security threats requires collaboration from all internet users and actors. This is informed by the fact that whereas governments have the primary mandate of controlling and mitigating national security risks including cyber threats, they usually do not have the direct authority and rights to control privately owned critical infrastructure and assets hence the urgent need for private involvement.

According to the CERT, the major goals of public-private partnerships in cybersecurity include information sharing between public and private entities as well as supporting national cybersecurity strategies, laws, and policies to ensure cyberspace safety. Subsequently, public-private partnerships also present diverse benefits to private organizations. This can be evidenced form the findings; "Collaboration between the private sector and the public sector on cyber security grants the private organizations an opportunity to be actively involved in crafting solutions and strategies aimed at addressing cyber security threats. In fact, the collaboration warrants the private sector more opportunities to gain additional knowledge on how to mitigate vulnerabilities and threats to cybersecurity".

Furthermore, some of the private sector representatives have held the view that cyber security regulations, which would be products of public-private partnerships are most likely to impose substantial costs that may reduce the profitability of the private sector. A private business will have to incur high costs in installing information infrastructures which are critical for cyber safety. Moreover, the private sector also assumes that partnership with other stakeholders including government agencies on cyber security would result in increased information sharing which may lead to the confidentiality and privacy of private business entities' data and information being compromised.

Despite this growing reluctance of the private sector to partner effectively with government agencies, governments have instituted policies, strategies and laws that provide mandatory requirements that private entities must comply with to preserve that state's cyber security. This is because public-private partnership in cyber security is considered very critical for purposes of

facilitating communication between the public sector and the private sector and also supporting national cyber security strategies.

**Information Sharing as a Role in Public - Private Partnerships**

Respondents acknowledged that one of the critical mandates of the private sector as far as cyber security is concerned is information sharing. Carr, (2016), the provision of actionable and timely cyber threat and alert information is a major expectation of the partnership between the private sector and public sector in cyber security. This implies that the private sectors have a role to communicate to the government and other cybersecurity stakeholders about their system vulnerabilities so that efficient actions can be undertaken by relevant parties. In this study, it was noted that in order for mutual collaboration between the private sector and the public sector in communication to exist, both parties must develop mutual trust among themselves. Subsequently, there is a need for the government and the private sector to mutually agree on the communication methods to be integrated, channels, rules of communication, and the specific agencies or entities that shall store the information and how the sensitive information shall be utilized.

This was informed by the fact that the private sector is less likely to share critical cyber security information with the public or government if there was no well-established trust among the parties. The private sector expects that upon sharing with the government critical information on their cyberspace, especially on their system vulnerabilities, no breach of their confidentiality and integrity rights would be violated, (Christensen, & Petersen, 2017).

According to Carr, (2016), there exist several barriers that limit the private sector's ability and willingness to perform their role of willingly sharing critical information with the government on cyber security. Firstly, the respondents noted that in most instances, it is not easy to immediately establish the nature of a cyber-attack and whether or not it is sustainable at the organizational level or whether it is a large-scale sustainable attack that needs expert intervention from the government agencies. This was noted in the study as the private sector is usually reluctant to share cyber security information and even cyber security best practices for fear that if it shares information with the government or other concerned parties about an attack, the information may be leaked to its competitors and this may jeopardize its operations.

According to the findings of the study, it was highlighted that the public sector should also share critical cyber-related information with the private sector. The public sector is obliged to share relevant information on unforeseeable vulnerabilities or cyber risks with the private sector so that the private sector can put in place action plans to address such gaps. Subsequently, the public sector can share with the private sector best practices that if implemented can result in the protection of the private sector cyberspace. This came out from the study as; private sector companies can share critical cyber threats and intelligence cyber information with the public sector and vice versa. This is very crucial for purposes of in-depth understanding of cyber-related threats and the development of efficient and effective strategies to mitigate the risks. Subsequently, when the public sector conducts audits and assessments periodically on their systems and those of the private sector, they should willingly share the results of the assessments with relevant agencies so that best practices of cyber security can be developed.

Noteworthy, the public sector has also remained reluctant to share very critical cyber security information with the private sector due to the sensitivity of such information. The government has remained reluctant to share sensitive information with the private sector. Therefore, the lack of trust and goodwill by both the private sector and the public sector continues to frustrate efforts to establish a synergy of communication between the private sector and the public sector on cyber security.

**Innovation as Role in Public- Private Partnerships**

Public-private sector partnership remains very critical in cyber security because the collaboration between the private sector, public sector and other agencies. This presents better opportunities for the private sector to offer innovation, agility and specialized knowledge in addressing cyber security threats, (Cavelty & Egloff, 2019). The private sector remains a very critical force for the technological development of cyber security systems. They have continued to play key roles in developing and even investing in key technologies including robotics, artificial intelligence and quantum computing among others.

Therefore, through public-private partnerships, both the private and the public sector enjoy the leverage to share their expert opinions and knowledge on the dynamics of cyber threats which may be very critical for developing new approaches and mechanisms of addressing cyber threats, (Cavelty & Egloff, 2019). This was well captured by the study findings; " the private sector has

the resources and expertise to develop innovative cyber-related solutions that can be relied upon to mitigate the risks of online cyber-related attacks as well as other forms of cyber-crime. Collaborative research between the public sector and the private sector and other agencies can therefore aid in accelerating the pace of innovation and bringing new approaches and ideas in managing cyber threats".

Also, the study acknowledged that the innovative role of the private sector in cyber security has remained constrained by a variety of factors. Firstly, most private organizations lack adequate resources and personnel to conduct adequate research that can result in the generation of new ideas and knowledge in the war against cybercrime. Innovation requires lots of commitment to time, resources, and personnel, which some of the private entities may not be able to sustain. Subsequently, the private sector has been reluctant to share their innovative ideas with the public sector and other agencies, due to a lack of trust in the private sector especially in maintaining their copyrights, using the innovative ideas responsibly including respect for the confidentiality and privacy of the private sector.

**5.3 Public-Private Partnership as a Tool for Cyber Awareness and Education**

Cyber awareness and sensitization stand out as the key issues in enhancing cyberspace. This is because a clear understanding of cyber risks and threats enables individuals to identify cyber vulnerabilities detect risks and thereafter institute necessary strategies to prevent the occurrence of such risks. The study found out that cyber awareness by both employees and the general public reduces the risk of cyber-attacks by limiting the occurrence of data breaches, phishing attempts, and malware infections among others. This was informed by the fact that cyber sensitization provides the stakeholders with adequate skills and knowledge on how they can protect and secure their data, in the contemporary society characterized by cyber-attacks. The sensitization programs also widen the understanding of stakeholders on cyber regulations and laws, hence the likelihood of mitigating cyber threats and risks.

The private sector has the critical mandate of provision of leadership in educating and sensitizing technology stakeholders including the general public and government agencies on cyber security. They could achieve this mandate by partnering with the government to organize training programs aimed at widening understanding of cyber vulnerabilities, risks, threats, and best practices of cyber security. The private sector and the public sector through the Ministry of Information,

Communication and Digital Economy. There is also need to collaborate with multiple stakeholders to discuss cyber threat management in the evolving landscape.

Some of the most important stakeholders in cyber security include technology companies such as Huawei Technologies, Microsoft, Oracle Technologies, Safaricom, Cisco System and Oracle among others. These training programs are equally important because they can also generate innovative ideas to counter the threat of cybercrime. This is well highlighted by the study's finding that the private sector has a mandate to support the government in closing the cyber security skill gap by providing expertise and training to government entities through the provision of critical expertise and also sharing their research findings on cyber security. The awareness and education programs will strengthen the competence level of individuals on cyber security, hence resulting in the adoption of cyber security best practices. Ideally, training programs help organizations improve their situational awareness and make very effective and efficient decisions on their data and systems.

Both the private and the public sectors can offer joint training aimed at bolstering the capacity of the stakeholders on cyber security. The joint training manuals should focus on cyber threat detection, response mechanisms, and strategies to reduce cyber-related vulnerabilities. This is key to the development of cyber defense postures. Joint training on cyber security is ideal as it fosters sharing resources for supporting cyber-related sensitization and education programs. The private sector collaborations in the form of joint training should also focus on highlighting the roles and responsibilities of every stakeholder in cybersecurity and an enhanced understanding of the major regulations and laws that guide cybersecurity.

Some of the challenges that limit private entities' abilities to perform their roles of training and sensitization of the general public on cybersecurity. This assertion is backed by the study's finding which states that,"public awareness and sensitization on cyber security demands commitments to personnel, time, infrastructure and even money, which may be out of reach by most of the private businesses. Subsequently, the private sector may also lack comprehensive training manuals or curriculum to complement their training programs.

In an attempt to address these limitations, private partnerships and collaborations with government agencies result in the development of joint training, which implies shared costs of the training and

sensitization. Through partnerships, the public and private sectors may use mass media platforms and social media platforms to sensitize the public on best practices of cyber security.

**Collaboration in Developing Norms and Regulations Guiding Cybersecurity**

The private and public sectors stand out as the key actors in cyberspace. This is because of the stake they have in the cybespace. Both the private and public sectors therefore have a collective mandate to actively involve themselves in the processes of crafting solutions and mechanisms that concern addressing or mitigating cyber threats, (Juma, Arman & Hidayat, 2023). The private sector and the public sector should therefore provide input and suggestions on the processes of developing national cybersecurity strategies. This is backed up by the study's finding that, "both the private and the public sector should collaborate on cyber security policies and regulations development to facilitate the development of very effective cybersecurity measures that align well with existing legal frameworks".

Ideally, the private sector should actively support the implementation of Kenya's National Cybersecurity Strategy, (NC4, 2022). This will be achieved by not only implementing its provisions but also providing necessary feedback that can aid in ensuring that the strategy aligns well with contemporary cyber security dynamics. The private sector is expected to write policy briefs and proposals that present alternative approaches to addressing the growing cyber security risks in the country. For instance, the media as a private sector entity can support the development and implementation of cyber security policies and frameworks including Kenya's Data Protection Act by providing a viable platform for sensitizing and educating the general public on their cyberrights and best practices to ensure they don't fall victims of cyber-attacks. Furthermore, the media isentitled to share policy briefs and proposals to develop cybersecurity strategies and legislation.

Noteworthy, public-private partnerships are also critical for purposes of standardization of policies and processes that guide cyber security. This is informed by the fact that collaboration of all the key actors of cyber security fosters harmonization of cyber security goals, objectives, interests, and sharing of experiences. This results in the formulation of cyber security best practices, (Juma, Arman & Hidayat, 2023). This is achievable given that the private sector is usually constituted of technical expertise whose inputs can be critical to the development of very effective and efficient cybersecurity frameworks.

The private sector in partnership with other stakeholders can periodically conduct system audits to confirm the suitability and efficiency of existing cyber security procedures and strategies and suggest areas that need improvement to deter system attacks. This is in consistent with the study's which states that when it comes to cyber security, the goal is not only compliance with laws and regulations but also guarding business, individuals and government actors against the dangers of persistent cyber-attacks or threats. The private sector can assist the government in developing counter-cyber security strategies by offering their expert opinions and suggestions during policy reviews and even formulation processes. They can also support counter-cyber security frameworks by being policy advocates, involving sponsoring, organizing and funding cyber security sensitization programs.

The private sector is not only subject to internal cyber security regulations but also to national regulations on cyber security. In an attempt to limit, cyber-related vulnerabilities, there is need for both the private and public sectors to enhance compliance with existing laws to guard their systems from cyber-attacks. This should involve strengthening cyber infrastructures which encompasses integrating information systems with firewalls, passwords and other security measures. For instance, both the private sector and public sectors were obliged to adhere to the provisions of the Computer Misuse and Cyber Crime Act No. 5 of 2018. The act is supported by the Data Protection Act No. 24 of 2019 which provides the necessary guidelines that must be adhered to by all the stakeholders including the private sector for data management, so that important information of organizations do not get into the hands of third parties.

**Resource Mobilization**

Integrating necessary critical infrastructure for detecting and preventing cyber-attacks demands lots of resources that the public sector and other agencies may not possess. The private sector being a profit-making entity is obliged to be a force in the process of mobilizing resources aimed at facilitating cyber security programs including sensitization, and adoption of modern technologies that detect and deter the occurrence of cyber-attacks. The private sector therefore can play the financial and personnel gap, that exists in developing sustainable systems that deter cyber-attacks. As one of the study's findings points out, "cyber threat deterrence is a shared responsibility. The private sector is expected to be at the forefront of supporting research programs and other programs that focus on establishing a cyber-friendly environment. With closer partnership and collaboration

with the public sector, both sectors can gain grants aimed at supporting their initiatives in cyber security. Therefore, the public-private partnership is a strategic approach towards pooling of resources".

Public-private sector partnership is critical for purposes of sharing threat intelligence for purposes of neutralizing cyber threats. For instance, a responsible private sector is expected to share anonymous cyber behaviors with other parties including the public sector for proper cyber action. This can be seen in one of the study's findings, "To combat cyber threats, cyber security actors must combine efforts because cyber threats involve shared risks. The collaboration and partnership are critical for developing in-depth knowledge and understanding of the threat landscape including cyber trends and their evolving nature. Subsequently, the private partnership is also supportive of establishing a stronger and coordinated workforce that is focused on fighting cyber-attacks. In fact, partnerships are significant for sharing experiences on cyber threats and this may be central in the development of cyber policies, strategies, and laws".

**Conclusion**

The study established that trust and information sharing issues, disclosure and exposure risks, differences in cyber security laws and policies and privacy rights are among the main issues that hinder public-private partnerships. It also found out that public-private partnerships are very critical because they help ing mitigating cyber security issues and fill in the gaps that hinder the war on cyber security. The study highlighted that public-private partnerships foster information or data sharing on cyber security and innovations. This facilitates the development of effective regulatory frameworks that guide cyber security. Subsequently, public-private partnership is a key strategy to fill in the resource gaps on cyber security given that it enables resource sharing between the public and the private sector in so far as mitigating cyber threats is concerned. Therefore, the partnership is very critical for resource mobilization. The study also established that public-private partnership is a key incentive for cyber security sensitization and education, a key step towards minimizing cyber vulnerabilities. Thus the study concludes by reiterating that addressing cyber security threats is a shared responsibility of all actors of cyber security. The actors drawn from both the private and the public sectors should develop common visions, missions, strategies, frameworks, processes and procedures for mitigating cyber security threats.

**Recommendations**

- **Development of effective and efficient systems of data sharing**

  The private and public actors should promptly share information and intelligence on cyber threats to the public sector and vice versa. This will enhance effective cyber security actions can be undertaken and defensive strategies adopted to prevent the occurrence of similar cyber security risks.

- **Developing effective cyber security inter-agencies**

  The agency should have its membership drawn from both the private and public sectors. The body should be mandated and tasked to develop a synergized operation between the private and the public sectors

- **Conducting Periodic Joint Audits and Assessments**

  Audits and assessments are critical to detecting cyber threats and vulnerabilities. This informs the development of defensive strategies and mechanisms that will be relied upon to prevent cyber-attacks in future. The audits and assessments can be jointly conducted and should involve all the stakeholders of cyber security including but not limited to public sector and private sectors. These audits and assessments should be conducted bi-annually. Organizations should also develop internal mechanisms for conducting audits and assessments frequently.

- **Joint pooling of resources**

  Cyber security is a shared responsibility. Public-private partnerships provide the best platforms for accessing more resources, personnel and experiences that are very critical for running cyber security programs and agendas and countering cyber security threats and vulnerabilities.

- **Critical Infrastructure Protection**

  Organizations must develop internal mechanisms for monitoring and evaluation of cyber systems to ensure that the systems are protected against any form of cyber attack or compromise.

- **Joint Training and Sensitization on Cyber Security**

  The Private sector needs to lead in efforts to mitigate cyber threats by organizing training and sensitization programs. These activities should target all the users of technology. During the training, the participants should be taught some of the risk factors of cyber-

attacks and prevention strategies that individuals and organizations can put in place to prevent any form of cyber-attack.

- **Strengthening Frameworks and Laws on Cyber Security**
  There is a need to enhance the implementation and compliance of cyber security laws and regulations including the Cybers Security Acts among others.
- **Establishing a joint effective Incident Response and Emergency Management Unit**
  This unit will be of importance especially in coordinating cyber security incident responses and designing emergency management plans.
- **Further Reasearch**
  The resaerchers, scholars and academicians should conduct further research so as to find out other roles other than the ones which have been mentioned in this study. This is so as the body of knowledge requires to have more information and knowledge concerning this particular field.

**References**

CAK, (2017). Communications Authority of Kenya, 2017.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Cavelty, M. D. and Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, *15*(1), 37-57.

Christensen, K. K. and Petersen, K. L. (2017). Public-private partnerships on cyber security: a practice of loyalty. *International Affairs*, *93*(6), 1435-1452.

Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *Georgetown Journal of International Affairs*, 69-78. https://www.jstor.org/stable/43773650

Juma, A. H., Arman, A. A., & Hidayat, F. (2023, September). Cybersecurity Assessment Framework: A Systematic Review. In *2023 10th International Conference on ICT for Smart Society (ICISS)* (pp. 1-6). IEEE.

NC4, (2022). National Cybersecurity Strategy 2022-2027, 2022.

O'Halloran, J. (2017). *Challenges of Public-Private Partnerships in Cybersecurity* (Doctoral dissertation, Utica College).

Rao Jangili Srinivasa and Thatikonda Anvesh, (2023). "The Role of Cyber Forensics in Addressing Cyber security Challenges in Smart Cities" *Journal of Science and Technology,* Vol. 08, Issue 10, Oct 2023, 1-10.

Tropina, T. and Callanan, C. (2015). Public-private collaboration: Cybercrime, cybersecurity, and national security. *Self-and co-regulation in Cybercrime, cybersecurity and national security*, 1-41.

US, (2017). Statement for The Record Worldwide Threat Assessment of The US Intelligence Community; May 23, 2017.

Van Goethem, E. and Easton, M. (2021). Public-Private Partnerships for Information Sharing in the Security Sector: What's in It for Me? *Information & Security*, *48*, 1-15.

# Enhancing Cyber Resilience through Adaptive Security Policies

**by**

**Thuranira Mark Linturi, and Chemosit Nick William**

**Abstract**

Rapid advancements in technology have led to increased cyber incidents and data breaches. This has made cyber resilience a crucial aspect of a comprehensive cybersecurity framework. Kenya has also seen a surge in cyberattacks targeting critical infrastructure and important government services. This underscores the need for a cybersecurity resilience framework based on adaptive security principles. The Directorate of Immigration and Citizen Services is crucial in providing efficient services and setting cybersecurity standards for all government agencies. This study investigates how adaptive security policies bolster cyber resilience within the Directorate of Immigration Services in Kenya while scrutinising the impact of organisational culture on both technical and non-technical aspects of cybersecurity resilience. The research design used a mixed-methods approach, including a systematic literature review and interviews with 73 cybersecurity professionals, system administrators, network engineers, and non-technical staff from the Directorate. Data collection methods included questionnaires, interviews, and forensic examination of past cyber incidents. Quantitative data was analysed using SPSS, while qualitative data underwent thematic analysis. The study reveals that the Directorate of Immigration Services uses advanced technologies and methods to address cyber threats. However, challenges remain in identifying, addressing, and recovering from these incidents. Organisational culture is vital in promoting cybersecurity awareness and practices among employees. To enhance cyber resilience in the Directorate of Immigration Services and throughout Kenya, a comprehensive strategy is needed. This strategy should include promoting awareness, providing targeted training, reviewing policies, and implementing cutting-edge technologies. The research also suggests developing a national cyber resilience framework, adopting an adaptive security approach, fostering a security- first culture, prioritising cyber resilience training, implementing a comprehensive risk management framework, and establishing standardised incident reporting and response mechanisms to ensure cybersecurity resilience in Kenya.

**Keywords:** *security, policies, cyber-resilience, immigration, cyber threats,*

**Introduction**

The Directorate of Immigration Services in Kenya plays a vital role in border security, immigrationmanagement, and safeguarding citizen data. However, its significance extends beyond these functions, as any breach in its cybersecurity could lead to severe consequences, including unauthorised access to sensitive information, identity theft, and national security risks. Additionally, as the overseer of theeCitizen platform, it serves as a critical gateway for citizens to access government services online,making it a prime target for cyberattacks. Thus, securing the Directorate is essential for ensuring smooth service delivery, setting cybersecurity standards across government agencies, and fostering a culture ofawareness and preparedness.

The rising prevalence of cyber threats in Kenya's public institutions, accelerated by rapid digitaltechnology adoption post-COVID-19, highlights the urgent need for enhanced cybersecurity measures (World Economic Forum's Global Risks Report, 2024). In 2023, the cybersecurity sector surpassed global tech growth rates, signalling significant innovation alongside escalating risks (Kabui & Omondi, 2023). This trend was exemplified when cyber incidents in July 2023 disrupted over 5,000 government services for 48 hours, impacting Kenya's digital financial ecosystem, including key platforms likeeCitizen (Kabui & Omondi, 2023). The COVID-19 pandemic's digital acceleration heightened cybersecurity concerns, with a surge in remote work creating opportunities for cybercriminals (Jaber et al., 2021). Kenya faces significant cybersecurity challenges, with the Communications Authority of Kenya (CAK) reporting over 7.7 million attacks since 2017, targeting critical information infrastructure and essential government services (Africanews, 2023).

Critics point out gaps in cybersecurity policies and knowledge disparities between IT professionals and non-IT officials (Sliwinski, 2014; Caruson et al., 2012). Resilient frameworks for e-government projects and the potential of big data analytics in cybersecurity present avenues for improvement (Alrubaiq and Alharbi, 2021; Sharma and Barua, 2023). Cyber resilience, essential in the digital era, ensures continuity and functionality under adverse conditions (Safitra et al., 2023). Achieving this resilience demands a holistic approach integrating technological solutions, heightened employee awareness, and collaboration (World Economic Forum, 2024). The shortage of skilled cybersecurity professionals is challenging, emphasising the need to upskill current staff and diversify the talent pool (World Economic Forum,

2024). A robust cybersecurity culture, emphasising continuous learning, transparent communication, and ethical behaviour, is central to cyber resilience (Aksoy, 2024).

While technology advancements and cybersecurity strategies drive positive outcomes, they also contribute to increased cyber incidents and data breaches (Onwubiko, 2020). This has spotlighted theimportance of cyber resilience within a robust cybersecurity framework, with a notable research gap inthis area (Onwubiko, 2020). Security leaders express growing concerns about organisational readiness against cyber threats.

An adaptive security policy approach addresses the evolving threats, risks, and contextual factorsspecific to organisations. It encompasses a proactive approach that adapts and evolves to tackle emerging threats. Contrary to traditional security measures that mainly rely on static rules and signatures to detect and prevent cyber-attacks, adaptive security dynamically adjusts to the changing landscape of cyberthreats. A resilient organisation adopts a proactive approach to cyber security by implementing measures to avert cyber-attacks, detect them promptly, respond effectively, and recover swiftly. This necessitates a comprehensive cyber security strategy integrating cutting-edge technologies, established best practices, and pertinent policies. (Shahzad & Qiao, 2022).

## Literature Review

### Adaptive Security Policy and Cyber Security Resilience

"Cyber resilience" emerged in the early 2000s as a response to the need for systems that can resist andrecover from cyber incidents. It has gained considerable attention and is widely recognised as a concept and critical element of comprehensive cybersecurity strategies. (Tzavara et al., 2024). Currently,cybersecurity and cyber resilience are two distinct concepts, with cybersecurity focusing on protecting information and computer systems by limiting access to sensitive data and addressing potential threats,while cyber resilience encompasses a system's ability to maintain functionality even in challenging situations, extending beyond technological measures and requiring employee awareness and cooperation. (Safitra et al., 2023),

The conversation surrounding cyber resilience has progressed. Montasari et al. (2018) emphasised the necessity of multi-layered, intelligence-driven strategies considering human psychology in attacks. Annarelli et al. (2020) advocated for robust tactics beyond traditional methods, highlighting the

significance of cyber resilience in the digital age. Caron et al. (2019) proposed an adaptive security strategy leveraging automation, machine learning, and real-time threat intelligence for quicker anomaly detection and incident response. Brass and Sowell (2020) discussed the vulnerabilities associated with the Internet of Things (IoT) and proposed an adaptive regulatory governance model for continuousknowledge exchange. Robertson and Laddaga (2012) explored a DARPA-supported project for creating a self-aware network using self-adaptive techniques to sustain computational functions during attacks.

Munusamy and Khodadi (2023) emphasised achieving resilience through resilience itself amid technological advancements. Halabi et al. (2022) applied adaptive control theory to Cyber-Physical Systems (CPSs) in Industry 4.0 to ensure secure control approaches. Abdullayeva (2023) introduced an approach for enhancing cloud computing security focusing on virtualisation, service layers, and a new cybersecurity reference model. Tsigkanos et al. (2016) proposed Bigraphical Reactive Systems forspeculative threat analysis in cyber-physical systems. Al-Hawamleh (2024) developed a Cybersecurity Resilience Framework integrating governance, external collaboration, and continuous monitoring.Mbanaso et al. (2019) introduced a Cybersecurity Resilience Maturity Measurement framework for South African nations, focusing on organisational readiness. Malatji et al. (2020) examined cybersecurity responsibilities within South Africa's water and wastewater sector, identifying gaps inimplementation and emphasising the need for a computer security incident response team.

Akech et al. (2020) highlighted cyber resilience vulnerabilities in Kakamega County, Kenya, emphasising collective responsibility in enhancing cyber resilience. Taruvinga (2020) comparedcybersecurity threats in Kenya and Zimbabwe, recommending prioritising human rights in cyber policies and implementing data protection laws.

**Organisation Culture and Cyber Security Resilience**

Organisational culture plays a crucial role in bolstering cyber security resilience. Leveraging organisational culture as an adaptive security policy is crucial for this endeavour; cyber resilience encompasses both technical and human aspects, including behaviours, values, and attitudes that shape an organisation's cybersecurity approach (Aksoy, 2024). A robust cybersecurity culture permeatesemployees' daily routines, practices, and mindsets, positioning the company's values and practices in both professional and personal spheres.

**Effective leadership** is crucial in cultivating organisational organisational culture. Leaders play a vital role in shaping the attitudes, behaviours, and practices related to cybersecurity within an organisation. According to Watkins (2013), organisational culture is essential for fostering collaboration, understanding, and goal alignment, key drivers of unified action within an organisation. How leaders allocate resources, demonstrate knowledge and skills, promote awareness, and encourage continuous learning all contribute to developing a strong cybersecurity culture.

Zgouva (2020) stressed the importance of aligning governance and management models with an organisation's strategic direction, emphasising the necessity of a cyber strategy, skilled personnel, effective communication between boards and security leadership, and a clear reporting structure tobolster cyber resilience. Njoroge (2020) identified key factors influencing cybersecurity culture in SMEs in Nairobi City County, such as top management support, reward systems, policies, change management, training, awareness programs, and monitoring. These findings highlight the importance of continuous engagement in cybersecurity practices.

Herath and Rao (2009) suggested that a positive cybersecurity culture can significantly reduce thelikelihood of successful cyberattacks. However, Alawida et al. (2022) warned of the rising cyberattack risks, especially during events like the Covid-19 pandemic. Amankwah-Amoah et al. (2021) and Battisti, Alfiero, and Leonidou (2022) emphasised the need for robust cybersecurity practices in remote working environments, which COVID-19 has accelerated. Obuhuma et al. (2020) focused on social engineeringin cybersecurity, highlighting the importance of user education, awareness, and the implementation of information security policies and legislation. Chitechi et al. (2023) identified a significant lack ofpreparedness for cybersecurity vulnerabilities in Kakamega and Bungoma counties, Kenya, indicating a need for improvement in cybersecurity management within Kenya's County Governments.

De Silva (2023) and Gupta et al. (2023) advocated involving employees in policy development, rewarding responsible behaviour, and investing in comprehensive training programs to cultivate a strong cybersecurity culture. However, da Veiga et al. (2020), Cano (2021), and Hassandoust and Johnston (2023) pointed out gaps in comprehensive frameworks addressing the impact of organisational culture on cybersecurity. Were (2021) stressed the significance of cybersecurity in the fourth industrial revolution, identifying gaps in Kenya's implementation

of UN Cyber Norms. Suggestions include

transitioning to international law, fostering collaboration between private and government sectors, and investing in cyber deterrence and transparency.

**Theoretical framework**

The Technology Acceptance Model (TAM) was used to understand ICT officers' and internal auditors' attitudes and perceptions towards ASP implementation. TAM is a theoretical framework developed to understand and predict how users adopt and use new information technologies. Fred Davis proposed it in the late 1980s, and has since become one of the most widely used models for studying user acceptance of technology. TAM provides a theoretical framework for examining ICT officers' and internal auditors' attitudes and perceptions regarding implementing adaptive security policy (ASP) and cybersecurityresilience within the Directorate of Immigration Services in Kenya. TAM uses the concepts of perceived usefulness and ease of use to predict the likelihood of adoption while identifying potential barriers and informing intervention strategies. By helping to understand stakeholders' acceptance of ASP, TAMfacilitates the assessment of obstacles to implementation and supports targeted interventions such astraining and support. Additionally, TAM enables the evaluation of success factors over time by monitoring changes in attitudes and adoption rates.

**Research Methodology and Design**

The research used a mixed-methods design, incorporating a systematic literature review and interviews with ICT officers and internal auditors from the Directorate of Immigration Services in Nairobi. The target population consisted of 89 individuals, including cybersecurity professionals, system administrators, network engineers, and non-technical staff. Data collection employed purposefulsampling to gather insights from experts in the field. A forensic examination of past cyber incidents was conducted to identify attack vectors and vulnerabilities. The sample size, calculated using Solvin's formula, comprised 73 respondents. Data collection tools included questionnaires and interviewschedules. Quantitative data was analyzed using SPSS software, while qualitative data underwentthematic analysis, ensuring a comprehensive examination of the research problem.

**Findings and Discussion**

**Cyber Security Resilience in directorate of immigration and citizen services**

The findings reveal that 50% of respondents believe their organisations would face challenges indetecting and responding to cyber threats. Ghelani (2022) conducted a qualitative study in Korea, highlighting a heavy reliance on preventive measures due to a focus on technology availability and limited awareness of broader security issues. The study suggests a need for a balanced approach thatintegrates preventive measures with other tactics at the operational level. Hasan et al. (2021) analysed 270 IT professionals in Bahrain and found that cyber-attacks are increasing and impacting organisational performance. Using the Technology-Organization-Environment framework, they identified seven factors that positively influence security performance, indicating that cybersecurity readiness enhances organisational security performance.

The findings on how often the organisation reviews and updates its cybersecurity policies and procedures indicate that 40% responded "others," suggesting no designated review timelines. Li et al. (2019) highlighted that employees with knowledge about company security policies demonstrate higher cybersecurity proficiency. A supportive organisational environment fosters compliance by enhancing threat and coping appraisals. Regarding disaster recovery, 90% of respondents confirmed having abackup disaster recovery plan. Chang (2015) emphasised the importance of disaster recovery in big data systems, proposing a multi-purpose approach that ensures close to 100% recovery rates.

The Directorate of Immigration experienced significant cyber incidents in 2023, mainly targeting itseCitizen platform. These attacks disrupted services, affecting Kenyan citizens and officials. Notableincidents involved Distributed Denial of Service (DDoS) attacks. Ali et al. (2022) warned of vulnerabilities in e-government due to technological advancements, while Shandler and Gomez (2022) highlighted the impact of cyber-attacks on public confidence. The Directorate employs a multifaceted approach to cyber risk management, with a dedicated cyber department overseeing security initiatives. Advanced technologies like load balancers, IDS, and IPS detect and prevent threats. Employee trainingprograms and regular updates mitigate vulnerabilities. Perimeter defences, system audits, and ethicalhacking tests further enhance resilience. DiMase et al. (2015) suggested a comprehensive risk management framework, emphasising the importance of

identifying and prioritising cybersecurity risks.

The Directorate has robust measures in place for rapid recovery from cyber incidents, including disaster recovery plans, backup systems, secure authentication, firewalls, antivirus software, and regular audits. Whitham (2023) emphasised the importance of detailed plans in accelerating recovery. Incident response plans reduce downtime and maintain public trust (Nichols, 2023). Cybersecurity training and awareness programs vary within organisations, with strategies ranging from regular sessions to ad hoc training tailored to system importance. Ongoing awareness campaigns reinforce cybersecurity practices and educate employees on combating cyberattacks. Buchanan Technologies (2022) highlighted the significance of security awareness training in building a proactive defence mechanism.

Challenges in achieving cyber resilience include a lack of IT knowledge, cybersecurity expertise, innovation, talent shortages, and financial constraints. Human vulnerabilities, increasing interconnectivity, and regulatory complexity contribute to cybersecurity breaches. Addressing thesechallenges requires a multifaceted approach involving technological innovation, regulatory measures, education, and stakeholder collaboration (Wyman, 2020; Oh, 2024).

**Adaptive Security Policy and Cyber Security Resilience**

The finding on whether there is an established process for incorporating feedback from security incidents into policy updates revealed that 90% of respondents answered yes. Incorporating feedback from security incidents into policy updates is crucial for organisational learning and enhancing risk awareness (Patterson et al., 2023; Connolly and Wall, 2019). It ensures that lessons learned translate into actionable changes to prevent future incidents. Regarding how the organisation adapts its security policies to address emerging cyber threats, it employs technological upgrades, proactive testing, education,research, and compliance with best practices. Sexton (2017) emphasised the importance of safeguarding organisations before breaches occur by evaluating current preparedness levels and implementingimprovement programs. Cybersecurity automation enhances efficiency and response times (Raizada,2024).

The organisation prioritises cybersecurity through a multifaceted approach, employing various technologies and strategies such as Intrusion Detection and Prevention Systems (IDPS), Network Access Control, Least Privilege Principle, and system hardening. Advanced technologies like machine learning (ML) and Data Loss Prevention (DLP) bolster defences, while automated

response mechanisms and

distributed security systems enhance real-time threat detection and mitigation. These cybersecurity automation technologies are a multiplier, improving security skills and impact (Wadhwa, 2023).

Machine learning and artificial intelligence (AI) are pivotal in enhancing cybersecurity, covering access management, threat detection, response, adaptability to emerging threats, automated auditing, access control, and government integration. While ML and AI hold significant potential in detecting andmitigating harmful activities within computer systems and networks (Holmes, 2023), a holistic approach combining these advanced technologies with traditional security measures is essential for bolsteringorganisational cybersecurity resilience (Atef, 2023).

The responses emphasise the importance of a comprehensive approach to cybersecurity, which includes reviewing and complying with policies, implementing education and awareness campaigns, updating infrastructure and technology, managing risks, and conducting evaluations. Continuous improvement, adaptation, and ongoing training and development efforts are also vital. Willie (2023) emphasisesfostering a security-focused culture to enhance resilience against cyber threats and protect vital digital assets. Temitayo et al. (2024) highlighted a trend towards leveraging advanced technologies like artificial intelligence (AI) and machine learning (ML) in cybersecurity. They also note the significant impact of human elements on cybersecurity outcomes and the influence of international policies onstandardising cybersecurity practices.

**Organisational Culture and Cyber Security Resilience**

50% of respondents rated the level of cybersecurity awareness among employees in the organisation as moderate, indicating existing vulnerabilities. Li et al. (2019) found that employees aware of their company's information security policies are better equipped to manage cybersecurity responsibilities. Kemper (2019) highlights employees as the primary vulnerability in organisations, emphasising the importance of engaging and motivating them to actively participate in cybersecurity efforts through clear policies and compliance strategies.

Regarding cybersecurity training provision, 90% of respondents confirmed that the organisationconducts such training. Aaltola and Taitto (2019) stress the significance of recognising and leveraging learners' existing skills, suggesting that the educational process should start by assessing participants' competencies. Tolossa (2023) recommends tailoring training for remote work

to enhance organisational

adaptability. Organisations can proactively safeguard assets and maintain a secure digital stance byinvesting significantly in cybersecurity awareness training. 60% of respondents confirmed that cybersecurity is included in the performance evaluation criteria for employees. Alqahtani and Erfani (2021) found a positive relationship between technical cybersecurity controls, accountability, monitoring, and employee stress levels. Koutsouris et al. (2021) stressed the importance of assessment methods in training initiatives and evaluation tools in enhancing organisational security measures.

Regarding reporting security incidents or suspicious activities, 90% indicated a clear process in place. Alharbi (2023) proposed the Holistic Evaluation Model for Information Security Awareness Programs, emphasising the need for a comprehensive approach combining passive and active data collection.Carpenter (2023) highlighted the importance of incident reporting in fostering a robust security culture, while Irei and Shea (2024) emphasised the risks associated with disorganised reactions to cyberattacks.

The organisational culture regarding cybersecurity reflects proactive vigilance mixed with occasionalindifference. Challenges persist in ensuring uniform adherence, especially among middle-level employees. Pavlova (2020) emphasised the role of management in maintaining organisational culture through education, reviews, rewards, and value hierarchies. Karlsson et al. (2021) suggested thatinternal-focused organisational cultures correlate with higher adherence to information security policies. Top management's proactive involvement in supporting cybersecurity initiatives is evident through their leadership, funding, and collaboration efforts. Loonam et al. (2020) highlighted the role of effective leadership in corporate-level attention to information security. Marotta and Pearlson (2019) discussed efforts by the leadership team at BPS to strengthen relationships and establish a robust cybersecurityculture.

Employee perceptions of cybersecurity vary; some show strong awareness and concern, while others exhibit neutral stances or lack awareness. Gratian (2018) stressed the importance of recognisingindividual differences in cybersecurity behaviours. Egelman and Peer (2015) and Sheng et al. (2010) found relationships between risk propensity and security behaviours. Barriers to fostering a more robust cybersecurity culture include limited resources, gaps in employee knowledge, dynamic cyber threats, communication difficulties, and inadequate training. Chaudhury (2020) highlighted challenges likefinancial constraints, organisational culture, and

time constraints, particularly for smaller enterprises.

Hinchy (2023) emphasised the need for security teams to access the latest information and effectively communicate with stakeholders to address evolving threats.

**Conclusion**

Cyber resilience is gaining prominence as technology advances and cyber threats become more sophisticated. Organisations now understand the need to defend against attacks and maintain operations during disruptions. Cyber resilience is a burgeoning field within cybersecurity and presents an opportunity for the research community to contribute and develop a strong knowledge base.

The examination of cyber security resilience within the Directorate of Immigration and Citizen Services underscores both strengths and challenges in the organisation's ability to address cyber threats. The analysis reveals a complex landscape where management is crucial in promoting a cybersecurity- conscious environment. The results highlight that Organisational culture and cybersecurity resilience are closely intertwined, with awareness, training, reporting mechanisms, and leadership playing vital roles. Advanced technologies such as machine learning and artificial intelligence can enhance security capabilities. However, a comprehensive approach that combines them with conventional measures isvital for effective resilience. To enhance cyber resilience within the Directorate of Immigration and Citizen Services and across public institution in Kenya. There is a need for a holistic approach that prioritises raising awareness, providing targeted training, reviewing policies, and adopting advancedtechnologies.

**Recommendations**

- Develop a national framework for cyber resilience tailored to the specific needs of public institutionsin collaboration with cybersecurity experts, academia, and industry stakeholders.
- Adopt an adaptive security approach integrating governance principles, external collaboration,continuous monitoring, and organisational culture.
- Encourage the adoption of multi-layered, intelligence-driven security strategies incorporatingpeople, automation, machine learning, and real-time threat intelligence.
- Promote a security-first culture aligning governance and management models with cybersecurityobjectives.

- Prioritise cyber resilience training and capacity building for all employees, covering both technical and non-technical aspects of cybersecurity.
- Implement a comprehensive risk management framework integrating physical, information,cognitive, and social domains.
- Establish standardised incident reporting and response mechanisms across organisations.
- Foster a continuous improvement and adaptability culture in cybersecurity practices through regularupdates, risk management, and evaluations.

**References**

Abdullayeva, F. J. (2023, September 1). Cyber resilience and cyber security issues of intelligent cloud computingsystems. Results in Control and Optimisation. https://doi.org/10.1016/j.rico.2023.100268

AFRICA NEWS (2023), https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a- year// retrieved march17 2024

Akech, P., Abeka, S., & Liyala, S. (2020). A Framework Based On Institutional Theory To Aid In Cyber Resiliency In County Governments Of Kenya. *International Journal of Innovative Research and Advanced Studies*(IJIRAS), 7(7), 142-147.

Aksoy, C. (2024). Building a cyber security culture for resilient organisations against cyber attacks. İşletme Ekonomi Ve Yönetim Araştırmaları Dergisi, 7(1), 96-110. https://doi.org/10.33416/baybem.1374001

Alharbi, T. (2023). A Holistic Evaluation Model for Information Security Awareness Programs in Work Environment. 2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ),CFP23RAC-ART, 1-4.

Ali, S., Jamali, A. K., Shah, S. Z. H., Qureshi, S. N., & Tanveer, S. (2022, October 3). *IMPACT OF CYBER-TERRORISM ON NATIONAL SECURITY OF PAKISTAN*. https://archives.palarch.nl/index.php/jae/article/view/11396

Alqahtani, M., & Erfani, E. (2021). Impact of Technical Controls, Accountability, and Monitoring on the JobPerformance of Employees: Assessing the Mediating Role of Stress. ACIS.

Alrubaiq, A., & Alharbi, T. (2021, May 18). *Developing a Cybersecurity Framework for e-Government Project inthe Kingdom of Saudi Arabia*. *Journal of Cybersecurity and Privacy*. https://doi.org/10.3390/jcp1020017

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient

systems.

*Computers & Industrial Engineering*, 149, 106829.

Atef, M. (2023, April 16). The Role of Artificial Intelligence and Machine Learning in Cybersecurity. Medium. Retrieved 28 March 2024 from https://medium.com/@m.atef_72234/the-role-of-artificial-intelligence- and-machine-learning-in-cybersecurity-6ebaa28f9d72

Brass, I., & Sowell, J. H. (2020, July 13). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, 15(4), 1092–1110.

Buchanan Technologies (2022, July 15). Five Major Benefits of Security Awareness Training. Buchanan Technologies. https://www.buchanan.com/benefits-security-awareness-training/

Caron, F. (2019). Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal.*

Carpenter, P. (2023, July 31). #HowTo: Create a Culture of Incident Reporting. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/create-culture-incident-reporting/

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012, December 4). *Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success*. *Journal of Homeland Security and Emergency Management.* https://doi.org/10.1515/jhsem-2012-0003

Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. Ad hoc networks, 35, 65-82.Chaudhury, D. (2020, July 6). Barriers to Inculcating Good Cyber Security Habits Amongst Employees. ITSecurityWire. https://itsecuritywire.com/featured/barriers-to-inculcating-good-cyber-security-habits-amongst-employees/

Cheptoo, K. P., & Obare, R. M. (2023). A Framework for Electronic Document Management in theImplementation of E-Government in Kenya.

Chitechi, K. V., Benjamin Kiprono, & Frank Tireito. (2023). Cyber- Security Vulnerability and Initiatives inKenyan County Governments. African Journal of Computing and Information Systems (AJCIS), 7(X), 35–51. https://doi.org/10.1234/ajcis.v7iX.38

Connolly, L., & Wall, D. S. (2019, November). The rise of crypto-ransomware in a changing cybercrimelandscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Corradini, I., & Nardelli, E. (2018). Building Organisational Risk Culture in Cyber Security: The Role

ofHumanFactors. Advances in Intelligent Systems and Computing.

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime.* demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems(pp. 2873-2882). ACM.

Fortinet. (2022). 2022 Cybersecurity Skills Gap Survey. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *AuthoreaPreprints*.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.

Gupta, V., Singh, S.P., Singh, C., & Mangla, A. (2022). A Systematic review on Cybersecurity: Models, Threats and Solutions. 2022 10th International Conference on Emerging Trendsin Engineering andTechnology - Signal and Information Processing (ICETET-SIP-22), 1 6

Halabi, T., Haque, I., & Karimipour, H. (2022, December). Adaptive Control for Security and Resilience ofNetworked Cyber-Physical Systems: Where Are We?. In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 239-247). IEEE.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organisations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Hinchy, E. (2023, March 9). 6 Ways To Go Beyond Awareness And Foster A Real Culture Of Cybersecurity.Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/03/08/6-ways-to-go-beyond-awareness- and-foster-a-real-culture-of-cybersecurity/?sh=7b782aba2168

Holmes, J. (2023, October 17). The Role of AI and ML in Business Cyber Security. Stanfield IT. https://www.stanfieldit.com/the-role-of-ai-and-ml-in-business-cyber-security/

Irei, A., & Shea, S. (2024, January 30). What is incident response? A complete guide. Security. https://www.techtarget.com/searchsecurity/definition/incident-response

Jaber, A. N., & Fritsch, L. (2021). COVID-19 and Global Increases in Cybersecurity Attacks: Review of Possible Adverse Artificial Intelligence Attacks. In 2021 25th International Computer Science and

Engineering Conference (ICSEC) (pp. 434-442).

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021, December 21). The effect of perceived organisational culture on employees' information security compliance. Information & Computer Security. https://doi.org/10.1108/ics-06-2021-0073

Kasowaki, L., & Eden, S. (2023). *The Human Element in Cubersecurity: Understanding and Mitigating Risks* (No.11642). Easyschair

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11- 14.

Koutsouris, N., Vassilakis, C., & Kolokotronis, N. (2021, July 26). Cyber-Security Training Evaluation Metrics. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. https://doi.org/10.1109/csr51186.2021.9527946

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating Cybersecurity Strategies in Africa. Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security, 1–19. https://doi.org/10.4018/978- 1-7998-8693-8.ch001

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

Loonam, J., Zwiegelaar, J.B., Kumar, P., & Booth, C. (2020). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. IEEE Transactions on Engineering Management, PP, 1-14.

Majumdar, N., & Ramteke, V. (2022, October). Human elements impacting risky habits in cybersecurity. In *AIP Conference Proceedings* (Vol. 2519, No. 1). AIP Publishing.

Marotta, A., & Pearlson, K. E. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. AmericasConference on Information Systems.

Marotta, A., & Pearlson, K.E. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. AmericasConference on Information Systems.

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019, June 27). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. The African Journal of Information and Communication.https://doi.org/10.23962/10539/27535

Montasari, R., Hosseinian-Far, A., & Hill, R. (2018). Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. Cyber criminology, 71-93.

Munusamy, T., & Khodadi, T. (2023). Building Cyber Resilience: Key Factors for Enhancing

OrganizationalCyber Security. Journal of Informatics and Web Engineering, 2(2), 59-71.

Nichols, C. (2023, September 5). 3 Benefits of an Incident Response Plan. Cybriant. https://cybriant.com/incident- response-plan/

Njoroge, G. M. (2020). Human Factors Affecting Favourable Cybersecurity Culture- a Case of Small and Medium- sized Enterprises Smes Providing Enterprise-Wide Information Systems Solutions in Nairobi City Countyin Kenya. http://erepository.uonbi.ac.ke/handle/11295/153139

OBUHUMA, J., & ZIVUKU, S. (2020, May). Social engineering based cyber-attacks in kenya. In 2020 IST-Africa Conference (IST-Africa) (pp. 1-9). IEEE.

Ogonji, M. (2019). Promoting Security In Africa Through Effective Counter Cyber Terrorism Strategies (Doctoral dissertation, University of Nairobi).

Oh, H. (2024, January 29). 4 Challenges Organisations Face When Operationalizing Cybersecurity. SolCyber.https://solcyber.com/4-challenges-organizations-operationalizing-cybersecurity/

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness ofmobile security threats. Information & Security, 32(2), 1.

Onwubiko, C. (2020). Focusing on the Recovery Aspects of Cyber Resilience. In International Conference onCyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-13). https://doi.org/10.1109/CyberSA49311.2020.9139685

Open Data Kenya, http://www.opendata.go.ke, accessed 15 March 2017.

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023, September). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

Pavlova, E. (2020). Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation. Information & Security: An International Journal, 46(3), 239–249. https://doi.org/10.11610/isij.4617

Pérez-Morón, J. (2022) Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, areview and future research agenda Open Access Journal of Asia Business Studies

Raizada, A. (2024, March 6). The Role of Automation in Making Cybersecurity Accessible to All. Copper Digital. Retrieved 28 March 2024 from https://copperdigital.com/blog/the-role-of-automation-in-cybersecurity-accessibility/

Resilience. (2023). 2023 Mid-Year Cyber Claims Report. https://unlock.cyberresilience.com/2023_midyear_claims_

Robertson, P., & Laddaga, R. (2012, September). Adaptive security and trust. In 2012 IEEE Sixth

InternationalConference on Self-Adaptive and Self-Organizing Systems Workshops (pp. 55-60). IEEE.

Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: a Case Study of Kenya (Doctoraldissertation, university of Nairobi).

Safitra, M. F., Lubis, M., & Kurniawan, M. (2023). Cyber Resilience: Research Opportunities. https://doi.org/10.1145/3592307.3592323

Schneier, B. (2008). "The New School of Information Security." Addison-Wesley Professional.

Security Scorecard. (2022). Cyentia Institute and SecurityScorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind. https://securityscorecard.com/research/cyentia-close-encounters-of-the- third-and-fourth-party-kind/

Sexton, L. (2017, July 6). How companies can stay ahead of evolving cyber threats - Financial Services Thought Gallery. Financial Services Thought Gallery. https://eyfinancialservicesthoughtgallery.ie/steps-financial- services-companies-need-take-stay-ahead-evolving-cyberthreats/

Sharma, P., & Barua, S. (2023). From Data Breach to Data Shield: The Crucial Role of Big Data Analytics in Modern Cybersecurity Strategies. International Journal of Information and Cybersecurity, 7(9), 31–59.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382).

Sliwinski, K. F. (2014, September 2). Moving beyond the European Union's Weakness as a Cyber-Security Agent.

*Contemporary Security Policy*, *35*(3), 468–486.

Taruvinga, F. (2020). Emerging Cyber Security Threats: A Comparative Study Of Kenya And Zimbabwe.http://erepository.uonbi.ac.ke/handle/11295/153882

Wadhwa, P. (2023, September 18). 7 Best Cybersecurity Automation Tools. Sprinto. Retrieved 28 March 2024 from https://sprinto.com/blog/cybersecurity-automation-tools/

Watkins, M. (2013). What is organisational culture? And why should we care. *Harvard Business Review*, *15*, 1-5.

Were, T. O. (2021). Implementation of UN Cyber Norms in the Promotion of International Security: a Case Studyof Kenya (Doctoral dissertation, University of Nairobi).

Whitham, C. (2023, October 6). What Are the Benefits of Cyber Resilience? - North East Business Resilience Centre. North East Business Resilience Centre. https://www.nebrcentre.co.uk/what-are-the-benefits-of- cyber-resilience/

Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture.

SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4564291

World Economic Forum. (2022). Global Cybersecurity Outlook 2022.

https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

World Economic Forum. (2023, November 17). Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector. https://www.weforum.org/publications/facilitating-global-interoperability-of-cyber- regulations-in-the-electricitysector/

Wout, V& Magdalena, C. (2019). Develop and maintain a cybersecurity organisational culture.

Wyman O (2020). The Seven Most Pressing Challenges Facing Cybersecurity. Retrieved march 29 2024 fromhttps://www.marshmclennan.com/insights/publications/2020/february/the-seven-most-pressing- challenges-facing-cybersecurity.html

# Technology Development and Cybercrime in Juja Sub-County

*By*

*Ndirangu Ngunjiri*

## Abstract

Before technological advancements, the world primarily dealt with physical threats. However, with the rise of technology, cybercrime has emerged, becoming accessible to anyone possessing the required skills. Cybercrimes, such as stalking, hacking, phishing, online fraud, identity theft, and virus dissemination, have increased, employing increasingly sophisticated methods daily. These offenses inflict damage ranging from personal identity theft to financial losses, particularly affecting developing countries transitioning to cashless economies. This article explores the impact of technological growth on cybercrime within the Juja sub-county, illustrating how crime evolves alongside technology. An extensive review of existing literature highlights various types of cybercrimes and their consequences, emphasizing the challenges they pose to law enforcement globally. While the Internet offers immense development opportunities, it also serves as a breeding ground for criminal activities. This paradox underscores the need for enhanced regulation and enforcement, particularly in developing nations lacking adequate technology and infrastructure. The expansion of technology has made communication borderless and transnational, complicating cybercrime investigations that often require cooperation across multiple jurisdictions. The paper advocates for a comprehensive approach to combat cybercrime, including establishing robust legal frameworks, strengthening enforcement agencies with advanced technology, and empowering youth with entrepreneurial skills to deter involvement in cybercriminal activities. It also calls for universal criminalization of cyber offenses under international laws and treaties. To reduce the adverse effects of technology on development, the paper recommends creating products that are resilient to cybercrime and enhancing the processes for crime detection and investigation. Tracing the historical evolution of technology, underscores both its positive innovations and negative consequences, urging policymakers, businesses, and individuals to recognize cybercrime as a global issue requiring collective action.

**Keywords:** *Cybercrime, Cyberspace, hacking, Cyber-attacks, Computer Crime, Identity Theft, phishing, hackers, fintech*

**Introduction**

Over the past few years, advancements and breakthroughs in technology have completely transformed our lifestyles, professions, and methods of communication. Although these progressions have offered countless advantages and openings, they have also introduced fresh obstacles, especially concerning cybersecurity. Cybercrime, which refers to criminal activities carried out using computers and the internet, has become a growing concern in many parts of the world, including the Juja Sub-County in Kenya (Njuguna et al.,2021 ). This paper explores how technological developments and innovations have influenced the rise of cybercrime in Juja Sub-County, and discusses potential solutions to address this issue.

Cybercrimes range from minor intrusions to severe instances like identity theft and phishing. Illustrations of cybercrimes encompass scams and phishing, identity theft, ransomware assaults, hacking, and online fraud. Phishing happens when criminals send spam messages claiming to be legitimate sources to collect personal information. Prevention of phishing relies on detection measures (Khonji et al., 2013). Ransomware involves the installation of programs holding the computers of a person or programs ransom demanding payments. Credit card fraud is also a common form of cybercrime that goes unnoticed. Other forms of cybercrime include harassment and bullying, intellectual property theft, and child pornography.

There is an increased awareness globally regarding the importance of cybersecurity and the prevalence of cybercrimes. The cost of cybercrime has been increasing each year and it is expected to rise by 5.7 trillion US Dollars between 2023 and 2024 (Petrosyan, 2023). The cost currently stands at $13.83 trillion and it is expected to reach its maximum in 2028. The number of new ransomware used by cybercriminals has been on the rise with the peak attained in 2017, the number has been declining since then (Petrosyan, 2023). Figure 1 shows the number of new ransomware families that are discovered each year.

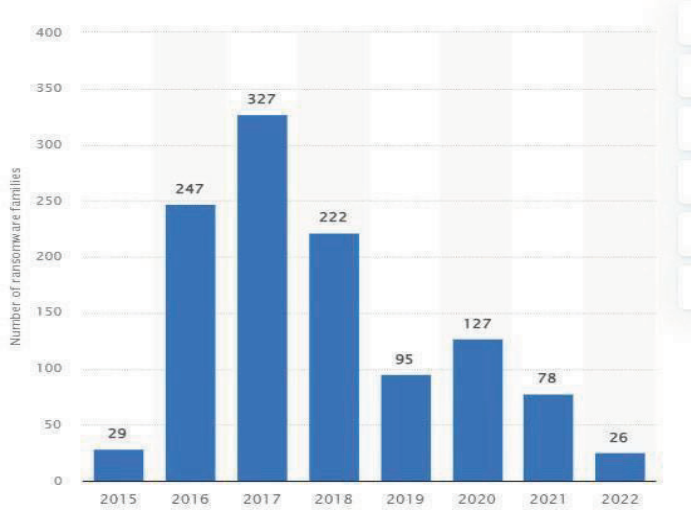


**Figure 3: Number of New ransomware each year**

Source: Statista,2023

Existing research shows that financial technology is the most affected sector by cybercrimes. Cybercrimes in this sector include the restriction of financial data, theft, modification of financial data, tampering with personal information stored in cards, etc. The ongoing digital transformations have led to increased risks of crimes in the financial sector, this is because of the rapid process of transformation with banks competing with the technological sector. For instance when the vulnerabilities of the SWIFT, the global financial system messaging system, were interfered with in 2016, over 100 Million dollars were lost (Maurer & Nelson, 2021) .

Deficiencies in cybersecurity law and existing loopholes are the greatest challenge to security globally in this century. Securing cyberspace is a challenge that has made it hard for even developed countries like the USA to manage their national security (Flowers et al., 2013. Countries are investing significantly in cybersecurity through the creation of institutions and security measures.

The paper addresses the issue of the recent surge in cybercrimes. There is increased development in the technology sector. As technology improves, there is also an increase in the need for people to adopt more security measures in the technology sector. More and more of human activities are being automated. Any cybersecurity dangers can affect almost all aspects of organizations. As

more and more aspects of organizations are digitized and as a large portion of everyday activities gets influenced by advancements in technology, so does cybercrime and the motivation of cybercriminals. Emily (2022) posits that technological advancement has improved the running of businesses, but that has also increased the need for cybersecurity.

Existing research shows that cybercrime is closely linked with technological advancement. However, the research also shows that technological development has led to a reduction in cybercrime (Bellasio & Silfversten, 2023). Different types of research conducted in the recent past show that an improvement in technology has encouraged more sophisticated forms of cybercrime (Oates, 2001). There is therefore a need to research to determine how technological development within Juja Sub-county in Kenya. Therefore, the main objective of this paper is to investigate how technological developments and innovations influence cybercrime in the Juja sub-county. The specific objectives are: First, to understand cybercrimes and technological developments in Kenya and specifically, the Juja sub-county. Second, to evaluate the effects of technological developments in Kenya on cybercrime in the Juja sub-county.Third, to examine the possible challenges and solutions for addressing cybercrimes in Juja Kenya

## Theoretical Literature review

### Diffusion of Innovation Theory

E.M. Rodgers introduced the diffusion of innovation theory in 1962, primarily employed in communication to elucidate the emergence and adoption of new concepts within a particular social group or population. The theory explains how new ideas and technology are spread (Rogers, 1962). The process by which new ideas are spread from one person to the other is heavily reliant on social capital and how cohesive a society is. The theory does not just explain the spread of ideas, technology, and information but also explains vices such as hacking, credit card fraud, and other cybercrimes.

According to the theory, people have different rates of adopting new ideas and technology. This is summarized by the chart below:


**Figure 4: Diffusion of technology**

Source: Leanmonitor Report,2022

Innovators and early adopters of cybersecurity benefitted from the benefits of securing their enterprises. Cybercriminals are innovators by nature and they keep coming up with new approaches when their old techniques are resolved, early adopters of cybersecurity can lock them out of their systems in time (Hasani et al., 2023). The offenders keep creating new malware and the defenders must keep innovating new methods of detecting the malware and dealing with them. One must always be ahead of the attackers to avoid being their next victim. The late majority and laggards are the ones that usually end up as victims of cyber-attacks.

**Technology Acceptance Model**

The Technology Acceptance Model (TAM) expands upon the Theory of Reasoned Action (Ajzen & Fishbein, 1980). Initially introduced by Davis in 1989, TAM offers further insights into how individuals perceive and adopt new technologies. The model explains how the ease of use and perceived usefulness influence the acceptance of technology (Davis, 1989). The model is mainly centered on explaining the perceptions of people and how they affect their adoption of technology. Innovators and those who come up with new products are also tasked with the responsibility of influencing the beliefs of the market concerning the perceived usefulness of their products.

Rick et al., (2016) argued that when users perceive the threat of cybercrime, they are likely to reduce their usage of technology or increase their adoption of cybersecurity measures. Cybersecurity farms have the responsibility of ensuring that companies and individuals understand

the usefulness of cybersecurity for them to adopt it. At times people discover this through their experiences when they experience one or more cybercrimes while at other times, the creation of awareness and sharing of information enables people to understand the usefulness of cybersecurity.

Analyzing the interplay between technological developments, innovations, and the rise of cybercrime in the Juja Sub-county reveals a complex relationship shaped by various factors. Firstly, technological advancements have facilitated the proliferation of cybercrime by providing sophisticated tools and platforms for illicit activities. The increasing digitization of financial transactions, communication channels, and personal data storage creates lucrative opportunities for cybercriminals to exploit vulnerabilities. Moreover, innovations such as artificial intelligence and cryptocurrency present new challenges for law enforcement agencies in detecting and preventing cybercrimes. AI-powered malware can evade traditional security measures, while cryptocurrencies offer anonymity and untraceable transactions, facilitating ransomware attacks and money laundering schemes.

Additionally, the rapid expansion of internet access and mobile technologies in the Juja Sub-county has widened the pool of potential targets for cybercriminals. As more individuals and businesses embrace digital technologies, they become more susceptible to cyber threats due to inadequate cybersecurity awareness and measures. Furthermore, the lack of robust cybersecurity infrastructure and regulations exacerbates the cybercrime problem in Juja Sub-county. Insufficient investment in cybersecurity initiatives and limited enforcement of existing laws create a conducive environment for cybercriminals to operate with impunity. The nexus between technological developments, innovations, and the rise of cybercrime in Juja Sub-county and Kenya at large underscores the urgent need for comprehensive cybersecurity strategies that encompass awareness campaigns, regulatory frameworks, and technological solutions tailored to the local context. Collaboration between government agencies, private sector stakeholders, and the community is essential to mitigate the escalating cyber threats and safeguard the digital ecosystem.

**Methodology**

The research design provides the blueprint of a study and it guides answering the research questions and how to minimize the errors (Dulock, 1993). This study used a qualitative descriptive research design to explore how technological developments and innovations influence the rise of cybercrime in Juja Sub-County, Kenya. The descriptive research design describes the relationship that exists between two different variables, such as technological progress and cybercrimes in this case (Siedlecki, 2020). A qualitative research design explains the aspects of a phenomenon that cannot be quantitatively measured (Patton, 2005). The qualitative Secondary data sources such as newspaper articles, published reports, research articles, and Journals were analyzed to understand the relationship between technological advancements and cybercrime.

The data collection process involved gathering relevant secondary data from various sources, including online newspapers, academic journals, research reports, and other published materials. The data was collected systematically and organized for analysis. A comprehensive search was conducted to identify relevant newspaper articles related to cybercrime and technological developments in the Juja Sub-County. Both print and online newspapers were considered for gathering recent information. Government reports, organizational reports, and any other published documents concerning cybercrime, technological advancements, and their impact on Juja Sub-County were also consulted to obtain the required. This paper also used academic studies and research papers published in scholarly journals and conference proceedings, focusing on cybercrime and the influence of technology. Peer-reviewed academic journals, books, and other relevant literature discussing the relationship between technology and cybercrime were also examined to gain insights into the topic.

A purposive sampling technique was used to select relevant secondary data sources for analysis. Only data that specifically pertains to technological advancements and cybercrime in the Juja Sub-County will be included in the study. The selected data sources were critically reviewed and analyzed for their relevance and reliability. The inclusion criteria required that all the data sources be recent and that the oldest source was not more than 30 years old. The data sources were also required to be reliable and relevant to technological developments and cybercrimes in Kenya.

The collected data was analyzed using thematic and content analysis. Themes related to the impact of technological developments on cybercrime trends in the Juja Sub-County will be identified and analyzed. Patterns, trends, and correlations will be examined to understand the influence of technological innovations on cybercrime. The data sources were critically evaluated to ensure their reliability and validity. Particular attention was paid to the credibility and authoritativeness of the sources. The findings from the content analysis are integrated to form a coherent understanding of how technological developments and innovations influence the rise of cybercrime in the Juja Sub- County. Existing theories or frameworks relevant to cybercrime and technology were considered in interpreting the findings to provide a theoretical perspective. The key factors influencing therise of cybercrime were identified, considering the technological landscape and its impact on cybercriminal activities in the area.

One of the limitations of this study is the availability and quality of secondary data sources. The accuracy and reliability of the data collected from newspaper articles, published reports, and other sources may vary. Efforts will be made to critically evaluate the sources and ensure the validity of the information used in the analysis.

**Discussion of Findings**

**Cybercrime in Kenya**

Cybercrime is a growing concern in Kenya, as the country continues to embrace digital technologies and the internet. As smartphone usage, social media engagement, and online activity continue to rise, cybercriminals are discovering novel methods to exploit both individuals and organizations for financial motives or nefarious purposes. This article aimed to delve into the diverse forms of cybercrimes prevalent in Kenya, elucidate their repercussions on individuals and enterprises, and examine the countermeasures being implemented to confront this escalating menace.

Phishing stands out as one of the prevalent forms of cybercrime in Kenya. This deceitful practice entails the transmission of fraudulent emails or messages to unsuspecting individuals, coaxing them into divulging sensitive information like passwords, credit card data, or personal particulars. These deceptive communications often masquerade as legitimate correspondences from trusted entities such as banks or government bodies, exhibiting a high degree of credibility. Upon

obtaining this sensitive data, cybercriminals can perpetrate various illicit activities, including monetary theft, identity fraud, or other unlawful endeavors.

Another prevalent form of cybercrime in Kenya is online fraud. This includes scams such as fake job offers, lottery scams, and online shopping scams. In these cases, individuals are tricked into sending money or personal information to cybercriminals under pretenses. These scams can have devastating consequences for victims, who may lose their life savings or fall into debt as a result.

Cyberbullying is also a significant issue in Kenya, particularly among young people. Cyberbullies use social media, messaging apps, and other online platforms to harass, intimidate, or threaten their victims. This can have serious consequences for the mental health and well-being of those targeted, leading to anxiety, depression, and even suicide in extreme cases.

The forms of cybercrimes and forms of cybercrimes reported in Kenya in 2021 are summarized in the table below:

| Cybercrime | Number in thousands |
|---|---|
| Malware | 181879 |
| Botnet/DDOS | 92108 |
| Web application attacks | 7037 |
| System vulnerabilities | 58046 |

Source: Statista,2022

Beyond the prevalent cybercrime types, Kenya grapples with the complexities of more advanced threats, including hacking, malware, and ransomware attacks. Hackers adeptly breach computer systems or networks without authorization, aiming to pilfer data, disrupt operations, or execute further malevolent deeds. Malware, encompassing viruses and spyware, surreptitiously infiltrates devices, siphoning sensitive information from users. Ransomware attacks add another layer of peril by encrypting victims' data, and extorting payment in exchange for the decryption key, often accompanied by the menacing prospect of data exposure if the ransom remains unpaid.

The number of cybercrimes in Kenya and online crimes increased from 339.1 million in 2021 to over 700M online crimes in 2022 (Lawi, 2023). The number of cyberattacks increased to over 860

million in 2023 (Musau, 2024). About 79% of these attacks were due to system vulnerabilities. The number of cybercrimes has been increasing from 7.7 million attacks 7 years ago to now over 800 million. Malicious attacks constitute 14% of the attacks, while "Distributed Denial of Services (DDoS)" contributed to approximately 6.55 of all the attacks.

The impact of cybercrime in Kenya is significant, affecting individuals, businesses, and the economy as a whole. Victims of cybercrimes can suffer financial losses, emotional distress, and damage to their reputations. Businesses may face disruption to their operations, loss of sensitive data, and damage to their brand image. The economy as a whole can suffer from the loss of consumer trust, reduced investment, and increased costs associated with cybersecurity measures.

To combat the growing threat of cybercrime in Kenya, the government and law enforcement agencies have taken steps to strengthen cybersecurity measures and improve awareness among the public. The Computer Misuse and Cybercrimes Act passed in 2018 (Governement of Kenya, 2018), provides a legal framework for prosecuting cybercriminals and protecting individuals and organizations from online threats. The Act criminalizes offenses such as unauthorized access to computer systems, cyberbullying, and online fraud, with penalties including fines and imprisonment.

In tandem with legislative actions, the government has set up the National Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) to streamline cybersecurity endeavors and address cyber incidents (Government of Kenya, 2024). This center collaborates with government bodies, private sector entities, and international collaborators to surveil and alleviate cyber threats, administer training and awareness initiatives, and extend assistance to victims of cybercrimes.

Private sector entities in Kenya are proactively fortifying their cybersecurity fortifications to shield against cyber threats. Numerous businesses are allocating resources toward cybersecurity technologies like firewalls, antivirus software, and encryption tools to fortify their data and networks. Additionally, they're instituting robust security policies and protocols to enlighten employees about the perils of cybercrime and advocate for secure online conduct.

Despite these efforts, cybercrime remains a significant challenge in Kenya, with new threats emerging regularly and cybercriminals becoming increasingly sophisticated in their tactics. To

effectively combat cybercrime, a multi-faceted approach is needed, involving collaboration between government agencies, law enforcement, private sector organizations, and the public. This includes investing in cybersecurity infrastructure, improving awareness and education programs, and strengthening legal frameworks to prosecute cybercriminals and protect victims. These efforts led to a 55% reduction in the number of cybercrimes in Kenya by the end of 2023 (Mwangi, 2023).

In a nutshell, cybercrime is a growing threat in Kenya, with a wide range of offenses including phishing, online fraud, cyberbullying, hacking, and malware attacks. These crimes have serious consequences for individuals, businesses, and the economy, leading to financial losses, emotional distress, and damage to reputation. To address this challenge, the government, law enforcement agencies, and private sector organizations must work together to strengthen cybersecurity measures, raise awareness among the public, and prosecute cybercriminals effectively. By taking a proactive and collaborative approach, Kenya can better protect itself from the growing threat of cybercrime and ensure a safe and secure online environment for all.

**Technological Developments and Innovations**

Technological advancements and innovations have revolutionized our interactions with the world. With the emergence of the internet, mobile devices, and social media platforms, connecting with others, sharing information, and conducting business online has become more accessible. Kenya stands out as the ICT hub of the East African region (International Trade Authority, 2023). Nevertheless, these advancements have also introduced new avenues for cybercriminals to exploit vulnerabilities within digital systems and networks.

One of the key technological developments that have influenced the rise of cybercrime in the Juja Sub-County is the proliferation of mobile devices. According to the World Bank, Kenya's ICT sector has grown by over 10.8% since 2016 (World Bank Group , 2019). Over 10 years ago, very few Kenyans had access to Android phones, but almost 85% of the people can now access these devices and about 80% of the country has access to a 3G network (Ngila, 2020). With the increasing popularity of smartphones and tablets, more people are accessing the internet and conducting transactions online. In 2010, internet penetration in Kenya was 9.7%, this has grown to over 89.7% in less than 15 years. There has also been a rise in fintech and other technologies within the past decade. Content consumption and other uses of technology such as online taxis, as well as e-commerce development are major developments in the technology sector. This has made

it easier for cybercriminals to target individuals and organizations through phishing scams, malware attacks, and other forms of cybercrime.

Another important technological development is the rise of social media platforms. Research shows that approximately 22.5 Million Kenyans had access to the internet in 2023 and the number is projected to increase to 39 million Kenyans by the year 2028 (Cowling, 2022). While these platforms have revolutionized the way we communicate and share information, they have also become breeding grounds for cybercriminals. Social media users are often targeted by scammers who use fake profiles and phishing emails to steal personal information and financial data. Moreover, the growth of e-commerce and online banking has created new opportunities for cybercriminals to carry out fraud and identity theft. With more people shopping and banking online, cybercriminals have developed sophisticated techniques to steal sensitive information and exploit vulnerabilities in digital payment systems.

**Technological Developments and Cybercrime in Kenya**

Technological developments have had a significant impact on cybercrimes in Kenya, as they have provided both opportunities for criminals to exploit and tools for law enforcement agencies to combat these crimes. Ngujiri(2022) noted that before technology developed the world's only threats were those from physical threats. People had to physically rob banks to steal and criminals had to engage in crimes by being at the actual scenes of crime.

One of the key effects of technological developments on cybercrimes in Kenya is the increasing sophistication of cybercriminals. The sophistication of cybercrimes has been increasing with an increase in technology. In the late 20$^{th}$ century, the cases of cybercrimes were low, however, as technology keeps advancing, so does the sophistication of cybercriminals (Ojedokun, 2005). As technology advances, cybercriminals can develop more complex and sophisticated methods of carrying out their illegal activities. The Business Daily newspaper in 2021 recorded that as internet usage in Kenya increased, cybercrime increased by 37% (Onyando, 2021). These advancements encompass sophisticated malware, phishing scams, and other tactics employed by cybercriminals to pilfer sensitive information, including financial data and personal details. Such advancements pose challenges for law enforcement agencies, as criminals continually adapt their tactics to outpace authorities, making it more arduous to detect and prevent cybercrimes.

Technological developments have also led to the increasing prevalence of online fraud and identity theft. With the rise of e-commerce and online banking, more and more Kenyans are conducting financial transactions online, making them vulnerable to cybercriminals who seek to steal their personal and financial information. Since the onset of the use of mobile money, over 30% of the users, approximately 5 Million accounts have been victims of theft and fraud (Sunday , 2020). Consequently, there has been a surge in cases of identity theft, wherein perpetrators utilize pilfered information to initiate fraudulent accounts or unauthorized transactions. The convenience and anonymity afforded by the internet facilitate cybercriminals in perpetrating these offenses, posinga substantial threat to individuals and enterprises in Kenya.

Furthermore, technological developments have also facilitated the spread of cybercrimes across borders. The proliferation of the internet and digital communication has empowered cybercriminals to operate from any location globally, rendering it challenging for law enforcement agencies to trace and apprehend them. Consequently, there has been a surge in transnational cybercrimes, encompassing online scams and cyberattacks, which can have profound repercussions for individuals and enterprises in Kenya. The global nature of cybercrimes presents a challenge for authorities, as they must work together with international partners to combat these crimes effectively.

In response to the growing threat of cybercrimes in Kenya, law enforcement agencies and government authorities have implemented various strategies to address the issue. One of the key strategies is the establishment of specialized cybercrime units within the police force, tasked with investigating and prosecuting cybercrimes. These units are equipped with the latest technology and training to combat cybercrimes effectively, including forensic tools to analyze digital evidence and track down cybercriminals. Additionally, the government has enacted legislation to criminalize cybercrimes and provide a legal framework for prosecuting offenders.

Another strategy being employed to combat cybercrimes in Kenya is the promotion of cybersecurity awareness and education. The government, in collaboration with private sector partners, has launched campaigns to educate the public about the risks of cybercrimes and how to protect themselves online. This includes providing tips on how to create strong passwords, avoid phishing scams, and secure personal information online. By raising awareness about cybersecurity

issues, the government aims to empower individuals and businesses to protect themselves from cybercrimes and reduce their vulnerability to online threats.

Furthermore, the government has also partnered with international organizations and law enforcement agencies to enhance cybersecurity capabilities in Kenya (KNA, 2023) This includes sharing information and intelligence on cyber threats, conducting joint investigations, and providing training and technical assistance to strengthen cybersecurity defenses. By collaborating with international partners, Kenya can leverage their expertise and resources to combat cybercrimes more effectively and protect its citizens from online threats.

Technological developments have had a significant impact on cybercrimes in Kenya, presenting both challenges and opportunities for law enforcement agencies and government authorities. While the increasing sophistication of cybercriminals and the prevalence of online fraud pose significant threats to individuals and businesses in Kenya, the government is taking proactive steps to address these issues. By establishing specialized cybercrime units, promoting cybersecurity awareness, and collaborating with international partners, Kenya is working to strengthen its cybersecurity defenses and combat cybercrimes effectively. However, the evolving nature of technology and the global reach of cybercrimes require a coordinated and multi-faceted approach to address these challenges effectively. By continuing to invest in cybersecurity capabilities and partnerships, Kenya can better protect its citizens and businesses from the growing threat of cybercrimes in the digital age.

**The Influence of Technological Developments on Cybercrime in Juja Sub-County**

The influence of technological developments on cybercrime in Juja Sub-County can be seen in the increasing number of cyberattacks and data breaches reported in recent years. According to a report by the Communications Authority of Kenya (2024), cybercrime incidents in Kenya have been on the rise, with a significant number of cases reported in Juja Sub-County.

One of the main factors driving the rise of cybercrime in Juja Sub-County is the lack of awareness and education about cybersecurity (KNA, 2023). Many individuals and organizations in the region are not adequately informed about the risks and threats posed by cybercriminals, making themmore vulnerable to attacks. In addition, the rapid pace of technological advancements has made it difficult for law enforcement agencies and cybersecurity experts to keep up with the evolving tactics and techniques used by cybercriminals.

The surge of cybercrime in Juja Sub-County is exacerbated by the absence of adequate cybersecurity measures and infrastructure. Many businesses and government entities lack robust protocols, rendering them vulnerable to cyber intrusions and data theft. Moreover, the prohibitive costs of cybersecurity solutions and the scarcity of skilled professionals in the field present significant challenges for organizations seeking to bolster their defenses against cyber threats.

Additionally, the ubiquity of social media platforms and online communication channels provides cybercriminals with ample opportunities to target individuals and entities in the Juja Sub-County. Scammers often employ social engineering tactics to deceive people into disclosing personal information or clicking on malicious links, resulting in data breaches and financial harm.

**Conclusion**

Technological developments and innovations have had a profound impact on the rise of cybercrime in the Juja Sub-County. The surge in mobile devices, social media platforms, and online communication channels has opened up new avenues for cybercriminals to exploit vulnerabilities and target individuals and organizations in the region. To counter this escalating threat, it is imperative to heighten awareness about cybersecurity risks, allocate resources toward cybersecurity infrastructure, and cultivate collaboration among stakeholders. By adopting a proactive and comprehensive strategy, Juja Sub-County can bolster its defenses against cybercrime and safeguard its residents and businesses from digital threats.

**Recommendations**

**Potential Solutions to Address Cybercrime in Juja Sub-County**

- To effectively address the rise of cybercrime in the Juja Sub-County, a tailored and comprehensive approach is essential, integrating technological solutions, educational initiatives, and collaborative efforts among stakeholders. One key strategy is to heighten awareness about cybersecurity risks and best practices specifically tailored to the local community. This can be achieved through targeted public awareness campaigns, specialized workshops, and training programs aimed at educating individuals and organizations in the region about the importance of safeguarding their personal information and digital assets.
- Moreover, it is critical to allocate resources towards strengthening cybersecurity infrastructure within the Juja Sub-County. This involves investing in localized solutions

such as firewalls, antivirus software, and encryption tools to fortify defenses against cyber threats tailored to the unique needs of the community. Additionally, conducting regular security audits and penetration testing exercises within local organizations can help identify and address vulnerabilities in their networks, enhancing overall cybersecurity posture.

- Furthermore, fostering collaboration among local government agencies, law enforcement authorities, and cybersecurity experts is paramount in combating cybercrime effectively. By facilitating information-sharing and resource pooling, stakeholders such as the county commissioner and the Ministry of Interior can work together to investigate cyberattacks, track down cybercriminals operating within the region, and prosecute offenders. Additionally, forging partnerships with international organizations and cybersecurity firms can provide access to advanced technologies and expertise, further enhancing the Juja Sub-County's cybersecurity capabilities in line with its specific challenges and requirements.

**References**

Bellasio, J., & Silfversten, E. (2023). The impact of new and emerging technologies on the cyber threat. *Kings College London*.

Cowling, N. (2022). Social Media in Kenya. *Statista*.

Dulock, H. L. (1993). Research Design: Descriptive research . *Journal of Pediatric Oncology Nursing*, 10(4),154-157.

Government of Kenya. (2018). The Computer Misuse and Cybercrimes Act. *Government of Kenya Printers*.

Government of Kenya. (2024). Communication Authority of Kenya. *Government Printers*.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, A., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business&Economics,3(5)*.

International Trade Authority. (2023). Kenya-Information, Communications, and Technology(ICT). *International Trade Administration*.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials, 15(4), 2091-2121*.

KNA. (2023). Government to strengthen cybersecurity measures and combat cybercrime. *Kenya News Agency*.

Lawi, J. (2023). Cybercrime is on the rise as Kenya faces 1 million threats every day. *The Star newspaper*.

Maurer, T., & Nelson, A. (2021). The global cyber threat to financial systems. *IMF Finance and Development*.

Musau, D. (2024). Kenya was hit by a record 860 million cyber-attacks in 2023. *Citizen Digital*.

Mwangi, K. (2023). Kenya cyber-attacks down 55pc on awareness drives, digital signatures. *Business Daily Africa.*

Ngila, F. (2020). How technology changed the lives of Kenyans in the past 10 years. *Business Daily Africa Newspaper*.

Ngujiri, N. (2022). Technological Developments Influence the Cybercrime in Juja Sub-County. *University of Nairobi.Research week presentation.*

Njuguna, D., Kamau, J., & Kaburu, D. (2021). Model for mitigating smishing attacks on mobile platforms. *In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE*.

Ojedokun, A. A. (2005). The evolving sophistication of internet abuses in Africa. *The International Information & Library Review*, 37(1), pp.11-17.

Onyando, W. (2021). Cybercrimes Surge by 37pc as usage of the internet increases. *Business Daily Africa Newspaper*.

Patton, M. Q. (2005). Qualitative research. *Encyclopedia of Statistics in Behavioral Science*.

Petrosyan, A. (2023). Concerns regarding cyberattacks worldwide. *Statista*.

Rick, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2),261-273.

Rogers, E. M. (1962). Diffusion of innovations. *New York.*

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*, 34(1),8-12.

Sunday, F. (2020). Phone Users losing millions through identity theft. *The Standard Newspaper*.

World Bank Group. (2019). Kenyan economic update: Accelerating Kenya's Digital Economy. *World Bank*.

# The Rise of State-Sponsored Cyber-attacks: The Case for International Cooperation in Strengthening Defence Systems

*By*

*C.A. Mumma-Martinon, Lucy W. Maina and James J. Kimuyu*

**Abstract**

The recent years have seen an increase in state sponsored acts of cyber-attacks that are becoming increasingly sophisticated. These attacks mainly target nation's critical infrastructure such as communication systems, electricity generation and distribution systems, transportation systems, health support systems and financial services whose collapse and unavailability can lead to partial or total collapse with huge reputation, economic, security and political implications. As organizations and nations grapple with the challenges posed by increasingly sophisticated cyber threats, it is imperative to examine how current cybersecurity strategies are responding to them and if these responses are adequate. Failure to address these challenges portends exposing critical infrastructure, sensitive data, and national security interests to unprecedented levels of danger and disruption. This study therefore seeks to analyze the rise of state-sponsored cyber-attacks and its significance lies in assessing how nations can enhance these capabilities; foster international cooperation and collaboration and strengthen cyber resilience and incident response preparedness. The study has adopted a mixed-methods research design to triangulate data from various documented sources and provide a comprehensive understanding of state-sponsored cyber threatsand cybersecurity strategies. It also provides recommendations such as robust governance structures, increasing investments, strengthening partnerships with allies and international organizations, information sharing and analysis centres, integrate robust incident response, development and training programmes, continuous monitoring and evaluation and eventually further research to be done.

**Keywords:** *cyber-attacks, state-sponsored, defence systems, international relations, national security.*

## Introduction

In recent years, there has been significant increase in the frequency and sophistication of state-sponsored cyberattacks targeting nations' critical infrastructure and sensitive government systems.

There was a 63% increase in state-sponsored cyberattacks globally in the past year alone. These attacks have ranged from espionage efforts aimed at stealing classified information to disruptive operations targeting essential services such as energy, healthcare and finance. (Crowdstrike, 2024). Despite heightened awareness and investment in counter cybersecurity measures, nations worldwide are grappling with substantial challenges in effectively mitigating the threats posed by state-sponsored cyberattacks. According to Verizon, 85% of data breaches involved human elements, (Verizon, 2023). This statistic underscores the increasingly sophisticated social engineering tactics employed by state actors, who leverage psychological manipulation and deception to exploit individuals within target organizations.

Moreover, the global shift towards remote work induced by the Coronairus-19 (COVID-19) pandemic has further exacerbated cybersecurity vulnerabilities on a massive scale. With remote work becoming the new norm, organizations have had to rapidly deploy technologies and infrastructure to support remote operations, often without adequate security measures in place. This hasty transition created fertile ground for cybercriminals, with the coming in of the new norm, there was a staggering 600% increase in phishing attacks targeting remote workers (Anti-Phishing Working Group, 2020).

This study therefore seeks to analyze the rise of state-sponsored cyber-attacks and its significance lies in assessing how nations can enhance these capabilities; foster international cooperation and collaboration and strengthen cyber resilience and incident response preparedness.

**Theoretical framework**

The theoretical underpinnings that guide the analysis of cybersecurity and cyber warfare and the role of states as perpetrators heavily borrows from both the Realist and Deterrence Theories. From a realist perspective rooted in international relations theory, cybersecurity and cyber warfare may be seen through the lens of power politics and state-centric behaviour, (Waltz, 1979). Accordingly, states are rational actors driven by the pursuit of power and security in an anarchic international system, (Mearsheimer, 2014). In the context of cybersecurity, this perspective informs on the role of states as primary actors in perpetrating cyberattacks and defending themselves against cyber threats and attacks to safeguard their national interests, (Libicki, 2014). Interpreted, empirical evidence supports this perspective as state-sponsored cyber espionage campaigns targeting rival nations and government networks are aimed at retaining sovereignty and gaining advantage and

power. Moreover, the proliferation of offensive cyber capabilities by states, such as the development of cyber weapons and the establishment of military cyber commands, underscores the realist notion of states prioritizing their strategic advantage in cyberspace over each other, (Arquilla & David, 1993).

The Deterrence theory adapted and applied by Libicki, (2009) provides further insights complementing the realist view. From this perspective, deterrence seeks to weaken the effects of cyberattacks to a minimal level at an acceptable cost. The state seeks to deter adversaries from engaging in malicious cyber activities through the credible threat of retaliation or punishment (Schelling, 1980). Studies have explored the effectiveness of deterrence strategies in the cyber domain, examining case studies of state responses to cyberattacks and their impact on adversarie" behaviour. States intentionally mount a cyber-attack for the sole purpose of displaying their capabilities to reduce the likelihood of being under attack (National Research Council, 2010).

Additionally, empirical data on state-sponsored cyber operations and responses, such as the attribution of cyberattacks and public condemnation by victim states, provide insights into the dynamics of cyber deterrence in practice (Nye, 2011). The two theories thus provide ground for analysing motivations by state to cyber-attack as well as the use of attacks to express their state power and safeguard their space. They also assist to analyse how states seek to influence the behaviour of adversaries through deterrence as contrasted with denial strategies that seek to improve technologies and processes to ensure low levels of success by attackers.

**Methodology**

This study has used a mixed-methods research design to triangulate data from various documented sources and provide a comprehensive understanding of state-sponsored cyber threatsand cybersecurity strategies, (Creswell & Creswell, 2017). Multiple data bases and information sources were used from which data was extracted and analysed qualitatively and quantitatively. Additionally, some data were re-analysed to explore state behaviour in cyberspace, the role of power dynamics in shaping cybersecurity policies and the effectiveness of strategies that are in place to counter cyber threats. The research design allowed mining and analyzing empirical data on cyber incidents, such as data breaches and cyberattacks attributed to state actors, to identify trends and patterns that align with the theoretical frameworks provided.

Data sources for the study included official government documents, academic literature, cybersecurity reports, and empirical datasets on cyber incidents. These were accessed from reputable sources such as government agencies, cybersecurity firms, tech company records and academic institutions. The data were then coded and categorized to extract insights into the topic including the motivations behind state-sponsored cyberattacks and the efficacy of cybersecurity deterrence strategies. By triangulating qualitative and quantitative data through thematic analysis and statistical analysis, this study provided a nuanced understanding of state-sponsored cyber threats, (Bhandari, 2023).

**Empirical Literature**

This section analyses from empirical literature in terms of: forms of cyber-attacks; evolution and trends in cyber threats; state-sponsored cyberattacks: nature and characteristics; impact on national security and critical infrastructure; current cybersecurity enhancing strategies and frameworks and challenges and shortcomings in countering cyber-attacks.

**Forms of cyber-attacks**

There are various Tactics, Techniques and Procedures (TTPs) employed by malicious actors in the cyberspace that have been adopted by states who engage in cyberwarfare. One of the most common forms of attack is known as phishing a**nd involv**es gaining unauthorized access to target networks. According to Verizon, (2020), 22% of data breaches involved phishing attacks, highlighting the effectiveness of this social engineering technique in compromising user credentials and delivering malware payloads. In this type of attack, once the hacker accesses the network, they hibernate for certain period of time, to avoid immediate correlations by security policies and detection. The hackers then conduct internal reconnaissance activities to locate critical servers or applications from which to steal confidential data, then gains access using privileged escalations, brute force methods or other mechanisms and performs data exfiltration to send the stolen data to external servers (Abad, 2005; Aburrous *et al.,* 2008; Bin, Qiaoyan and Xiaoying, 2010).

On the other hand, ransomware attacks have become more popular today. This is due to the fact that hackers can quickly gain financial benefits from the victim organizations by encrypting their data and files needed for normal business activities. The hackers then demand ransom payments in exchange for decryption keys. In most cases, businesses pay the ransom to get the locked data

restored and continue with normal business, (Kapoor *et al.,* 2021; Kaur, Dhir & Singh, 2017; Maurya *et al.,* 2018).

The use of Distributed Denial of Service Attack (DDOS) has also gained prominence in the recent past. This type of attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic (Douligeris & Mitrokotsa, 2004; Tayyab, Belaton & Anbar, 2020; Vishwakarma & Jain, 2020). DDOS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic (Huang *et al*., 2020; Nooribakhsh & Mollamotalebi, 2020). DDOS attack can be likened to an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination, thus denying the rightful users the right to use the systems. In response, most organisations end up pulling down the affected ICT System, effectively enabling the attackers achieve their intended purposes.

Data theft, leakages, illegal access and disgruntled employees continue to pose a significant threat to governments and organisations. Despite the good intention, the manner in which the data and information is obtained breaches internal security and confidentiality requirements. Another method of attack is the Zero-Day Exploits which exploits previously unknown vulnerabilities in software and hardware systems (Khandelwal, 2019). For instance, the Stuxnet worm, attributed to state-sponsored actors, leveraged multiple zero-day exploits to target Iran's nuclear enrichment facilities, demonstrating the sophistication of offensive cyber operations (Zetter, 2011). Water holing is another strategy involving the setting up of a fake website or compromising authentic sites for the purpose of exploiting users.

**Evolution and Trends in Cyber Threats**

The evolution and magnitude of cyber security attacks have been extensively documented through empirical studies, showcasing a trajectory marked by increasing frequency and sophistication. Studies have documented the evolution of cyber threats over time, illustrating the increasing frequency and sophistication of cyberattacks, (Böhme & Stefan, 2009). There is a steady rise in the number of cyber threats detected each year, with a 56% increase in new malware variants in 2020 compared to the previous year, (Symantec, 2021). This surge underscores the relentless

innovation of cybercriminals, who continually adapt their tactics to bypass traditional security measures. Cybercrime damages would cost the world $6 trillion annually by 2021, demonstrating the escalating financial impact of cyber threats, (Computer Crime Ventures, 2021).

**State-Sponsored Cyberattacks: Nature and Characteristics**

State sponsored cyberattacks have been identified as the most pervasive and diverse with ramifications being quite serious and long-lasting (Thomas & Buchanan, 2015). Espionage, sabotage and influence operations are the primary objectives of state-sponsored cyberattacks (Cyber Threat Alliance, 2020). Moreover, the "MITRE ATT&CK Framework" provides empirical data on the TTPs commonly employed by state actors, including phishing, malware deployment, and exploitation of software vulnerabilities (The MITRE Corporation, 2020).

Reports indicate that Ukraine has experienced numerous state-sponsored cyberattacks the most notable incident being the 2017 *NotPetya* cyberattack, which targeted Ukrainian infrastructure but spread globally, causing billions of dollars in damages to businesses worldwide. This attack, widely attributed to Russia, disrupted critical services in Ukraine, including banks, airports, and government agencies. Another case is that of Iran whereby in 2010, the Stuxnet worm believed to have been developed by the United States and Israel, targeted Iran's nuclear facilities, causing significant damage to its uranium enrichment program. In retaliation, Iran launched cyberattacks against various targets, including U.S. financial institutions and critical infrastructure. Additionally, South Korea has on several occasions faced state-sponsored cyberattacks from North Korea, aimed at disrupting government operations and undermining national security (Feigenbaum & Nelson, 2021). One notable incident is the 2014 cyberattack on Sony Pictures Entertainment, attributed to North Korea, which resulted in the leak of sensitive corporate data and the cancellation of the release of a controversial film (Feigenbaum & Nelson 2021).

The SolarWinds cyberattack, attributed to Russian state-sponsored actors, involved compromising the software supply chain of SolarWinds, a prominent IT management software provider. According to reports from cybersecurity firms such as Fire Eye and CrowdStrike, the attackers inserted malicious code into SolarWinds' Orion software updates, which were then distributed to thousands of organizations, including government agencies and Fortune 500 companies

(Kaspersky Lab, 2021). This sophisticated supply chain attack resulted in unauthorized access to sensitive data and networks further demonstrating the extent of the threat posed by state-sponsored actors to global cybersecurity.

In Kenya, 2023 was a turning point within the Cybersecurity domain. The country faced a massive DDOS attack on the critical eCitizen platform and other critical infrastructure entities rendering the System inaccessible. The attack attributed to the hacktivist group "*Anonymous Sudan*," originated from various international locations. Its intent and motivations remain unclear, but the incident highlighted the potential for severe economic and security implications for the country and led to loss of revenue due to the ongoing digitization of government services while at the same time affecting delivery of crucial government services, (Mwai & Nkonge, 2023).

**Impact on National Security and Critical Infrastructure**

The most notable characteristic of cyber-attack is the surprise element that it is associated with. Unlike conventional warfare where the threat is known way before an actual attack, cyber-attacks are asymmetrical and at times executed without warning or prior signs. They therefore present great anxiety and are associated with great magnitude of loss or damage. In this regard evidence on cyber espionage from cybersecurity firms, government agencies, and intelligence reports document the pervasive threat of state-sponsored cyber espionage to national security and intelligence interests. For example, the Chinese state-sponsored hackers that targeted the USA jeopardized intellectual property and trade secrets provides empirical data on the scope and scale of such operations (U.S. Department of Justice, 2020).

**Cyber-attacks have the capability to cause massive disruption of critical infrastructure** such as energy, transportation, and healthcare systems. They have the potential to disrupt government operations that are delivered through online platforms. The 2021 Cybersecurity Insights Report by the International Business Machines (IBM) highlights the increasing frequency of cyberattacks targeting critical infrastructure, with 59% of surveyed organizations reporting a rise in such incidents. Reports from incident response investigations and forensic analysis of cyber incidents provide insights into the tactics and techniques used by state-sponsored actors to disrupt essential services and undermine national security (IBM Security, 2021).

***Current Cybersecurity Enhancing Strategies and Frameworks***

Comparing strategies is often complicated venture given the nature of attack is a confounding variable in many of the cases. According to McLean, (2017), traditional perimeter-based defences remain prevalent, they are insufficient in addressing the evolving tactics of cyber adversaries. Perimeter-based defenses fail to detect and mitigate insider threats or advanced persistent threats that bypass perimeter defences through techniques like social engineering or zero-day exploits, (McLean, 2017).

The Cybersecurity Framework was developed by the National Institute of Standards and Technology (NIST) and is widely recognized and adopted framework for improving cybersecurity risk management. The framework provides a flexible and customizable approach to managing cybersecurity risks, offering guidance on identifying, protecting, detecting, responding to and recovering from cyber threats. Organizations can use the NIST Cybersecurity Framework to assess their current cybersecurity practices, identify gaps, and prioritize investments to improve their overall cybersecurity resilience, (NIST, 2024).

**S**tudies have identified several challenges and gaps in cybersecurity defence mechanisms that hinder effective cyber threat mitigation (Dhillon & Sushil, 2015). There is shortage of skilled cybersecurity professionals as a significant challenge faced by organizations worldwide, with 61% of surveyed companies reporting a shortage of cybersecurity expertise, (IBM Security, 2021). Moreover, only 38% of organizations have a formal cybersecurity strategy in place, indicating a gap in strategic planning and implementation, (PwC, 2021). The shortage of skilled professionals hampers organizations' ability to effectively defend against cyber threats, as they may lack the necessary talent to develop and implement robust security measures, monitor systems for potential breaches, and respond to cyber incidents in a timely manner. Without a comprehensive strategy, organizations may struggle to prioritize cybersecurity investments, align security initiatives with business objectives, and effectively coordinate cybersecurity efforts across departments and stakeholders. This lack of strategic planning leaves organizations vulnerable to cyber threats and increases the likelihood of security breaches.

While different nations have adopted varied approaches and strategies for ensuring cyber security, there is an evolving culture of best practices that arise from the works of cyber security firms and tech companies in the USA and Europe. The US for instance has in place the Cybersecurity and Infrastructure Security Agency (CISA) which regularly publishes reports and assessments of national cybersecurity policies and initiatives. The country's cybersecurity strategy and implementation plan provide an overview of the U.S. government's approach to cybersecurity, including priorities, goals, and action plans. Additionally, the National Cyber Strategy outlines strategic objectives and initiatives aimed at enhancing cybersecurity resilience and combating cyber threats. On the other hand, the European Union Agency for Cybersecurity (ENISA) produces empirical data on national cybersecurity policies and initiatives across the EU member states indicating a modicum of international cooperation. The Annual Cyber Security Strategy Reports assess the implementation of national cybersecurity strategies and highlight best practices and areas for improvement. Furthermore, the EU Cybersecurity Strategy outlines policy objectives and legislative initiatives to strengthen cybersecurity cooperation and resilience at the European Union level, (European Commission, 2022).

The African continent action on cyber security has been slow and the continent lags behind in governance, laws and regulations, technical capacity, research and development, training among others. However, countries such as South Africa, Nigeria, Ghana and Kenya have made some strides in putting up Cybersecurity structures and in the development of a Cybersecurity posture for a more secure cyberspace. For instance, Kenya's **Cybersecurity Posture** is exemplified by the National Computer and Cybercrimes Coordination Committee (NC4), the Communications Authority of Kenya (CA) and the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) who work jointly to coordinate cybersecurity efforts and response to cyber incidents.

Kenya also has in place several policies and frameworks to guide its cybersecurity initiatives including the Computer Misuse and Cybercrimes Act (CMCA), 2018, the Kenya Information and Communications Act (KICA), 1998 and the Data Protection Act of 2019 which provide legal frameworks for cybersecurity and data protection. Additionally, the National Cybersecurity Strategy, 2022 – 2027 and the CMCA, 2018 Regulations, provide a roadmap for improving

cybersecurity resilience and enhancing coordination among stakeholders. The implementation of these strategies is incumbent upon capacity building, public-private collaboration and adequate funding for cybersecurity initiatives to counter the evolving nature of cyber threats.

**Challenges and Shortcomings in Countering Cyber-attacks**

This section incorporates attribution challenges, sophistication of tactics, skill shortage, under-investment in cyber resilience and implications for national security and international cooperation in strengthening defence systems.

**Attribution Challenges**

Empirical data from cybersecurity incident response and forensic investigations reveal the difficulties in accurately attributing cyberattacks to state-sponsored actors. According to Fire Eye, (2020), the complexity of attribution due to the use of false flag tactics, proxy servers and encrypted communications by malicious actors. This evidence underscores the challenge of holding state actors accountable for cyber aggression and enforcing consequences. Attackers can deliberately manipulate digital evidence to make it appear as though the cyberattack originated from a different source than the actual perpetrator. This deceptive technique complicates attribution efforts at times leading investigators to attribute the attack to the wrong entity based on false information, highlighting the challenge of accurately identifying state-sponsored actors behind cyberattacks, (Fire Eye, 2020).

**Sophistication of Tactics**

Analysis of cyber incidents attributed to state-sponsored actors demonstrates the increasing sophistication of their tactics and techniques. The MITRE ATT&CK Framework provides data on the use of Advanced Persistent Threats (APTs) by state actors, including reconnaissance, lateral movement and data exfiltration techniques, (The MITRE Corporation, 2020). This empirical evidence illustrates the evolving nature of cyber threats and the challenge of defending against state-sponsored cyber aggression using traditional cybersecurity approaches.

**Skill shortage**

Skill shortage is another challenge in countering cyber-attacks. Skilled cybersecurity professionalsis a significant gap in current cybersecurity approaches. ISC2 Cybersecurity Workforce Study,

(2023), found that the global shortage of cybersecurity professionals reached 3.1 million in 2020, representing a 63% increase since 2019. The United States faced a shortage of over 500,000 cybersecurity professionals in 2020. Similarly, the United Kingdom faced a shortage of over 140,000 cybersecurity professionals in the same year. This shortage has been exacerbated by factors such as the increasing demand for cybersecurity expertise across various sectors, the prevalence of cyber threats targeting states and the poaching of professionals to work remotely from across the globe. This shortage is further exacerbated by the rapid growth of cyber threats, the evolving nature of cybersecurity technologies, and the lack of adequate cybersecurity education and training programs (ISC2 Cybersecurity Workforce Study, 2023).

**Under-investment in Cyber Resilience**

The analysis of cybersecurity budgets and expenditures reveals a gap in investment in cyber resilience measures, such as incident response planning and cyber insurance. Surprisingly, only 35% of organizations have a dedicated cyber resilience budget, with the majority of cybersecurity spending focused on prevention and detection capabilities, (European Commission, 2022). While this challenge is most often felt in developing countries, it also affects big economies. Germanyhas been cited to have gaps in investment in cyber resilience and that a significant cyber security spending is allocated to prevention and detection capabilities and less on response and insurance. Australia has many organizations focusing their cybersecurity spending on prevention and detection capabilities at the expense of other areas. This evidence suggests a need for organizations to prioritize investments in cyber resilience to mitigate the impact of cyber incidents and enhance overall cybersecurity posture, (European Commission, 2022).

**Implications for National Security and International Cooperation in Strengthening Defence Systems**

Cyber security is inextricably connected to global security and therefore attracts the attention to international relations. The International Telecommunication Union (ITU) highlights the correlation between geopolitical tensions and cyber threat activity, with state-sponsored actors targeting adversaries' critical infrastructure and strategic assets. State-sponsored cyber operations are aimed at advancing geopolitical interests and often target military organizations, government systems, financial and foreign governments. Often, such attacks are used to generate revenue,

gather intelligence, and or exert influence on the international stage. Attacks such as those advanced by Iran and North Korea among others highlight the complex interplay between state's regional and global geopolitical strategies.

Despite the nature and character of cyber security as a global threat, the normative framework underpinning counter measures reflect gaps and ambiguities. One of the most visited section of international law applicable to cyber operations is the Talinn Manual 2.0 seeking to regulate state behaviour on the cyberspace and mitigate the risk of conflict escalation. In implementing cyber security laws, nations have to grapple with definition of what can be considered acceptable behaviour in cyberspace, as informed by analysis of international agreements and norms.

Additionally, and as observed elsewhere in this study, cyberattacks attribution can be challenging due to the complexities of cyber operations and the ability of attackers to obfuscate their identities. In a case such as that of the Stuxnet attack by the US and Israel targeting Iranian nuclear programme, while the attack is associated with specific actors, the challenges of attribution persist due to the covert nature of cyber operations and the use of advanced obfuscation techniques. This particular attack raised the significant question about the applicability of existing international law to cyberspace. The same case was observed regarding the *WannaCry* attack to the North Korean state-sponsored cyber group known as Lazarus Group. This incident in particular highlighted the urgent need for international cooperation and coordination to address cyber threats effectively. Despite widespread condemnation of the attack and calls for collective action to enhance cyber security, efforts to achieve collective cyber security have been minimal. However, achieving consensus on these issues requires ongoing dialogue and collaboration among governments, international organizations and other stakeholders.

Lastly, the characteristics of cyberattacks are such that no nation can claim to have total safeguards against it. Even when safeguards are in place, cyber-attacks take the form of *moving target* and every safeguard is only valid for a short time while prediction of likely threats can never be totally accurate. Analysis of global cybersecurity trends and threat intelligence data reveals the dynamic and evolving nature of the cyber threat landscape. There is increasing frequency and sophistication of cyberattacks, with state-sponsored actors posing significant challenges to national security and critical infrastructure. This underscores the urgency for nations to collaborate and innovate in

enhancing cybersecurity capabilities to address emerging threats effectively, (IBM Security, 2021).

Additionally, cybersecurity incident reports and economic impact assessments highlight the significant financial and reputational costs of cyberattacks for nations and organizations. For example, the 2020 report on Cost of a Data Breach by the IBM and the Ponemon Institute estimates that the average cost of a data breach is $3.86 million, with higher costs associated with state-sponsored cyber incidents. This further underscores the imperative for nations to pool together to strengthen their cybersecurity defences to mitigate the impact of cyber threats and protect national interests. (IBM Security, 2021).

**Conclusion**

This study has carefully examined case studies of cyber-attack incidents, their typologies and evolving nature and characteristics. It further analyses impacts of cyber-attacks on national security and infrastructure and the strategies that states have adopted to counter them providing a comprehensive critique on why these strategies and frameworks have failed in the face of modifying and increasing sophistication characterising present day attacks. Clearly, there are challenges further undermining cyber security such as attribution dilemma, greater sophisticating that affords more anonymity to aggressors, skill shortages and under-investment in cyber security emerging from the study. The Realist and Deterrence theories provided vital analytical lenses that aided not only the analysis of drivers of cyber-attacks but allowed an examination of gaps in strategies adopted by nations to counter them. Against the backdrop of identified challenges and shortcomings, the paper delved into the strengths of existing cybersecurity capabilities and strategies and the great opportunity for cooperation in counteracting cyber-attacks.

**Recommendations**

- **Elect Robust Governance Structures**

  Lessons emerging from the study attest that there is a need for states to put in place robust governance structures to manage their national cyberspace. This should go hand in hand with continually developing articulate cyber deterrence policies, laws and regulations to anchor cybersecurity and cyber warfare operations. It is not sufficient for countries to have their own

cyber security domestic laws which calls for the involvement of regional security mechanisms. These policies, laws and regulations should encompass diplomatic, economic, and military responses to cyber threats and attacks. There is evidence that clear cyber deterrence policies, laws and regulations alongside promoting international norms of responsible behaviour in cyberspace could ward-off adversaries. Additionally, efforts to bolster offensive cyber capabilities, including developing advanced cyber weapons and conducting cyber operations to dissuade adversaries from engaging in hostile cyber activities have great potential for success. Enforcing cybersecurity standards is crucial for maintaining trust, attracting investments, and safeguarding national economic interests.

- **Increasing Investments in Cyber Security**

  This is paramount and requires setting aside funding to continually audit and secure sectors such as telecommunications, finance and banking, government systems, energy, transportation, and healthcare which are often targeted. Such funding can incentivize organizations to invest in advanced cybersecurity measures thus strengthening their overall security posture. Additionally, the adoption of cyber insurance policies can help mitigate financial losses and facilitate recovery from cyber incidents. Businesses and organizations require to set aside critical funding to mitigate cyber threats, ultimately strengthening nations overall incident response capabilities.

- **Strengthening Partnerships With Allies and International Organizations**

  This will assist in coordination of deterrence efforts against state-sponsored cyber aggression has great potential and this should include sharing of information with partners, imposing collective consequences on aggressor states and building resilience. This should also go hand in hand with involvement and ratification of international cybersecurity and cybercrimes conventions such as the Budapest convention on cybercrimes by the Council of Europe and the Malabo conversion on Cybersecurity and personal data protection by the African Union (AU). Partnerships with international organizations such as the United Nations Office on Drugs and Crime (UNODC), the AU and the ITU to access empirical data, success case studies, and best practices in cybersecurity are an imperative.

- **Information sharing and analysis centres (ISACs)**

  This will enhance cybersecurity coordination and response capabilities which are imperative. This is tied to collaborative cybersecurity efforts to protect critical infrastructure. Establishing sector-specific ISACs facilitates real-time information sharing and coordinated responses to cyber threats and is tantamount to fostering a more resilient cybersecurity ecosystem. Establishing ISACs enhances the ability to detect and respond to cyber threats promptly, minimizing potential disruptions.

- **Integrate robust incident response**

  Like in other forms of enhancing security, cyber security strategies have to integrate robust incident response plans for effectively mitigating and responding to cyber incidents. By developing and regularly testing incident response plans at the national and sectoral levels, nations can ensure a coordinated and timely response to cyber incidents, minimizing their impact on critical infrastructure, government systems, and the economy.

- **Development and training programmes**

  Further, investing in cybersecurity workforce development and training programmes will go a long way in improving skills and expertise of incident response personnel, enabling them todetect, contain, and remediate cyber threats more effectively. This goes hand in hand withbuilding a resilient cybersecurity ecosystem and enhancing the country's ability to respond to cyber incidents.

  Due to underdevelopment of systems for mitigating cyber security in developing countries, there will be need to strengthen cybersecurity capacity-building efforts in and across these nations. Leaving behind a great majoring of populations will not achieve global cyber security since they may become the havens to launch attacks. Through technical assistance programs, systematic training and knowledge-sharing initiatives, advanced nations can collaborate with the not-so-endowed nations to help improve cybersecurity capabilities in these countries, promoting a more inclusive and resilient global cyber ecosystem. In response, developing countries should express their interest in securing their cyber space by investing in support infrastructure, offensive cyber capabilities and amplifying their deterrence efforts.

Due to the changing nature of cyber security, continuous research towards developing resilient technologies and defence mechanisms should be promoted. This will entail more engagement with private sector and academia**.** Collaborative efforts between government agencies, private companies, and academic institutions in sharing case studies, conducting joint research projects, and organizing workshops and seminars to disseminate best practices emerging from lessons in cybersecurity resilience should be encouraged. Such engagements will in addition provide valuable insights into global cybersecurity trends, emerging threats, and effective mitigation strategies, for incorporation into cybersecurity policies and practices.

- **Continuous monitoring and evaluation**

  These practices includes regular assessments will help identify gaps, measure progress and refine strategies. This ensures that efforts remain aligned with evolving cyber threats and organizational needs. This will also inform development of multi-layered defence Strategies which emerge from best practices to mitigate cyber risks effectively. From documented evidence, continuous monitoring and threat hunting has great potential to fall stall attacks underscoring the importance of proactive threat detection and response capabilities in enhancing cybersecurity resilience and minimizing the impact of cyber incidents.

- **Recommendations for Future Research**

  **F**uture research may delve into how countries can cooperate to develop advanced threat monitoring, detection, prevention and response techniques that may aid in mitigating such attacks. More research is needed towards attribution capabilities to accurately identify and correctly attribute state-sponsored cyberattacks. Secondly, as stated, there are gaps in policy, law and regulation development efforts. Future research and policy initiatives should leverage empirical evidence and stakeholder input to develop consensus-based norms and mechanisms for enforcing compliance to cyber space regulations.

## References

Abad, C. (2005). The economy of phishing: a survey of the operations of the phishing market. First Monday 10, 1–11. doi:10.5210/fm.v10i9.1272.

Aburrous, M., Hossain, M. A., Thabatah, F. and Dahal, K. (2008). Intelligent phishing website and reporting. International Journal of Security and Networks, 12(3), 188.

Anti-Phishing Working Group (2020). Phishing Activity Trend Report. 1st Quarter 2020 Plus COVID-19 Coverage. May 2020. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf?g

Arquilla, J. and David R. (1993). Cyberwar is coming!. Comparative Strategy 12.2 (1993): 141-165.

Bhandari, P. (2023, June 22). *Triangulation in Research | Guide, Types, Examples.* Scribbr. Retrieved May 18, 2024, from https://www.scribbr.com.

Bin, S., Qiaoyan, W. and Xiaoying, L. (2010). A DNS based anti-phishing approach. In second international conference on networks security, wireless communications and trusted computing, Wuhan, China, April 24–25, 2010. (IEEE), 262–265. doi:10.1109/NSWCTC.2010.196.

Böhme, R. and Stefan K. (2009). Models and Measures for Correlation in Cyber-Threat Defense. Proceedings of the 2009 ACM Workshop on Cyber Security (pp. 57-66). ACM, 2009).

Computer Crime Ventures (2021) Annual Cybercrime Report- 2021. Retrieved on 12th January 2024. Available at: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.

Creswell, J. W. and Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed Methods Approaches. Sage publications.

Crowdstrike Global Threat Report, (2024). Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report. Media contact. Timo Burbidge. timo.burbidge@uk.verizon.com.

Cyber Threat Alliance (2020). Cyber Threat Intelligence Estimate.

DBIR (2023). Data Breach Investigations Report 2023. Verizon 2021.

Dhillon, G. and Sushil, S. (2015). Cybersecurity in the Cloud: Risks and Strategies. Information Systems Frontiers 17.2 243-258.

Douligeris, C. and Mitrokotsa, A. (2004). DDOS attacks and defense mechanisms; classification and state-of-the-art. Compt. Netw. 2004, 44, 643–666.

European Commission (2022). European Cybersecurity Investment Platform. European Union.

Feigenbaum, E. A and Nelson, M. R. (2021). The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way. Carnegie Endowment For International Peace.

Fire Eye (2020). M-Trends 2020 Special Report. https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Huang, K., Yang, L.Y., Yang, X., Xiang, Y., Tang, Y.Y. (2020). A low-cost distributed denial-of-service attack architecture. IEEE Access 2020, 8, 42111–42119.

IBM Security (2021). Cybersecurity Insights Report. IBM, 2021.

ISC2 Cybersecurity Workforce Study (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. IS2.

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G. and Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: A review and Future Directions. Sustainability, 14(1), 8. https://doi.org/10.3390/su14010008.

Kaspersky Lab. (2021). Solarwinds Cyberattack: What We Know And What We're Doing To Learn More. Retrieved from https://www.kaspersky.com/blog/solarwinds-cyberattack/37932/

Kaur, G., Dhir, R. and Singh, M. (2017). Anatomy of ransomware malware: Detection, analysis.

Khandelwal, S. (2019). A Deep Dive into Zero-Day Vulnerabilities and Exploits. International Journal of Computer Applications, 180(40), 1-6.

Libicki, Martin C. (2009). Cyber-deterrence and Cyberwar. RAND Corporation, 2009.

Libicki, Martin C. (2014). Cyberspace is not a warfighting domain. Strategic Studies Quarterly 8.3 (2014): 34-65.

Maurya, A. K., Kumar, N., Agrawal, A. and Khan, R. A. (2018). Ransomware evolution, target and safety measures. International Journal of Computer Sciences and Engineering, 6(1), 80–85. https://doi.org/10.26438/ijcse/v6i1.8085

McLean, C. (2017). Beyond the perimeter: The need for early detection and response in the strategies of cybersecurity. Journal of Cybersecurity 3.1 (2017): 29-42.

Mearsheimer, J. (2014). The tragedy of great power politics. W.W Norton & Company, 2014.

Mwai, P. and Nkonge, A. (2023). *Kenya Cyber-Attack: Why is eCitizen down?* BBC World Africa. https://www.bbc.com/news/world-africa-66337573.

National Research Council (2010). *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*. National Academies Press.

NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0. Available at https://doi.org/10.6028/NIST.CSWP.29.

Nooribakhsh, M. and Mollamotalebi, M. (2020). A review on statistical approaches for anomaly detection in DDOS attacks. Information Security Journal. A Global Perspective. 29, 118–133.

Nye, Joseph S. (2011). Deterrence And Dissuasion In Cyberspace: Strategic Studies Quarterly 5.4 (2011): 38-55.

PwC (2021). The Global State of Information Security Survey 2021. PwC, 2021.

Schelling, T. (1980). The strategy of conflict. *Harvard University Press.*

Symantec (2021). Internet Security Threat Report 2021. Symantec.

Tayyab, M., Belaton, B.; and Anbar, M. (2020). ICMPv6-based DoS and DDOS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access, 8, 170529–170547.

The MITRE Corporation. (2020). MITRE ATT&CK® Framework. The MITRE Corporation, 2020.

Thomas, R. and Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies 38.1-2 (2015): 4-37.

U.S. Department of Justice. (2020). Indictment of Chinese state-sponsored hackers for cyber espionage activities. Retrieved from [URL] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

Verizon (2020). Data Breach Investigations Report 2020. Verizon

Verizon (2023). Data Breach Investigations Report 2023. Verizon

Vishwakarma, R. and Jain, A.K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication System, 73, 3–25.

Waltz, Kenneth N. (1979). Theory of International Politics. McGraw-Hill Higher Education, 1979.

Zetter, K. (2011). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.

# The Socio-Economic Implications of Terrorism on Human Security in the Horn of Africa Region: The Case of North Eastern Kenya.

***By***

***Samuel Mwiti Njagi and Martin Odhiambo Ouma***

**Abstract**

Terrorism poses a serious threat to peace and security in the international system. Many studies however examine these threats from a state-centric security perspective where the emphasis is on the immediate damages caused when terrorist strike. Though terrorism significantly compromises freedom from fear, it equally affects the freedom from want. This study thus examines the impact of terrorism on human security in the Horn of Africa, with a major focus on the North Eastern region in Kenya. To achieve this objective, the study focuses on how the Al-Shabaab terrorist group has compromised some core qualitative variables such as human rights, sustainable economic opportunities, safety, and the rule of law. The study further underscores how terrorism has created a toxic environment for the attainment of human development in the region. The primary data used to corroborate the secondary sources was obtained through interviews with experts. Expert opinion among security officials, local administrators, and scholars who are versed in the subject was sought. The data analysis entailed triangulation of the forms of data collected, that is, for both primary and secondary sources. The findings of this study depict that human security has been negatively affected by terrorism. The study reveals that the aspects of human security affected by terrorism include human rights, sustainable economic opportunities, safety, the rule of law, and human development. Thus, this study recommends that there is urgent need for policymakers to rethink the impact of terrorism on security from a human security perspective. In addition, the study recommends that counter-terrorism measures should promote safety and the rule of law, participation and human rights, economic opportunities, and human development. Understanding how terrorism impacts human security in North Eastern Kenya is crucial for developing comprehensive security strategies that address the root causes and effects of terrorism, rather than just the symptoms.

**Keywords:** *Al-Shabaab, Social exclusion, sustainable economic opportunities, Socio-cultural Rights*

**Introduction**

The post-Cold War era triggered a paradigm shift in understanding the concept of security. The idea changed from the narrow state-centric view, where the use of military and state security was the main concern, to human security, which is people-centered (Bayeh, 2014). This shift underlines not only the multi-dimensional nature of security but also the fact that security ought to be inclusive, context-specific, and prevention-oriented. The shift to human security was accentuated by the United Nations Development Programme in its Human Development Report (UNDP, 1994).

Though many countries, social actors, and institutions across the globe are now concerned with ways and means of tackling non-military threats to peace to attain human security, many challenges are hindering this endeavor in the Horn of Africa. The most pernicious of these challenges in this region is terrorism (Wyk, 2007).

Though contested in its definition, terrorism gained latitude in policy and academic discourse in the second half of the 19th Century. At the turn of the 20th Century, the intensity and frequency of terrorism worsened, with far-reaching security implications (Makariusova, 2014). Asiedu (2019) underscores that from 1970 to 2017, more than 20,000 cases of terrorism were recorded in Africa. In the Horn of Africa, where diverse terrorist groups have taken advantage of the weak and failed states, terrorism remains one of the major threats to peace and security, with threats leading to the deaths and maiming of many people, destruction of property and generally promoting the atmosphere of fear and insecurity in the region.

Al Shabaab, the main terrorist group in the region, has for instance conducted several attacks in Kenya, including the 2013 Westgate attack, the 2016 Garissa University attack, the 2019 Dusit Hotel complex attack, and the 2014 bus attack that led to the death of 28 non-Muslims. Centre for Human Rights and Policy Studies depicts a 26 percent increase in terrorism incidences in Kenya by Al Shabaab in the year 2022 as compared to 2021 (CHRIPS, 2023). The report further shows that Mandera, Garissa, and Wajir had 37, 21, and 19 terror-related attacks respectively. It underlines that terrorism by Al Shabaab poses a security threat in North Eastern since the frequency of terror-related attacks, largely targeting non-locals and security personnel, has significantly increased (ibid). The trend of terrorism in Kenya depicts that this menace risks destabilizing the country both politically and economically.

The socio-political and economic costs of terrorism in Kenya should be a wake-up call to policymakers and scholars to rethink its impact in terms of human security. This menace has perhaps affected all seven dimensions of human security: political, economic, personal, health, food, community, and environmental security. Though many studies examine the impact of terrorism from a state-centric security perspective, the literature is largely muted on how terrorism affects human security.

It is against this background, that this article seeks to examine the impact of terrorism on human security. The four key indicators of human security adopted from the Ibrahim Index of African Governance (IIAG) report of 1998 have been examined. These indicators, that is, safety and rule of law, participation and human rights, sustainable economic opportunity, and human development have been examined as the key parameters for this study. The study specifically seek to answer the following research questions: Has terrorism threatened human rights in the North Eastern region of Kenya? If yes, in what specific ways? What is the impact of terrorism on sustainable economic opportunities in North Eastern? To what extent has terrorism affected safety and the rule of law in North Eastern region? In what ways has terrorism affected human development in the North Eastern region?

The paper begins by presenting the theoretical framework before examining terrorism and human rights nexus. It seeks to demonstrate how human rights, a key component of human security, have been affected by terrorism in Northern Kenya. Further, the paper analyzes how terrorism has negatively impacted the sustainable economic opportunities in the region before making conclusions and recommendations.

**Theoretical Framework**

This study is anchored on the liberalism theory which observes that peace and security is attainable in the international system through the promotion of democracy, human rights, private property, and free enterprise. Woodrow Wilson who is one of the key proponents of this theory underscores the need to protect human rights such as civil, political, economic, and socio-cultural rights (Menchik, 2021). He further postulates that security could be enhanced by combating deprivations and discrimination that manifest in the form of religious, sexual, and ethnic affiliations amongother factors (Collins, 2019). This theory generally underscores that human beings have inherent rights such as the right to life, liberty, and property which ought to be protected for peaceful co-

existence.

Liberalism underscores the efficacy of maintaining the rule of law for sustainable peace and security. Here the rule of law implies that everyone, including the government, must be subjected to the same law without fear or favor. It emphasizes the need to treat all individuals fairly without discrimination. This paradigm further underlines that even the government does not have arbitrary power to interfere with people's rights. The rule of law thus forms a firm foundation upon which a sustainable and positive peace is maintained in a country or a region. This theory is the most appropriate for this study in examining how terrorism affects the basic dimensions of human security, hence undermining the key tenets of liberalism.

**Study Methodology**

This study was premised on descriptive research design for its suitability in examining people`s social, economic, and political dynamics. It also provided information on key human characteristics of concern like behavior, opinion, beliefs, and knowledge. Different methods for both primary and secondary data collection were applied. Interviews were conducted particularly targeting a target population of 50 participants (Academicians, security experts, practitioners working in civil society organizations, and scholars in the area of security) as shown in Table 1.1. Due to the sensitivity of the subject matter within the region, the study used purposive and snowballing sampling techniques to help draw the study sample. The research findings were therefore analyzed to help answer the set-out study questions.

Table 1
*The Study Target Population*

| **Target group** | **Population** | **Proportion** |
|---|---|---|
| Academicians | 5 | 10% |
| Security experts | 10 | 20% |
| Civil society organizations | 5 | 10% |
| Members of Faith Based Organizations | 10 | 20% |
| Community Representatives | 20 | 40% |
| **Total** | **50** | **100%** |

**Source: Research Data, 2024**

**Discussion of the Findings**

**Terrorism and human rights**

This study observed that, since the end of WW II, several international human rights instruments have been enforced. These include the Universal Declaration of Human Rights of 1948, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, both of 1966 which highlights some of the inalienable rights every individual is entitled to. These rights include the right to life, liberty and security of persons, health, education, adequate food, and clean water, among others which were also affirmed largely by the target population for this study. Additionally, these instruments underscore fundamental freedoms such as freedom from slavery, torture or inhuman treatment, freedom of movement, thought, conscience, and religion that every human being must enjoy (UDHR, 1948; ICCPR, 1966 and ICESCR, 1966). The majority of the respondents, especially from the faith-based institutions observed that protection of the fundamental rights and freedoms was critical in the realization of human security. This was also mentioned by Mwagiru (2008).

Human security underscores "freedom from fear", "freedom from want" and human dignity, focusing on humans as the referent object as highlighted by liberal thought. Mwagiru (2008) observes that this approach to security is paramount for national, regional, and global stability. Many of the respondents in this study observed that human security has been significantly compromised in the HoA. Further, the region has witnessed high levels of terrorism that significantly compromise the freedom from fear

The HoA region has suffered the brunt of terrorism due to several push factors such as lack of access to opportunities, perceived injustices, authoritarian regimes, and weak states (Jose, 2016). In Addition, the region has diverse ethnic and religious groups, some of who feel aggrieved, but sometimes lack avenues to express their dissent. Most of the governments in the region are characterized by high levels of corruption while at the same time lacking control over their borders, an environment that also breeds terrorism. This environment has nurtured terrorism which has negatively people's rights enshrined in most international human rights instruments (Bayeh, 2014).

From the study findings, the majority of the respondents (83%) mainly from the civil society and faith-based groups have observed that the North Eastern part of Kenya had been one of the main theatres of terrorism in the region due to human rights violation-related issues that have seen a bigger percent of the locals joining the terror groups like Al Shabaab. Attacks by Al Shabaab have therefore been a major source of insecurity in the region. This has significantly affected human rights and as a result human security in the region. The attacks carried out by the Alshabab have caused a lot of destruction and deaths, thus breeding fear and uncertainty. For instance, since the year 2011 to date, so many people have lost their lives due to terrorism in this region. Some of the notable cases include but are not limited to: The attack on the Pentecostal Church in Garissa on 5th November 2011, leading to the deaths of two people, the same month on 22nd, a Nairobi bound bus was attacked where 28 people (non-Muslims) were killed, on 2nd December 2014 an attack on quarry workers led to the deaths of 36 people (non-locals) and 2nd April 2015 Garissa University was attacked leading to the deaths of 148 and close to 80 injuries among other attacks.

This study observed that in the case of the North Eastern region, terrorism had affected not only the freedom from fear and want, but also the freedom to live in dignity. It therefore affirms the liberalist theoretical perspective that this study is anchored on which holds that such a menace threatens people's lives, their liberty, social order, and dignity in various ways, including through kidnapping, extortion, assault, hostage-taking, and robbery. These acts of terrorizing members of the public constitute a violation of their rights and dignity. Even though the security of an individual citizen is a fundamental right, individuals living in the North Eastern region are not guaranteed this right, a development that compromises human security.

Terrorism has led to the collapse of the physical, and economic infrastructure in the region. Further, resources that could ideally be allocated for development and other social programs have instead been re-directed to the fight against Al Shabaab, a development that has negatively affected the economic, social, and cultural rights of many civilians in the region. As observed by the majority of respondents drawn from the security fraternity, terrorism has undermined the normal operations of the government in the region, negatively impacting civil society and social and economic development. All these inhibit the enjoyment of the fundamental human rights that are envisaged by liberalism and consequently human security.

The environment of terror in North Eastern has perpetuated abject poverty, and illiteracy, and limited the freedom of movement, especially for non-locals. It has further made it difficult for people to access health care and nutrition in some areas. This situation is made worse whenever there are counter-terrorism operations in the region, viewed as a threat to human security (Akokpari, 2007). As underlined by the theoretical foundation of this study, it would be difficult to achieve the objective of human security in such an environment where human rights are violated daily.

Terrorism has led to forced displacement especially to the non-locals hence negatively affecting learning institutions as non-local teachers targeted by terrorists abandon their duties (UN, 2005). The right to basic education for children from North Eastern region has therefore negatively been affected by terrorism. This is due to the many incidences of terrorism witnessed in the Region, some of which target learning institutions. On 27th October 2011 Ministry of Education officials were attacked where four died; on 16th February 2019 a primary school in Wajir was attacked, leading to the deaths of three teachers of Christian faith and more recently in October 2022, a suspected Al Shabaab terrorist hurled explosive into a primary school in Fino, injuring a class seven pupil. The attack targeted the pupils, teachers, and Members of the County Assembly. These incidences have compromised the right to basic education as enshrined in the Kenyan Constitution.

Besides learning institution, Al shabaab has targeted other socio-economic amenities, thus limiting other rights of the residents. They have destroyed communication infrastructure in the region, sabotaged development projects as many contractors working on road networks have been killed among others. From 2020 to 2022 for instance, Al Shabaab destroyed over ten communication masts in Wajir and Mandera counties besides other development projects. Generally, the attacks have negatively impacted on the socio-economic status of the society and compromised several dimensions of human security.

United Nations Security Council has noted the following regarding the impact of terrorism on human rights:

> Terrorism threatens the dignity and security of human beings everywhere, endangers or takes innocent lives, creates an environment that destroys the freedom from fear of the people, jeopardizes fundamental freedoms, and aims at the destruction of human rights. Moreover, it has an adverse effect on the establishment of the rule of law, undermines pluralistic civil society, aims at the destruction of the democratic bases of society, and destabilizes legitimately constituted Governments (UNSC, 2003).

The frequent use of Improvised Explosive Devices (IEDs) by terrorists has not only led to the death of many but has also maimed thousands and instilled an environment of fear, thus limiting the freedom of movement. Civilians, especially non-locals and security agents find it difficult to freely move and do their businesses due to the fear of attack by IEDs often planted by terror groups. This not only interferes with their freedom of movement but also limits their potential, a situation that leads to structural violence. As underlined in this section, terrorism has negatively affected various human rights in the North Eastern region, thus creating an environment that compromises several dimensions of human security.

**Terrorism and sustainable economic opportunities**

Terrorism has detrimental effects on economic opportunities that manifest directly in terms of both short and long-term- economic opportunities within the region. Terrorism affects economic opportunities directly through deaths, injuries, and destruction of property. Asked about the extent of the effect, 80% affirmed with a yes response whereas 20% downplayed the impact as indicated in Figure 1

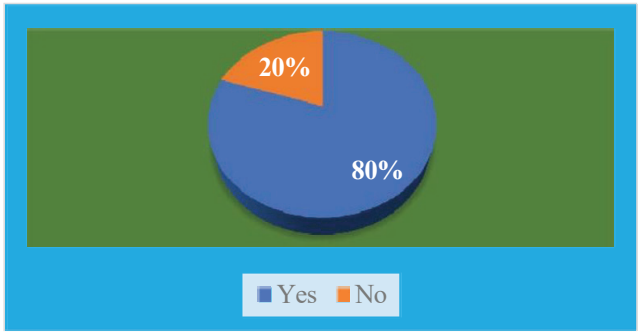


**Figure 1: Socio-economic Impact of Terrorism.**
**Source: Field Data, 2024.**

The maiming, loss of lives and the destruction of private and public properties witnessed during a terrorist attack cause a significant economic disruption (Bardwell and Iqbal, 2020). As was stated

by some respondents, the disruptions inevitably shrink economic activities in the region and subsequently diminish economic opportunities for the residents. Hotel industries and tourism are some of the economic activities that have significantly been affected by terrorism in the region, a development that has reduced job opportunities for the residents.

The high number of terror incidences in the region has culminated in the direct loss of human resources, leading to concomitant loss of production. The attacks have also disrupted the normal functioning of the labor market, leading to high levels of unemployment. Furthermore, the attacks that have targeted health centers, schools, and other public institutions have significantly disrupted access to social services and livelihoods hence the negative effect on the economic opportunities in the region (Ross, 2022).

In line with the liberalist theory which this study is premised, some economic experts interviewed observed that high incidences of terrorism have led to a decrease in Foreign Direct Investments (FDI) and savings. It further diverts funds meant for development projects to security related expenditure. Thus, terrorism has a negative effect on FDI and the volume of trade, a situation that adversely impacts on economic activities and opportunities (Bayrak, 2020). Furthermore, terrorism destroys social structure and order, traditional governance systems and social networks. This makes people live in fear, high levels of uncertainty and economic underdevelopment. This has been the case in North Eastern region where incidences of terrorism have been on the increase in the last decade.

Terrorism has imposed unprecedented levels of emotional toll to not only the residents of North Eastern region, but the entire country. The victims of terrorism whether relatives, friends or the survivors have had to deal with emotional trauma that has sometimes made them unable to engagein productive business. Additionally, terrorism has altered economic behavior mainly by changing investment and consumption patterns. The menace has forced policy makers to divert resources from productive activities to protective security measures. All this has a ripple effect on shrinking the economic opportunities, a development that further heightens cycles of poverty, discontent and more terrorism.

The high levels of uncertainty caused by terrorism in the North Eastern region have led to the diversion of foreign resources to other counties that are considered more peaceful. This has significantly reduced economic opportunities in the region, further exacerbating the already dire economic situation in the region. Further, the uncertainty due to terrorism has led to the postponement of long-term investments in the region. Besides, this menace in the region has made policymakers to shift their attention from productive spending on health, education, food security among others to focus more on security (Meierrieks and Gries, 2013).

Terrorism has bred structural violence in North Eastern region of Kenya, a development that could trigger more instability and rebellion in the future. In addition, the increasing incidences of terrorism in North Eastern have negatively affected economic opportunities in the area of farming, livestock keeping, and infrastructure development. The increasing attacks and extortion by Al Shabaab have made it very difficult for the residents to engage in productive economic activities such as farming and livestock keeping.

> Infrastructural developments such as roads, electricity, water, schools among others have negatively been affected due to the fear of attacks (interview, 2023).

Al-Shabaab activities have been an antithesis to economic growth and development in the North Eastern region. This terrorist group often disrupts main supply routes, a development that hinders trade even between counties in the North Eastern region. The group establishes roadblocks where they extort those transporting food, and medical equipment, among other necessities. It is at the same roadblocks that the terrorists attack those deemed enemies, particularly the non-locals who are not of Islamic faith. This negatively affects economic growth of the region and subsequently diminishes economic opportunities in the area, thus breeding more poverty.

Through interviews, it was reported that Al Shabaab extorts locals through the forced Zakat collection, kidnapping and demanding ransom and sometimes engaging in illegal economic activities such as money laundering, drug trafficking, human smuggling, among other black market practices, a development that negatively affects the genuine business. This sometimes creates a very hostile environment for business to thrive, a development that has forced some locals to

relocate, taking business to other counties. This has a net effect of constricting economic opportunities in the region, hence negatively affecting the human security of the residents.

It is a clear indication therefore that terrorism compromises human security and economic opportunities in diverse ways including : creating an environment of uncertainty where business cannot thrive, forcing domestic and local investors to re-locate their businesses, destruction of properties, killing and maiming productive workforce, disrupting business environment including trading routes among others.

**Terrorism, safety and the rule of Law**

Al Shabaab has significantly affected safety, security, and the rule of law in the North-Eastern region. The group has targeted not only civilians but also national and county leaders. Security personnel, Members of the County Assembly, and Governors have all been targets for attacks. In 2017, the public works principal secretary (PS) was for instance abducted and attacked, leading to her death. In one of the interviews conducted, respondents indicated that this had created a lot of fear among many stakeholders, a situation that continues to compromise the provision of basic services by the government, thus adversely affecting the rule of law.

The majority of the respondents mainly from the security sector (74%) observed that the continued attacks on the security personnel using Improvised Explosive Devices (IEDs) and ambushes have significantly restricted security patrols and vehicle surveillance in the region, hence negatively affecting the law enforcement in the region culminating in lawlessness that creates "ungoverned spaces" that terrorist has in turn used to install informal governance structures where they even collect taxes. This has subsequently compromised accountable and transparent governance, personal security, democracy and various rights and freedoms, hence adversely affecting human security.

The study observed that magistrates, judges and other judicial staff charged with the responsibility to dispense justice in the region operates under intense fear of attack by terrorists. This uncertainty has made many judicial staff to be reluctant to work in North Eastern region, resulting in the delays in delivering justice since only few cases are handled to conclusion. Further, prosecution and

conviction in terrorism cases has been a toll order due to a number of reasons including, the difficulty to convert intelligence into evidence and lack of witnesses to testify for fear of reprisal attacks (Jose, 2016). Failure to deliver justice promptly has had adverse effect on the rule of law and consequently human security in the region.

Actions by Al Shabaab have no regard for human rights which sometimes compels the security forces to respond in ways that may not reflect democratic culture (Aning and Lartey, 2019). The majority of the respondents drawn largely from the security personnel (63%) observed that in cases whereby the society may be seen to be harboring terror suspects and being reluctant to reveal their whereabouts to law enforcement agencies, counter-terrorism operations are therefore likely to result into abuse of human rights. When terrorists target security officers and other key installations, as has been the case mostly in North Eastern Kenya, an officer whose colleague has been killed is likely to hit back vengefully especially in cases whereby the society may be unwilling to cooperate with the security agencies. Thus, locals end up suffering in the hands of terrorists and/or security agencies.

Security agencies have been a major target of terrorists in the North Eastern Region. Since 2019, more than 100 security officers have been killed in the region mainly by suspected terrorists. On 15th June 2019, terrorists attacked and killed 11 police officers and abducted 3 police reservists in Wajir. On 26th October 2019, 11 General Service Unit (GSU) officers were killed and on 6th December the same year, 6 police officers and 4 civilians were killed in Wajir. On 9th January 2020, 4 police officers were killed within the Liboi and Kulan areas of Garissa County (CHRIPS, 2023). Similar attacks were sustained in the year 2021, 2022, and 2023 with many casualties. The latest of these incidences include the attack on the border patrol unit officers, Alunga police station, and the July 2023 attack on the Special Operations Unit in Mandera that claimed the lives of at least 6 security officers *(Ibid)*

Whether during war time, in emergency or at peace, good governance demands that the actions of groups, government institutions or even individuals must be consistent with the law of the land at all times (Igwe, 2014). The rule of law is very critical since it protects civilians from the arbitrary exercise of state power. However, the rule of law is often put under stress when the actions of Al

Shabaab leads to national security emergencies. The actions of terrorists, like Al Shabaab, sometimes also compel governments to enforce curfews that equally undermine the rule of law. This is inconsistent with the liberal thought that envisions a free state where the security of an individual is upheld.

Terrorism continues to erode the social fabric of the residents of North Eastern region due to its disruptive nature on the society, hence affecting it socially by negatively impacting the norms, traditions, and value systems that hitherto hold the community together. Further, many people especially the youth harbor extremist ideologies that continue to erode the social fabric, while the victims of terror live in unprecedented levels of fear and anger, a situation that has compromised community security.

The increasing levels of terrorism fueled partly by other vices such as corruption has heightened impunity in the North Eastern region. Terrorists and sometimes government officials have acted with a lot of impunity, a development that has created an atmosphere where residents feel less obliged to respect the rule of law. To most residents, maintenance of the rule of law has become a burden, rather than an obligation. This is exacerbated by the perception among the residents that, very few terrorism cases are successfully prosecuted and convicted, thus they perceive the region to be a jungle where the rule of law is never taken seriously (Yamamoto, 2017).

The majority of the respondents largely drawn from the NGOs (83%) observed that terrorism coupled with other incidences of insecurity in the North Eastern region has made the area to continue lagging in terms of development as some parts of the region now suffer the acute absence of government services occasioned by insecurity. Mahmud, (2020) affirms this on his accretion that due to acts of terror, some basic services that are ideally supposed to be provided by the government are instead being offered by Non-Governmental organizations (NGOs) whose funding is largely foreign-based. Alade ( 2021) reports that 91 percent of the funding of most local NGOs operating in the area is from international sources, while the local sources and the government account only for 8 and 1 percent respectively. This should raise the question: whose interests do these NGOs serve? Is it the Kenyan government's interests or the interests of those who funds them? This has an indirect negative effect not only on the rule of law and safety but also on human security.

**Terrorism and Human Development**

Based on key indicators such as long and healthy life, decent standard of living life expectancy, education, and career progression, the study examined how terrorism has affected human development. Human development involves the process of enabling people to achieve the goals that they value, engaging them actively in shaping development and expanding their freedom to enjoy long, healthy and creative lives. It also involves empowering individuals in all aspects of life so that they can enjoy greater civil and political liberties (HDR, 2010).

Table 2
*Impact of Terrorism on Human Development*

| Key Indicators | Number of Respondents | Proportion |
|---|---|---|
| Long and healthy life | 20 | 40% |
| Decent standard of living | 10 | 20% |
| Life expectancy | 5 | 10% |
| Education and Currier progression | 25 | 50% |
| **Total** | **50** | **100%** |

**Source: Research Data, 2024**

The study reveals that terrorism has had adverse effects on human development in an already vulnerable region as captured on Table 2 It has negatively affected business activities, leading to retarded economic growth in the region. It has further culminated in low enrolment rates in schools, high rates of illiteracy, poor water and sanitation services and low levels of health care services among other basic services, hence significantly compromising the standards of living and subsequently human development.

Human security must underline sustainability, equity and grassroots participation to allow citizens to exercise their many choices including access to markets and social opportunities, a move that plays a key role in promoting human development (UNDP, 1994). Engaging residents actively in shaping development is a key pillar in promoting human development (Mahmud, 2020). However, the high levels of terrorism in North Eastern region has negatively affected the cardinal pillars of human development, including market sustainability, equity, grassroots participation and

stakeholder engagement in shaping development, hence compromised the key pillars of human development and negatively affecting human security.

Alkire (2003) links human development to human security by observing that the latter is the pre-condition for the former. He asserts that an underlying pre-condition for sustainable human development is human security. This is because human security addresses various aspects of human life such as psychological, social, political, and economic. He further observes that in times of crisis or severe deprivations, these aspects are compromised, making the survival of individuals and groups very difficult. These compromises subsequently affect a decent standard of living, life expectancy, and health, which are some of the key indicators of human development. This underscores the United Nations report which argues that countries can achieve sustainable development by promoting human security (UN, 1994).

The increased incidences of terrorist attacks in the North Eastern Region have decreased the legitimacy of the government in the region. The residents feel alienated and their political security is threatened. They feel their social contract with the government has been breached, hence they rarely depend on the government for some services, including provision of security. This has hindered the residents from achieving their set goals in life, shaping development in the region, and enjoying long, healthy, and creative lives, thus affecting human development and security.

**Conclusion**

This study depicts that human security in the North Eastern region of Kenya has been significantly affected by terrorism which has in turn negatively affected some of the key qualitative indicators of human security such as human rights, sustainable economic opportunities, safety, the rule of law and human development. This has culminated in high levels of insecurity, human rights abuse, diminished economic opportunities, and disregard for the rule of law by the residents, a development that has further bred more terror groups.

Further, the study reveals that terrorism has detrimental effects on economic opportunities in North Eastern region. These effects manifest either directly in terms of short-term costs of terrorism on economic opportunities or indirectly in terms of medium or long-term costs. The direct short-term

costs of terrorism includes deaths, injuries and the properties destroyed when terrorists attack. The indirect costs of terrorism on economic opportunities may include the uncertainty that terrorism creates that kills the investor confidence, diverting resources that would have been used for development in counter-terrorism, the failure by residents to engage in productive economic activities such as farming and livestock keeping due to terrorism and low production in various sectors due to insecurity. This in turn compromises several dimensions of human security.

Terrorism has adverse effects on human development in an already vulnerable region. It has negatively affected welfare improvement, human capital development and business activities in the region. This has culminated in low enrolment rates in schools, high rates of adult illiteracy, poor economic growth and low levels of service delivery. As a result, this has negatively affected the standards of living and subsequently human security. The high levels of terrorism in North Eastern region have negatively affected the cardinal pillars of human development, including market sustainability, equity, and grassroots participation in shaping development. This has culminated in human insecurity in the region.

**Recommendations**

Based on the findings of this study, this paper recommends that policymakers need to rethink the impact of terrorism on security in the region from a human security perspective. It, therefore, recommends that policymakers should come up with policies that address not only the direct short-term costs of terrorism but also the indirect costs that examine structural issues that have far-reaching implications on an individual or the society at large. Policymakers and scholars have largely been examining the effect of terrorism from the direct short-term costs which is largely narrow in scope.

Effective counter-terrorism measures and the protection of human rights are complementary and mutually reinforcing objectives which stakeholders must take a pensive balancing to pursue together as part of the intervention strategy and a duty to protect individuals within their jurisdiction.

The study further recommends that counter-terrorism measures should seek to restore confidence among residents by addressing the key indicators of human security often negatively affected by terrorism. These indicators are safety and rule of law, participation and human rights, sustainable economic opportunities, and human development.

**References**

Akokpari, J. (2007) The Political Economy of Human Insecurity in Sub-Saharan Africa, VRF Series, No. 431

Alade, O.B et al (2021) Terrorism, Human Capital Development and Economic Growth in Nigeria, *International Journal of Economics Development Research, Vol. 2, no. 2*

Aning, K (2007) Africa's Major Human and International Security Challenges, *International Peace Institute*

Aning, K and Lartey, E.A (2019) Governance Perspectives of Human Security in Africa, *Asian Journal of Peace Building,* Vol. 7, No. 2

Arin, K.P et al, (2016) Brutality or Frequency? An Empirical Investigation of the Effects of Terrorism on Economic Growth in India, *Revue Economique*, Vol. 67, No. 6

Badayneh, D.A (2010) Human Development, Peace, Corruption and Terrorism in the Arab World, Research Gate

Bardwell, H and Iqbal, M. (2020) The Economic Impact of Terrorism from 2000 to 2018, *Peace Economics Peace Science and Public Policy*

Bayeh, E. (2014) Human Security in the Horn of Africa: Trends and Challenges, *International Journal of Multidisciplinary Research and Development,* vol. 1, No. 7,

Bayrak, R. (2020) *A Literature Review on "The Effects of Terrorism on Economy*".

Benedek, W. (2008) Rethinking Human Security, *International Social Science Journal*

Debrah, R.A (2021) An Assessment of the Socio-Economic Effects of Terrorism in the Sahel Region of West Africa Ghana, *Research Gate*

Jose, L. (2016) Countering Violent Extremism: The Horn of Africa, *European Union Institute for Security Studies*

Menchik, J (2021). Woodrow Wilson and the Spirit of Liberal Internationalism. *Politics, Religion & Ideology* 22(2)

Mahmud, S.F. (2020) The Impact of Terrorism on Human Development in Iraq, *Global Journal of Management and Economics,* Vol. 1, No.1

Makumi, M. (2008) Human Security: Setting the Agenda for the Horn of Africa, *Kenya Africa Peace Forum*

Meierrieks, D. and Gries, T. (2013) Causality between Terrorism and Economic Growth, *Journal of Peace Research*, Vol. 50, No. 1

Ombaka, D.M (2015) Explaining Kenya's Insecurity: The Weak State, Corruption, Banditry and Terrorism, *International Journal of Liberal Arts and Social Science*, Vol. 3, No. 3

Rathbone A. and Rowley C. K. Terrorism, *Public Choice, Mar. 2002,* Vol. 111, No. 1/2 (Mar., 2002)

Shinn D. Poverty and Terrorism in Africa: The Debate Continues, *Georgetown Journal of International Affairs, Summer/Fall 2016*, Vol. 17, No. 2 (Summer/Fall 2016)

Wilkinson, P. 1974. Political Terrorism, Macmillan Press, London

Wojciechowski, S. 2016. Reasons of Contemporary Terrorism: An Analysis of the Main Determinants, In Sroka, A. et al, Radicalism and Terrorism in the 21st Century

Yamamoto, M. 2017. The Cause and Threat of Terrorism, Center for International and Security Studies, U Maryland

## Authors Biographies

**Colonel Evans Ombati Onchweri**

Colonel Evans Ombati Onchweri is a senior officer in the Kenya Defence Forces (KDF) with expertise in cybersecurity, intelligence, and computing. Currently, he serves as the Colonel of Research at the Centre for Security and Strategic Studies (CSSS) at the National Defence University-Kenya (NDU-K). Previously, he was the Director at the National Computer and Cybercrimes Coordination Committee (NC4) and served as the Senior Officer in charge of Technical Intelligence at Defence Headquarters. He holds a Master of Science in ICT Policy and Regulation and a Bachelor of Science in Computer Science and has completed various military education programs.

**Gen (Dr) Robert K Kibochi**

General Robert Kariuki Kibochi served as the Chief of the Kenya Defence Forces from 2020 to 2023. Throughout his career, he held various important command and staff positions, including Vice Chief of the Defence Forces, Commander of the Kenya Army, Assistant Chief of Defence Forces in charge of Operations, Plans, Doctrine and Training at Defence Headquarters (DHQ), Chief of Strategic Plans and Policy, Director of the International Peace Support Training Centre, Col Operations Requirements (CIS), and Commander of the Corps of Signals. Gen Kibochi holds a PhD degree in Peace and Conflict Management, a master's Degree in International Studies, a master's Degree in Computer Information Systems, and a Bachelor of Technology in Communication and Electronics Engineering. He has also completed professional training in National Security Studies at the National Defence College (Kenya), Army Command and Staff Course (UK), Overseas Telecoms Engineering Course (UK), Signal Officers Degree Telecommunications Engineering Course (India), Sub Unit Commanders Course, Platoon Commanders Course, Regimental Signal Officers Course, and other relevant training courses.

**Prof. Lucy W. Maina (Ph.D, OGW**

Prof. Lucy W. Maina (Ph.D, OGW) is an Associate Professor of Sociology at the Department of Sociology, Gender and Development and is the immediate former Dean of the School of Security, Diplomacy and Peace Studies at Kenyatta University. She has over

25 years of experience in higher education which includes programme development and training in Military and strategic studies, security and peace studies, International Relations areas as well as Corrections. She is an avid researcher and has published widely in peer reviewed journal outlets.

**Prof. Fred Jonyo**

Fred Jonyo is the current Chairman of the Department of Political Science and Public Administration at the University of Nairobi. He has a Bachelor's Degree in Anthropology and Political Science from the University of Nairobi, a Master's Degree in International Relations from the International University of Japan, and a PhD in Political Science and Public Administration from Makerere University in Uganda. His areas of specialization include Political Economy, International Relations, Trade and Investment Policy, and Security Studies. He has also held various government appointments and provided consulting services for organizations such as the National Assembly, Center for Parliamentary Studies and Training, National Counter Terrorism Center, and others.

**Thuranira Mark and Nick Chemosit**

Thuranira Mark and Nick Chemosit work in the public sector and are Ph.D. scholars at Kenyatta University's Department of Public Policy and Administration. Their research focus on "Managing the Commons and the Sustainability of Kenya's Blue Economy" and "Policy Networks and Shaping of Climate Security in Kenya," respectively. Both have published in peer-reviewed journals.

**FA Ndirangu Ngunjiri**

FA Ndirangu Ngunjiri is a Doctoral (Finance & Accounting) fellow at the University of Nairobi with a research interest in; inequality & poverty, cyber security, climate change, innovations, international trade, and productivity. He is a full member of the Institute of Directors, Institute of Internal Auditors, and Institute of Certified Financial Analysts.

**Dr. Martin Odhiambo Ouma**

Dr. Martin Odhiambo Ouma is a Senior lecturer at the University of Nairobi, Department of Diplomacy and International Studies (DDIS). He is a holder of PhD in International studies and a distinguished scholar with wide experience in postgraduate teaching and supervision. His key thematic areas of teaching and competency include: Academic research methodology and also in international studies with specialty in international security, peace studies, strategic studies and diplomacy, areas under which he has taught, mentored and supervised several PhD and Master's Degree students.

**Col (Dr) James J Kimuyu, PhD**

Col (Dr) James J Kimuyu, PhD is the Director at the National Computer and Cybercrimes Coordination Committee (NC4), Kenya national body mandated with cybersecurity matters under the Ministry of Internal Security and National Administration. He holds a PhD in Information Systems, MSc in Information Systems, BSc in Information Sciences and PgD in Strategic Studies. Before he joined NC4, he was a Senior Lecturer and Head of Research at the Centre for Security and Strategic Studies (CSSS), a national think tank under the National Defence University-Kenya (NDU-K). He has over 23 years' experience in Military and National security, Cybersecurity, Information Systems development and deployment, university level teaching, research, strategic analysis, curriculum development, aviation and technical maintenance support and quality assurance.

**Dr. Mumma-Martinon**

Dr. Mumma-Martinon is a lecturer in the University of Nairobi's Department of Political Science and a member of the National Defence University - Kenya. She holds a PhD in Political Science (International Conflict Management) from the University of Leipzig, Germany, and a Master's in Diplomacy and International Studies. She has taught at various institutions and worked at IPSTC as Head of Applied Research and trainer. She has supervised PhD. Masters and undergraduate students. She has numerous publications and authored "MA and PhD Thesis Writing: A Practical Guide."

**Dr. Samuel Mwiti Njagi**

Dr. Samuel Mwiti Njagi is a senior lecturer at the National Intelligence and Research University College (NIRUC). He has a PhD in International Studies and an M.A in International Conflict Management, both from the University of Nairobi- Institute of Diplomacy and International Studies. Further, Dr. Njagi has a post graduate Diploma in Security and Strategic Studies, from the University of Nairobi- Department of Political Science and a bachelor's degree in education from Kenyatta University. He is currently pursuing another bachelor's degree in Biblical Studies at Ethnos College, United States of America. His research interests include human security, geopolitics and violent extremism.

**Dr. Martine Ouma Oleche**

Martine Oleche holds a Doctor of Philosophy Degree in Economics from the University of Nairobi. He is a Senior Lecturer and Chairman of the Department of Economics and Development Studies at the University of Nairobi, specializing in Development Economics, Health Economics, and Economic Policy Analysis. Prior to his current role, he worked at The National Treasury and Economic Planning, focusing on Economic Policy matters. Martine has also conducted training for various government institutions on enhancing


NATIONAL DEFENCE UNIVERSITY - KENYA
P.O. BOX 3812-20100
NAKURU